RÉPUBLIQUE DE CÔTE D'IVOIRE

AUTORITÉ DE RÉGULATION DES TÉLÉCOMMUNICATIONS/TIC

ARTCI

POLITIQUE DE CONFIDENTIALITÉ DE LA PLATEFORME CERTINUM

La présente politique établit, de façon complète, les règles de collecte, d'utilisation, de communication, de conservation, d'archivage, de sécurisation et de gouvernance des données à caractère personnel traitées dans le cadre de l'exploitation de la plateforme CERTINUM. Elle affirme expressément que CERTINUM est la propriété exclusive de l'ARTCI et qu'à ce titre, cette dernière détermine les finalités, les moyens de traitement et les garanties applicables à l'ensemble des traitements mis en oeuvre sur la plateforme.

Ce document a été rédigé pour servir de référence opérationnelle, juridique, organisationnelle et institutionnelle. Il peut être annexé à des documents contractuels, intégré à un dispositif de conformité, communiqué aux usagers de la plateforme ou conservé comme texte officiel de gouvernance interne et externe en matière de protection des données.

APPROBATION, PORTÉE ET FORCE DU DOCUMENT

La présente politique de confidentialité est adoptée comme document institutionnel de référence applicable à la plateforme CERTINUM. Elle engage l'ARTCI dans son rôle de propriétaire exclusif de la plateforme et de responsable de la gouvernance des données qui y sont traitées, sous réserve des délégations internes, des mandats techniques et des contrats de sous-traitance conclus pour le fonctionnement du service.

Le document a vocation à être lu comme un ensemble cohérent. Chaque article précise une obligation, un principe, une méthode de contrôle, un mécanisme de sécurisation ou une modalité d'exercice des droits. Les dispositions doivent être interprétées de manière complémentaire afin d'assurer un haut niveau de protection des personnes concernées, de sécurité des dossiers, de conformité réglementaire et de confiance institutionnelle.

En cas de divergence entre une version abrégée, une note d'information, une foire aux questions ou tout autre support de vulgarisation, la présente version détaillée prévaut. Cette hiérarchie documentaire permet de sécuriser la doctrine applicable, de limiter les interprétations contradictoires et de garantir que la plateforme fonctionne selon un référentiel clair, stable et opposable.

La politique est destinée à être signée, approuvée et diffusée selon les modalités fixées par l'ARTCI. Elle peut être complétée par des procédures internes, des chartes d'habilitation, des instructions de sécurité, des clauses contractuelles, des engagements de confidentialité, des registres de traitement, des plans de continuité d'activité et des rapports d'audit.

ARTICLE 1 - OBJET, AMBITION ET PHILOSOPHIE GÉNÉRALE DU DOCUMENT

OBJET, AMBITION ET PHILOSOPHIE GÉNÉRALE DU DOCUMENT est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à objet du document. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à objet du document doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier objet du document à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de protection des personnes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour objet du document sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de objet du document doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à philosophie de confiance numérique. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à philosophie de confiance numérique doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier philosophie de confiance numérique à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sécurité juridique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour philosophie de confiance numérique sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système,

de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de philosophie de confiance numérique doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à propriété exclusive de l'ARTCI. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à propriété exclusive de l'ARTCI doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier propriété exclusive de l'ARTCI à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de souveraineté numérique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour propriété exclusive de l'ARTCI sont pertinentes, documentées et effectivement appliquées. Cette

démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de propriété exclusive de l'ARTCI doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à objet du document. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à objet du document doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier objet du document à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de protection des personnes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour objet du

document sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de objet du document doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à philosophie de confiance numérique. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à philosophie de confiance numérique doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier philosophie de confiance numérique à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sécurité juridique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour philosophie de confiance numérique sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de philosophie de confiance numérique doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à philosophie de confiance numérique demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à propriété exclusive de l'ARTCI. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à propriété exclusive de l'ARTCI doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier propriété exclusive de l'ARTCI à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de souveraineté numérique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour propriété exclusive de l'ARTCI sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de propriété exclusive de l'ARTCI doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 2 - IDENTITÉ DU RESPONSABLE DU TRAITEMENT ET STATUT DE LA PLATEFORME

