Note : Les textes modifiés sont identifiés par un trait vertical dans la marge de gauche. Dans la présente, le genre masculin est utilisé dans le seul but d'alléger le texte.

A. Contexte

La Financière agricole du Québec (la « **FADQ** ») est soucieuse de protéger les renseignements personnels et confidentiels qu'elle détient. C'est pourquoi elle met en œuvre les moyens technologiques et administratifs nécessaires afin que ceux-ci soient traités de façon sécuritaire tout au long de leur cycle de vie.

Afin de s'acquitter de ses obligations législatives en matière de protection des renseignements personnels et confidentiels, la FADQ se dote d'une Directive sur la destruction et l'anonymisation des renseignements personnels ou confidentiels (la « **directive** »).

La directive découle de la Politique-cadre en matière d'accès aux documents et de protection des renseignements personnels (la « **politique-cadre** ») et elle doit se lire en concordance avec celle-ci, notamment en ce qui concerne les définitions.

La Directive doit être respectée en complément à la Politique de cybersécurité et à la Politique-cadre en matière d'accès aux documents et de protection des renseignements personnels de la FADQ. Toute violation sera traitée conformément aux procédures contractuelles et disciplinaires en vigueur.

B. Objet de la directive

La directive vise à présenter les exigences de sécurité et de conformité concernant la destruction et l'anonymisation de renseignements personnels ou confidentiels détenus par la FADQ, et ce, indépendamment de leur support d'information (un support papier ou numérique).

Elle a pour finalité de préserver, lors de la destruction ou de l'anonymisation, la confidentialité ainsi que la sécurité des renseignements personnels ou confidentiels détenus par la FADQ, et ce, tout en assurant le respect des autorisations requises du délai au Calendrier de conservation des documents de la FADQ et, le cas échéant, du Code des professions.

C. Champ d'application

La directive s'applique aux membres du personnel de la FADQ ainsi qu'à toute personne, entreprise ou tout ministère et organisme qui collectent, utilisent, communiquent, conservent, détruisent, ou anonymisent des documents renfermant des renseignements personnels détenus par la FADQ ou en son nom.

Elle couvre tous les aspects liés à la destruction et l'anonymisation des données, incluant :

- destruction des supports d'information ;
- anonymisation des données ;
- gestion des supports ;
- formation et sensibilisation ;
- conformité et surveillance.

D. Cadre légal, réglementaire et normatif

Cette Directive supporte le cadre légal de la Politique-cadre en matière d'accès aux documents et de protection des renseignements personnels.

Elle tient également compte de :

- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) (la « **Loi sur l'accès** ») ;
- la Loi sur les archives (RLRQ, c. A-21.1) ;
- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ. chapitre G- 1.03) ;

- le Code des professions (RLRQ, c. C-26) ;
- le Règlement sur l'anonymisation des renseignements personnels (Décret 783-2024) ;
- le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ, c. A-21.1, r. 2) (le « **Règlement** ») ;
- la Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur support informatique amovible (2003) (la « **directive du Conseil du trésor** »).

E. Principes généraux

Les principes directeurs de la Politique de cybersécurité demeurent applicables. Ces principes directeurs doivent guider l'application de la directive, en veillant à ce que les pratiques de destruction et d'anonymisation respectent également les exigences légales définies dans la Politique-cadre en matière d'accès aux documents et de protection des renseignements personnels.

Lorsque les fins pour lesquelles un renseignement personnel ou confidentiel a été recueilli ou utilisé sont accomplies, la FADQ doit le détruire, ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la Loi sur les archives et, le cas échéant, du Code des professions. Cette obligation s'applique, peu importe le type de support (papier ou numérique) tant aux documents originaux qu'à toutes les copies de ceux-ci.

F. Définitions

Les définitions applicables à l'interprétation de la directive qui en découlent sont prévues à l'annexe 1 de la présente.

G. Rôles et responsabilités

Cette section vise à préciser les rôles et responsabilités spécifiques au champ d'application de la directive.

Responsable de l'accès aux documents et de la protection des renseignements personnels (« RPRP »)

- soutient les personnes visées par l'application de la directive, notamment quant à son interprétation et son administration ;
- veille à la sensibilisation et la formation de toutes les personnes visées par la directive.

Chef de la sécurité de l'information organisationnelle

- soutient les personnes visées par l'application de la directive quant à son interprétation et son administration en ce qui concerne toute question relative à la sécurité de l'information ou toute situation impliquant des mesures de sécurité visant à préserver les actifs informationnels de la FADQ ;
- veille à ce que la FADQ utilise des mesures et des techniques généralement reconnues comme étant les meilleures pratiques en vue de procéder à l'anonymisation de renseignements personnels et confidentiels.