IDENTITÉ DU RESPONSABLE DU TRAITEMENT ET STATUT DE LA PLATEFORME est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à responsable du traitement. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits,

l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à responsable du traitement doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier responsable du traitement à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de maîtrise des finalités joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour responsable du traitement sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de responsable du traitement doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à gouvernance institutionnelle. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de

sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à gouvernance institutionnelle doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier gouvernance institutionnelle à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de pouvoir de décision joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour gouvernance institutionnelle sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de gouvernance institutionnelle doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à qualité de propriétaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à qualité de propriétaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier qualité de propriétaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de obligations de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour qualité de propriétaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de qualité de propriétaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à responsable du traitement. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à responsable du traitement doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier responsable du traitement à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de maîtrise des finalités joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour responsable du traitement sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de responsable du traitement doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à responsable du traitement demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à gouvernance institutionnelle. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à gouvernance institutionnelle doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier gouvernance institutionnelle à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de pouvoir de décision joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour gouvernance institutionnelle sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices

d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de gouvernance institutionnelle doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à qualité de propriétaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à qualité de propriétaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier qualité de propriétaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de obligations de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour qualité de propriétaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration

peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de qualité de propriétaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 3 - DÉFINITIONS, INTERPRÉTATIONS ET LECTURE DES TERMES

DÉFINITIONS, INTERPRÉTATIONS ET LECTURE DES TERMES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à définitions opératoires. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à définitions opératoires doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier définitions opératoires à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de donnée personnelle joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour définitions opératoires sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de définitions opératoires doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à portée des expressions. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à portée des expressions doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier portée des expressions à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif

est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traitement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour portée des expressions sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de portée des expressions doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à interprétation uniforme. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à interprétation uniforme doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier interprétation uniforme à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées,

selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personne concernée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour interprétation uniforme sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de interprétation uniforme doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à interprétation uniforme demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à définitions opératoires. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à définitions opératoires doit être pensée au

regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier définitions opératoires à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de donnée personnelle joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour définitions opératoires sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de définitions opératoires doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à portée des expressions. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la

plateforme, affirme que toute opération relative à portée des expressions doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier portée des expressions à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traitement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour portée des expressions sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de portée des expressions doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à interprétation uniforme. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée

réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à interprétation uniforme doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier interprétation uniforme à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personne concernée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour interprétation uniforme sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de interprétation uniforme doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 4 - CHAMP D'APPLICATION MATÉRIEL, PERSONNEL ET TERRITORIAL

CHAMP D'APPLICATION MATÉRIEL, PERSONNEL ET TERRITORIAL est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à usagers concernés. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à usagers concernés doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier usagers concernés à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personnes physiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour usagers concernés sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de usagers concernés doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à opérations couvertes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à opérations couvertes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier opérations couvertes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personnes morales joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour opérations couvertes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de opérations couvertes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à opérations couvertes demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à environnement territorial. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à environnement territorial doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier environnement territorial à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prestataires et partenaires joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour environnement territorial sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de environnement territorial doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à usagers concernés. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à usagers concernés doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier usagers concernés à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personnes physiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être

proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour usagers concernés sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de usagers concernés doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à opérations couvertes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à opérations couvertes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier opérations couvertes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de personnes morales joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour opérations couvertes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de opérations couvertes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à environnement territorial. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à environnement territorial doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier environnement territorial à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prestataires et partenaires joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures

d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour environnement territorial sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de environnement territorial doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 5 - PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES

PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à licéité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à licéité doit être pensée au regard de la protection des personnes

concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier licéité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de limitation des finalités joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour licéité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de licéité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à licéité demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à loyauté et transparence. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à loyauté et transparence doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier loyauté et transparence à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de intégrité et confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour loyauté et transparence sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de loyauté et transparence doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à minimisation et exactitude. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à minimisation et exactitude doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier minimisation et exactitude à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de responsabilité démontrable joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour minimisation et exactitude sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de minimisation et exactitude doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à licéité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à licéité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier licéité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de limitation des finalités joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour licéité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de licéité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas

seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à loyauté et transparence. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à loyauté et transparence doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier loyauté et transparence à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de intégrité et confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour loyauté et transparence sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de loyauté et transparence doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix

répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à minimisation et exactitude. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à minimisation et exactitude doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier minimisation et exactitude à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de responsabilité démontrable joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour minimisation et exactitude sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de minimisation et exactitude doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est

pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à minimisation et exactitude demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM

.

ARTICLE 6 - CADRE JURIDIQUE APPLICABLE ET SOURCES NORMATIVES

CADRE JURIDIQUE APPLICABLE ET SOURCES NORMATIVES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à loi ivoirienne 2013-450. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à loi ivoirienne 2013-450 doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier loi ivoirienne 2013-450 à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de bonnes pratiques internationales joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour loi ivoirienne 2013-450 sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de loi ivoirienne 2013-450 doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à cybercriminalité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à cybercriminalité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier cybercriminalité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif

est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.
En outre, la notion de doctrine de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour cybercriminalité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de cybercriminalité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à transactions électroniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à transactions électroniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier transactions électroniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées,

selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sécurité réglementaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour transactions électroniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de transactions électroniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à loi ivoirienne 2013-450. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à loi ivoirienne 2013-450 doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier loi ivoirienne 2013-450 à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni

manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de bonnes pratiques internationales joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour loi ivoirienne 2013-450 sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de loi ivoirienne 2013-450 doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à cybercriminalité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à cybercriminalité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier cybercriminalité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité

identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de doctrine de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour cybercriminalité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de cybercriminalité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à cybercriminalité demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à transactions électroniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion

de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à transactions électroniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier transactions électroniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sécurité réglementaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour transactions électroniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de transactions électroniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces

supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 7 - CATÉGORIES DE DONNÉES COLLECTÉES ET NIVEAUX DE SENSIBILITÉ

CATÉGORIES DE DONNÉES COLLECTÉES ET NIVEAUX DE SENSIBILITÉ est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à identification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à identification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier identification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de classification interne joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour identification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de

remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de identification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à coordonnées. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à coordonnées doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier coordonnées à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sensibilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour coordonnées sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus

de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de coordonnées doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à données techniques et dossiers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à données techniques et dossiers doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier données techniques et dossiers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de nécessité de traitement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour données

techniques et dossiers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de données techniques et dossiers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à identification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à identification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier identification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de classification interne joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ;

il faut encore que l'ARTCI puisse prouver que les modalités retenues pour identification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de identification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à identification demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à coordonnées. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à coordonnées doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier coordonnées à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sensibilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles

d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour coordonnées sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de coordonnées doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à données techniques et dossiers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à données techniques et dossiers doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier données techniques et dossiers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de nécessité de traitement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour données techniques et dossiers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de données techniques et dossiers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 8 - MODALITÉS DE COLLECTE ET MOMENTS DU TRAITEMENT

MODALITÉS DE COLLECTE ET MOMENTS DU TRAITEMENT est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à inscription. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire.

Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à inscription doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier inscription à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de parcours utilisateur joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour inscription sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de inscription doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à soumission de dossiers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la

production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à soumission de dossiers doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier soumission de dossiers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de journalisation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour soumission de dossiers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de soumission de dossiers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à collecte indirecte. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les

informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à collecte indirecte doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier collecte indirecte à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour collecte indirecte sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de collecte indirecte doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à collecte indirecte demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à inscription. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à inscription doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier inscription à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de parcours utilisateur joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour inscription sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de inscription doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à soumission de dossiers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à soumission de dossiers doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier soumission de dossiers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de journalisation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour soumission de dossiers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de soumission de dossiers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à collecte indirecte. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à collecte indirecte doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier collecte indirecte à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour collecte indirecte sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de collecte indirecte doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 9 - FINALITÉS DÉTAILLÉES DES TRAITEMENTS

FINALITÉS DÉTAILLÉES DES TRAITEMENTS est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à gestion des comptes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à gestion des comptes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier gestion des comptes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prévention des fraudes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour gestion des comptes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de gestion des comptes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à conformité réglementaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à conformité réglementaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier conformité réglementaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de pilotage du service joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures

d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour conformité réglementaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de conformité réglementaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à conformité réglementaire demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à amélioration du service. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à amélioration du service doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier amélioration du service à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à

une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de production de preuve joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour amélioration du service sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de amélioration du service doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à gestion des comptes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à gestion des comptes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier gestion des comptes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la

capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prévention des fraudes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour gestion des comptes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de gestion des comptes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à conformité réglementaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à conformité réglementaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier conformité réglementaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de pilotage du service joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour conformité réglementaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de conformité réglementaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à amélioration du service. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à amélioration du service doit être pensée au regard de la protection des personnes concernées, de la

préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier amélioration du service à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de production de preuve joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour amélioration du service sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de amélioration du service doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 10 - BASES LÉGALES DES TRAITEMENTS ET JUSTIFICATION DE LEUR USAGE