Personne compétente de la Direction des infrastructures, des plateformes technologiques et de sécurité (la « DIPTS »)

- supervise le processus d'anonymisation ;
- veille à ce que la FADQ utilise des techniques généralement reconnues comme étant les meilleures pratiques en vue de procéder à l'anonymisation de renseignements personnels.

Responsable de la gestion intégrée documentaire

- soutient les personnes visées par l'application de la Directive quant à son interprétation et son administration en ce qui concerne toute question relative à la gestion documentaire ou toute situation impliquant notamment le calendrier de conservation applicable à la FADQ.

Gestionnaire

- assure l'application de la Directive dans son unité ;
- désigne un responsable de la conservation et de la destruction des renseignements dans son unité afin notamment d'assurer le respect du calendrier de conservation de la FADQ.

Membre du personnel de la FADQ

- doit prendre toutes les mesures de sécurité requises pour assurer la confidentialité et la protection des renseignements personnels et confidentiels, et ce, durant tout leur cycle de vie.

H. Modalités

Les modalités applicables en matière de destruction et d'anonymisation de la directive sont prévues à l'annexe 2 de la présente.

De plus, les références aux méthodes de destruction adaptées au support et au niveau de confidentialité des documents afin d'en assurer la destruction définitive des renseignements personnels et confidentiels qu'ils contiennent sont indiquées à l'annexe 3 de la présente.

I. Révision de la directive

La directive fera l'objet d'une révision tous les cinq ans par le RPRP, en collaboration avec la DIPTS, sauf s'il est nécessaire de le faire avant.

J. Diffusion de la directive

Le RPRP, en collaboration avec la DIPTS, est responsable de la diffusion et de l'application de la directive au sein de la FADQ.

K. Approbation et entrée en vigueur

Cette directive a été approuvée par le président-directeur général et prend effet à la même date.

Annexe 1 — Définitions applicables

La présente annexe comprend les définitions applicables à la Directive sur la destruction et l'anonymisation le terme « renseignement personnel » peut également s'appliquer à un renseignement confidentiel.

Anonymisation : L'anonymisation est une solution de rechange à la destruction des renseignements personnels lorsque les fins auxquelles ils ont été recueillis ou utilisés sont accomplies, à condition que ces renseignements anonymisés soient utilisés à des fins sérieuses et légitimes. Il s'agit d'une opération irréversible dans le but que la personne concernée ne soit pas ou plus identifiable. Il n'existe aucun moyen de rattacher les renseignements à la personne concernée lorsqu'elle est effective.

Calendrier de conservation : Au sens de la Loi sur les archives, tout organisme public doit établir un calendrier de conservation qui détermine les périodes d'utilisation et les supports de conservation des documents actifs et semi-actifs et indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés.

Conservation : La conservation représente la période durant laquelle la FADQ conserve les renseignements personnels et confidentiels, sous quelque forme que ce soit et peu importe que le document soit actif, semi-actif ou inactif tel que défini en vertu de la Loi sur les archives.

Critère de corrélation : Le fait de ne pas être en mesure de relier entre eux des ensembles de données qui concernent une même personne.

Critère d'individualisation : Le fait de ne pas être en mesure d'isoler ou de distinguer une personne dans un ensemble de données.

Critère d'inférence : Le fait de ne pas être en mesure de déduire des renseignements personnels à partir d'autres renseignements disponibles.

Cycle de vie d'un renseignement personnel : Ensemble des étapes de traitement des renseignements personnels. Les étapes du cycle de vie d'un renseignement personnel sont : sa collecte, son utilisation, sa communication, sa conservation et sa destruction ou son anonymisation.

Cycle de vie de l'information : Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction.

Destruction : Correspond à la fin du cycle de vie du renseignement personnel. Ainsi, la destruction du renseignement est définitive, irréversible et irrécupérable, et ce, qu'il soit sur un support papier ou numérique.

Document : Désigne un ensemble de renseignements constituant une unité distincte et détenant une valeur d'information, quel qu'en soit le support ou le mode de transmission.

Document technologique : Document produit, transmis, reçu ou conservé par des moyens technologiques.

Information : Tout renseignement détenu par un organisme public.

Moyen technologique : Tout procédé technique, tout moyen ou tout système permettant de produire, de communiquer, de recevoir, de conserver ou de traiter de l'information.

Renseignement anonymisé : Un renseignement est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement une personne concernée.

Le terme « irréversible » implique qu'il ne doit pas être possible, au moment de l'anonymisation et en tout temps, et ce, en considérant un futur prévisible, d'identifier de nouveau la personne concernée directement ou indirectement.

Support : Élément matériel ou virtuel permettant de consigner, de conserver et de consulter l'information.

Annexe 2 — Modalités applicables

La présente annexe comprend les modalités applicables en matière de destruction et d'anonymisation de la directive sur la destruction et l'anonymisation des renseignements personnels et confidentiels.