BASES LÉGALES DES TRAITEMENTS ET JUSTIFICATION DE LEUR USAGE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à consentement. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à consentement doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier consentement à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de intérêt légitime de sécurité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour consentement sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de consentement doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à consentement demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à obligation légale. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à obligation légale doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier obligation légale à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de équilibre des intérêts joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour obligation légale sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de obligation légale doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à exécution du service. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à exécution du service doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier exécution du service à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité de la base légale joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour exécution du service sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de exécution du service doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à consentement. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à consentement doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier consentement à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de intérêt légitime de sécurité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être

proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour consentement sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de consentement doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à obligation légale. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à obligation légale doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier obligation légale à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de équilibre des intérêts joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour obligation légale sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de obligation légale doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à exécution du service. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à exécution du service doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier exécution du service à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité de la base légale joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures

d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour exécution du service sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de exécution du service doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à exécution du service demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 11 - INFORMATION DES UTILISATEURS, TRANSPARENCE ET PREUVES D'INFORMATION

INFORMATION DES UTILISATEURS, TRANSPARENCE ET PREUVES D'INFORMATION est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à information préalable. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à information préalable doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier information préalable à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mentions visibles joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour information préalable sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de information préalable doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à formulation claire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à formulation claire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier formulation claire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mise à jour joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour formulation claire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de formulation claire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix

répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à preuve de délivrance. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à preuve de délivrance doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier preuve de délivrance à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité documentaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour preuve de délivrance sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de preuve de délivrance doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est

pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à information préalable. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à information préalable doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier information préalable à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mentions visibles joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour information préalable sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de information préalable doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à formulation claire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à formulation claire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier formulation claire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mise à jour joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour formulation claire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de formulation claire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à formulation claire demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à preuve de délivrance. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à preuve de délivrance doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier preuve de délivrance à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité documentaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour preuve de délivrance sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de preuve de délivrance doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 12 - COOKIES, TRACEURS, JOURNAUX TECHNIQUES ET ANALYSE D'USAGE

COOKIES, TRACEURS, JOURNAUX TECHNIQUES ET ANALYSE D'USAGE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à traceurs techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à traceurs techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier traceurs techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation

des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de consentement lorsque requis joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour traceurs techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de traceurs techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à sécurité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à sécurité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier sécurité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de préférences utilisateur joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour sécurité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de sécurité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à mesure d'audience. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesure d'audience doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesure d'audience à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de conservation limitée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesure d'audience sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesure d'audience doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à traceurs techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à traceurs techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier traceurs techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de consentement lorsque requis joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour traceurs techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de traceurs techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à traceurs techniques demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à sécurité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à sécurité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier sécurité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de préférences utilisateur joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour sécurité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de sécurité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à mesure d'audience. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesure d'audience doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesure d'audience à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de conservation limitée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesure d'audience sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesure d'audience doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 13 - SÉCURITÉ DES DONNÉES ET ARCHITECTURE DE PROTECTION

SÉCURITÉ DES DONNÉES ET ARCHITECTURE DE PROTECTION est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à mesures techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesures techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesures techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de chiffrement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesures techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesures techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à mesures organisationnelles. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesures organisationnelles doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesures organisationnelles à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de authentification joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesures organisationnelles sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesures organisationnelles doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à défense en profondeur. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à défense en profondeur doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier défense en profondeur à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de surveillance continue joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour défense en profondeur sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de défense en profondeur doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à défense en profondeur demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à mesures techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesures techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesures techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées,

selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de chiffrement joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesures techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesures techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à mesures organisationnelles. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à mesures organisationnelles doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier mesures organisationnelles à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à

une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de authentification joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour mesures organisationnelles sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de mesures organisationnelles doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à défense en profondeur. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à défense en profondeur doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier défense en profondeur à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation

des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de surveillance continue joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour défense en profondeur sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de défense en profondeur doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 14 - GESTION DES ACCÈS, HABILITATIONS ET RESPONSABILITÉS INTERNES

GESTION DES ACCÈS, HABILITATIONS ET RESPONSABILITÉS INTERNES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à moindre privilège. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à moindre privilège doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier moindre privilège à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de revue des accès joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour moindre privilège sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de moindre privilège doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à séparation des rôles. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à séparation des rôles doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier séparation des rôles à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de journalisation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour séparation des rôles sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de séparation des rôles doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à séparation des rôles demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à contrôle périodique. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à contrôle périodique doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier contrôle périodique à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sanctions internes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour contrôle périodique sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de contrôle périodique doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à moindre privilège. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à moindre privilège doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier moindre privilège à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de revue des accès joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour moindre privilège sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de moindre privilège doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à séparation des rôles. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à séparation des rôles doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier séparation des rôles à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de journalisation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être

proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour séparation des rôles sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de séparation des rôles doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à contrôle périodique. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à contrôle périodique doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier contrôle périodique à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de sanctions internes joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour contrôle périodique sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de contrôle périodique doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 15 - PROTECTION DES DOSSIERS CONFIDENTIELS ET DOCUMENTS SENSIBLES

PROTECTION DES DOSSIERS CONFIDENTIELS ET DOCUMENTS SENSIBLES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à dossiers déposés. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à dossiers déposés doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier dossiers déposés à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de restriction d'accès joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour dossiers déposés sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de dossiers déposés doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à dossiers déposés demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à documents probants. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée

comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à documents probants doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier documents probants à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de lecture contrôlée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour documents probants sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de documents probants doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à renforcement des protections. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à renforcement des protections doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier renforcement des protections à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de copie limitée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour renforcement des protections sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de renforcement des protections doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de

confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à dossiers déposés. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à dossiers déposés doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier dossiers déposés à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de restriction d'accès joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour dossiers déposés sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de dossiers déposés doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix

répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à documents probants. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à documents probants doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier documents probants à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de lecture contrôlée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour documents probants sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de documents probants doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est

pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à renforcement des protections. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à renforcement des protections doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier renforcement des protections à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de copie limitée joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour renforcement des protections sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de renforcement des protections doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à renforcement des protections demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 16 - HÉBERGEMENT, LOCALISATION, SOUVERAINETÉ ET MAÎTRISE INFRASTRUCTURELLE

HÉBERGEMENT, LOCALISATION, SOUVERAINETÉ ET MAÎTRISE INFRASTRUCTURELLE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à hébergement sécurisé. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à hébergement sécurisé doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier hébergement sécurisé à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à

une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de contrôle contractuel joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour hébergement sécurisé sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de hébergement sécurisé doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à localisation maîtrisée. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à localisation maîtrisée doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier localisation maîtrisée à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation

des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de protection juridique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour localisation maîtrisée sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de localisation maîtrisée doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à souveraineté. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à souveraineté doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier souveraineté à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de résilience joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour souveraineté sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de souveraineté doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à hébergement sécurisé. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à hébergement sécurisé doit être pensée au regard de la protection des personnes concernées, de la

préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier hébergement sécurisé à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de contrôle contractuel joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour hébergement sécurisé sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de hébergement sécurisé doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à localisation maîtrisée. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de

propriétaire exclusif de la plateforme, affirme que toute opération relative à localisation maîtrisée doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier localisation maîtrisée à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de protection juridique joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour localisation maîtrisée sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de localisation maîtrisée doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à localisation maîtrisée demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité

crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à souveraineté. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à souveraineté doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier souveraineté à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de résilience joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour souveraineté sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de souveraineté doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix

répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 17 - CONSERVATION, ARCHIVAGE, TRI ET SUPPRESSION SÉCURISÉE

CONSERVATION, ARCHIVAGE, TRI ET SUPPRESSION SÉCURISÉE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à durées de conservation. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à durées de conservation doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier durées de conservation à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de besoin probatoire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour durées de conservation sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de durées de conservation doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à archivage intermédiaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à archivage intermédiaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier archivage intermédiaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de obligation légale joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour archivage intermédiaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de archivage intermédiaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à destruction sécurisée. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à destruction sécurisée doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier destruction sécurisée à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de réduction du risque joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures

d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour destruction sécurisée sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de destruction sécurisée doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à durées de conservation. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à durées de conservation doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier durées de conservation à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de besoin probatoire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour durées de conservation sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de durées de conservation doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à durées de conservation demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à archivage intermédiaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à archivage intermédiaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier archivage intermédiaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de obligation légale joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour archivage intermédiaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de archivage intermédiaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à destruction sécurisée. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à destruction sécurisée doit être pensée au regard de la protection des personnes concernées, de la

préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier destruction sécurisée à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de réduction du risque joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour destruction sécurisée sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de destruction sécurisée doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 18 - DESTINATAIRES DES DONNÉES ET PARTAGE STRICTEMENT ENCADRÉ

DESTINATAIRES DES DONNÉES ET PARTAGE STRICTEMENT ENCADRÉ est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à personnels habilités. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à personnels habilités doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier personnels habilités à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de besoin d'en connaître joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour personnels habilités sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de personnels habilités doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à prestataires. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à prestataires doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier prestataires à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour prestataires sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de prestataires doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à autorités compétentes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à autorités compétentes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier autorités compétentes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de encadrement contractuel joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour autorités compétentes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système,

de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de autorités compétentes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à autorités compétentes demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à personnels habilités. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à personnels habilités doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier personnels habilités à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de besoin d'en connaître joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour personnels habilités sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de personnels habilités doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à prestataires. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à prestataires doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier prestataires à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être

proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour prestataires sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de prestataires doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à autorités compétentes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à autorités compétentes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier autorités compétentes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de encadrement contractuel joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des

obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour autorités compétentes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de autorités compétentes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 19 - TRANSFERTS INTERNATIONAUX ET GARANTIES APPROPRIÉES

TRANSFERTS INTERNATIONAUX ET GARANTIES APPROPRIÉES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à transferts transfrontaliers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à transferts transfrontaliers doit être pensée au regard de la protection des personnes concernées, de la

préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier transferts transfrontaliers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de évaluation du pays joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour transferts transfrontaliers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de transferts transfrontaliers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à garanties équivalentes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de

propriétaire exclusif de la plateforme, affirme que toute opération relative à garanties équivalentes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier garanties équivalentes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de clauses contractuelles joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour garanties équivalentes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de garanties équivalentes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à garanties équivalentes demeurent adéquates, lisibles et proportionnées. Une politique de

confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à autorisation préalable. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à autorisation préalable doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier autorisation préalable à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mesures compensatoires joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour autorisation préalable sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de autorisation préalable doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en

exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à transferts transfrontaliers. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à transferts transfrontaliers doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier transferts transfrontaliers à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de évaluation du pays joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour transferts transfrontaliers sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de transferts transfrontaliers doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits

de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à garanties équivalentes. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à garanties équivalentes doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier garanties équivalentes à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de clauses contractuelles joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour garanties équivalentes sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de garanties équivalentes doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à autorisation préalable. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à autorisation préalable doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier autorisation préalable à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mesures compensatoires joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour autorisation préalable sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de

remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de autorisation préalable doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 20 - DROITS DES PERSONNES CONCERNÉES ET CONDITIONS D'EXERCICE

DROITS DES PERSONNES CONCERNÉES ET CONDITIONS D'EXERCICE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à droit d'accès. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à droit d'accès doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier droit d'accès à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de limitation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour droit d'accès sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de droit d'accès doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à droit d'accès demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à rectification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à rectification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier rectification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de preuve d'identité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour rectification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de rectification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à opposition et suppression. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à opposition et suppression doit être pensée au regard de la protection des personnes concernées, de la

préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier opposition et suppression à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de délais de réponse joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour opposition et suppression sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de opposition et suppression doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à droit d'accès. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la

plateforme, affirme que toute opération relative à droit d'accès doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier droit d'accès à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de limitation joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour droit d'accès sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de droit d'accès doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à rectification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée

réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à rectification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier rectification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de preuve d'identité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour rectification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de rectification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à opposition et suppression. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits,

l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à opposition et suppression doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier opposition et suppression à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de délais de réponse joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour opposition et suppression sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de opposition et suppression doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il

appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à opposition et suppression demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 21 - GESTION DES INCIDENTS, VIOLATIONS ET CONTINUITÉ DE SERVICE

GESTION DES INCIDENTS, VIOLATIONS ET CONTINUITÉ DE SERVICE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à détection. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à détection doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier détection à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de notification joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour détection sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de détection doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à qualification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à qualification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier qualification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mesures correctives joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être

proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour qualification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de qualification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à réponse à incident. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à réponse à incident doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier réponse à incident à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de retour d'expérience joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation,

des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour réponse à incident sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de réponse à incident doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à détection. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à détection doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier détection à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de notification joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des

obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour détection sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de détection doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à qualification. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à qualification doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier qualification à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mesures correctives joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures

d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour qualification sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de qualification doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à qualification demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à réponse à incident. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à réponse à incident doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier réponse à incident à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité

identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de retour d'expérience joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour réponse à incident sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de réponse à incident doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

Article 22 - SOUS-TRAITANCE, ENGAGEMENTS CONTRACTUELS ET CONTRÔLE DES TIERS

SOUS-TRAITANCE, ENGAGEMENTS CONTRACTUELS ET CONTRÔLE DES TIERS est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à prestataires techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à prestataires techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier prestataires techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de audits joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour prestataires techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de prestataires techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à instructions documentées. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à instructions documentées doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier instructions documentées à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour instructions documentées sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de instructions documentées doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en

exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à obligations de sécurité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à obligations de sécurité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier obligations de sécurité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de réversibilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour obligations de sécurité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de obligations de sécurité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits

de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à prestataires techniques. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à prestataires techniques doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier prestataires techniques à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de audits joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour prestataires techniques sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de prestataires techniques doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à prestataires techniques demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à instructions documentées. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à instructions documentées doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier instructions documentées à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de confidentialité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour instructions documentées sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de instructions documentées doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à obligations de sécurité. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à obligations de sécurité doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier obligations de sécurité à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de réversibilité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour obligations de sécurité sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de obligations de sécurité doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 23 - GOUVERNANCE, RÔLES INTERNES ET PILOTAGE DE LA CONFORMITÉ

GOUVERNANCE, RÔLES INTERNES ET PILOTAGE DE LA CONFORMITÉ est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à pilotage interne. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à pilotage interne doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier pilotage interne à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages,

la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de revues périodiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour pilotage interne sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de pilotage interne doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à référent ou DPO. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à référent ou DPO doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier référent ou DPO à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de registre joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour référent ou DPO sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de référent ou DPO doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à reporting. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à reporting doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier reporting à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de culture de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour reporting sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de reporting doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à reporting demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à pilotage interne. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à pilotage interne doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier pilotage interne à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de revues périodiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour pilotage interne sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de pilotage interne doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à référent ou DPO. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à référent ou DPO doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier référent ou DPO à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de registre joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour référent ou DPO sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de référent ou DPO doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la

légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à reporting. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à reporting doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier reporting à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de culture de conformité joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour reporting sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de reporting doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix

répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 24 - AUDIT, CONTRÔLE, MISE À JOUR ET AMÉLIORATION CONTINUE

AUDIT, CONTRÔLE, MISE À JOUR ET AMÉLIORATION CONTINUE est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à audit interne. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à audit interne doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier audit interne à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de évolutions technologiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour audit interne sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de audit interne doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à audit externe. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à audit externe doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier audit externe à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mise à jour réglementaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour audit externe sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de audit externe doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à audit externe demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à révision documentaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à révision documentaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier révision documentaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées.

L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité des versions joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour révision documentaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de révision documentaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à audit interne. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à audit interne doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier audit interne à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des

habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de évolutions technologiques joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour audit interne sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de audit interne doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à audit externe. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à audit externe doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier audit externe à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni

consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de mise à jour réglementaire joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour audit externe sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de audit externe doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à révision documentaire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à révision documentaire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier révision documentaire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des

procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de traçabilité des versions joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour révision documentaire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de révision documentaire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

ARTICLE 25 - ENGAGEMENT INSTITUTIONNEL, ACCEPTATION ET DISPOSITIONS FINALES

ENGAGEMENT INSTITUTIONNEL, ACCEPTATION ET DISPOSITIONS FINALES est traité ci-après avec un niveau de détail destiné à encadrer aussi bien les

obligations de l'institution que les attentes légitimes des utilisateurs, partenaires et autorités de contrôle.

Le présent article organise en profondeur la matière relative à engagement de confiance. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à engagement de confiance doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier engagement de confiance à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de document opposable joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour engagement de confiance sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de engagement de confiance doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en

exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à engagement de confiance demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Le présent article organise en profondeur la matière relative à acceptation par l'usager. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à acceptation par l'usager doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier acceptation par l'usager à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prééminence institutionnelle joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour acceptation par

l'usager sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de acceptation par l'usager doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à force obligatoire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à force obligatoire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier force obligatoire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de signature joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ;

il faut encore que l'ARTCI puisse prouver que les modalités retenues pour force obligatoire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de force obligatoire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à engagement de confiance. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à engagement de confiance doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier engagement de confiance à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de document opposable joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour engagement de confiance sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de engagement de confiance doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à acceptation par l'usager. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à acceptation par l'usager doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier acceptation par l'usager à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de prééminence institutionnelle joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir compte de la sensibilité des informations traitées

et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour acceptation par l'usager sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de acceptation par l'usager doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Le présent article organise en profondeur la matière relative à force obligatoire. Dans l'économie générale de la présente politique, cette question ne doit pas être abordée comme une simple formalité documentaire mais comme une condition de validité, de sécurité et de crédibilité du dispositif CERTINUM. La plateforme opère dans un environnement où les informations confiées peuvent conditionner l'accès à des droits, l'analyse de conformité, la production de pièces, la vérification de déclarations ou la gestion de démarches à portée réglementaire. Pour cette raison, l'ARTCI, en sa qualité de propriétaire exclusif de la plateforme, affirme que toute opération relative à force obligatoire doit être pensée au regard de la protection des personnes concernées, de la préservation des preuves, de la continuité du service et du respect du cadre juridique applicable.

L'approche retenue par l'ARTCI consiste à lier force obligatoire à une chaîne complète de garanties. Cette chaîne comprend l'information des utilisateurs, la limitation des usages, la traçabilité des accès, l'encadrement des intervenants, la formalisation des procédures et la capacité de démontrer, à tout moment, que le traitement réalisé répond à une finalité identifiée et légitime. En pratique, cela signifie que les données ne sont ni manipulées ni consultées de manière diffuse. Elles le sont dans des conditions maîtrisées, selon des habilitations définies, avec des contrôles adaptés et des responsabilités attribuées. L'objectif est double : éviter l'arbitraire d'une part, et produire un niveau de confiance élevé d'autre part.

En outre, la notion de signature joue ici un rôle central. Elle rappelle que la conformité ne se limite pas à énoncer des principes généraux ; elle exige aussi des mécanismes concrets, observables et audités. Ainsi, l'ARTCI peut fixer des procédures d'enrôlement, des règles d'authentification, des modalités de revue des dossiers, des obligations de confidentialité, des paramètres de journalisation, des délais de conservation, des restrictions d'export et des contrôles de suppression. Chaque mesure doit être proportionnée aux risques identifiés, tenir

compte de la sensibilité des informations traitées et rester compatible avec les missions assignées à CERTINUM. Cette approche favorise une gouvernance sobre, structurée et défendable.

Le présent article doit également être lu à la lumière du principe de responsabilité démontrable. Autrement dit, il ne suffit pas que la plateforme poursuive une finalité utile ; il faut encore que l'ARTCI puisse prouver que les modalités retenues pour force obligatoire sont pertinentes, documentées et effectivement appliquées. Cette démonstration peut résulter de chartes internes, de contrats de sous-traitance, de matrices d'habilitation, de comptes rendus de revue d'accès, de rapports d'audit, de journaux système, de plans de remédiation, de procès-verbaux de validation ou de décisions de gouvernance. Plus le traitement est sensible, plus la charge de justification doit être rigoureuse.

Enfin, le traitement de force obligatoire doit rester intelligible pour l'utilisateur. La densité technique ou juridique du dispositif ne doit jamais conduire à masquer les droits de la personne, les responsabilités de l'institution ou les voies de recours disponibles. C'est pourquoi la présente politique privilégie une rédaction approfondie mais explicite, en exposant le raisonnement, les étapes, les garde-fous et les conséquences pratiques. Ce choix répond à une exigence simple : faire de CERTINUM une plateforme de confiance dont la légitimité ne repose pas seulement sur l'autorité de son propriétaire exclusif, mais aussi sur la qualité des garanties effectivement offertes.

Dans une logique de maîtrise du risque, le présent article implique enfin une démarche de réévaluation périodique. Les usages évoluent, les menaces se transforment, les attentes des utilisateurs se précisent et les obligations réglementaires peuvent se renforcer. Il appartient donc à l'ARTCI d'examiner régulièrement si les mesures associées à force obligatoire demeurent adéquates, lisibles et proportionnées. Une politique de confidentialité crédible n'est pas un texte figé : c'est un instrument vivant de pilotage, de redevabilité et de confiance publique.

Pour l'application opérationnelle du présent article, l'ARTCI peut édicter des procédures complémentaires, des formulaires, des notes d'instruction, des circuits de validation ou des clauses techniques permettant d'assurer la mise en oeuvre fidèle des principes ci-dessus. Ces supports d'exécution ne diminuent en rien la portée normative du présent document ; ils en assurent au contraire la traduction concrète dans les opérations courantes de CERTINUM.

PAGE DE VALIDATION ET DE SIGNATURE

La présente Politique de Confidentialité de la plateforme CERTINUM est arrêtée comme cadre officiel de référence pour l'ensemble des traitements de données à caractère personnel réalisés dans le cadre de exploitation de la plateforme CERTINUM. Elle entre en vigueur à compter de sa date d'approbation et demeure applicable jusqu'à l'adoption d'une version révisée expressément validée par **l'ARTCI.**

Les versions successives du document sont conservées afin d'assurer la traçabilité des évolutions, la démonstration de conformité et la preuve de la doctrine applicable à une date donnée. Toute diffusion externe doit correspondre à la version formellement validée.