Destruction

Les règles suivantes doivent être respectées pour assurer une destruction sécurisée des supports et des documents :

1. **Niveau de confidentialité** : La destruction des documents et des supports doit être guidée par le niveau de confidentialité des informations qu'ils contiennent. Cette destruction doit être exécutée avec la technique appropriée, comme indiqué dans les règles ci-dessous.

2. **Conformité** : La FADQ doit éliminer, détruire, effacer ou anonymiser en toute sécurité les informations sensibles, telles que les renseignements personnels, quelle que soit la méthode de stockage, conformément aux lois applicables concernant les calendriers de conservation des dossiers et de manière à prévenir la perte, le vol, une mauvaise utilisation ou un accès non autorisé, et utilise des techniques ou des méthodes pour garantir la suppression ou la destruction sécurisée des informations personnelles (y compris les originaux, les copies et les enregistrements archivés).

3. **Méthodes et moyens** :

Traitement des supports électroniques

L'effacement des supports de stockage, incluant les disques durs (HDD), les disques SSD, les clés USB, et autres supports amovibles, doit être réalisé à l'aide d'un outil certifié ou d'une méthode répondant aux standards de l'industrie, tel que le DoD 5220.22-M. Cet outil doit être capable d'effectuer un effacement complet, irréversible et sécurisé, garantissant qu'aucune donnée ne puisse être récupérée par des moyens conventionnels ou avancés.

Les processus d'effacement doivent respecter les normes suivantes et reconnues :

- **DoD 5220.22-M** : Cette méthode prescrit un effacement sécurisé en plusieurs passes, incluant l'écriture de données aléatoires et une vérification finale pour garantir la destruction complète des informations.
- **NIST SP 800-88** : Ce standard recommande des techniques spécifiques adaptées aux types de supports, telles que :
    - l'effacement logique sécurisé (**Nettoyer**) pour rendre les données irrécupérables par des moyens standards ;
    - la démagnétisation ou l'effacement à niveau élevé (**Purger**) pour rendre les données irrécupérables même avec des outils spécialisés ;
    - la destruction physique (**Détruire**) lorsque la réutilisation du support n'est pas souhaitée.

Les gestionnaires et détenteurs de l'information doivent s'assurer que des rapports de conformité détaillés sont générés et conservés, attestant que les supports de stockage ont été traités conformément à cette directive. Ces rapports seront utilisés pour démontrer la conformité lors des audits internes et externes.

Traitement des supports papier, CD et autres supports non électroniques

Pour les supports non électroniques tels que les documents papier, les CD, DVD, disquettes et autres médias physiques, des méthodes de destruction appropriées doivent être utilisées pour garantir la protection des informations confidentielles.

Cela inclut :

- **supports papier** : Les documents doivent être déchiquetés à l'aide d'une déchiqueteuse à coupe croisée ou micro-coupe pour garantir que les informations ne puissent pas être reconstituées ou déposés dans des contenants sécurisés barrés dont la destruction est certifiée ;
- **CD, DVD, disquettes** : Ces supports doivent être physiquement détruits à l'aide d'un broyeur spécialisé pour supports optiques ou cassés de manière irréversible, afin de rendre toute récupération impossible ou déposés dans des contenants sécurisés barrés dont la destruction est certifiée.

Dans tous les cas, la méthode de destruction doit correspondre à la sensibilité des informations contenues et garantir la conformité avec les standards de sécurité en vigueur. Un certificat de destruction doit être généré pour chaque opération de destruction de supports non électroniques afin d'attester de la conformité lors des audits.

4. **Contrôle des supports :** Le contrôle et l'accès aux supports influencent la décision de procéder à la destruction. Cette considération est cruciale lorsque les supports quittent le contrôle organisationnel. Exemples de contrôle :

   - **sous contrôle de la FADQ :** Les supports remis pour entretien sont considérés comme étant sous contrôle de l'organisation si des accords contractuels garantissant la confidentialité des informations sont en place ;
   - **hors contrôle de la FADQ :**Les supports échangés pour garantie, rabais ou autres fins sans retour spécifique à l'organisation sont considérés comme étant hors du contrôle organisationnel.

5. **Rédaction et application des procédures de destruction**

   Les procédures élaborées devront respecter la présente directive. Elles devront être documentées et approuvées par le niveau de gestion approprié. Consulter l'intranet de la FADQ pour les directives et les procédures.

6. **Transport et entreposage**

   Tous les documents, présent sur l'un ou l'autre des types de support, contenant des renseignements personnels et confidentiels doivent être transportés de manière sécuritaire et être conservés à tout moment dans un endroit à accès contrôlé et sécurisé, et ce, jusqu'à ce que le processus de destruction soit terminé.

<u>Anonymisation</u>

Les règles suivantes doivent être respectées pour assurer l'anonymisation des renseignements personnels et confidentiels comme le prévoit le règlement.

1. **Conformité au Règlement sur l'anonymisation des renseignements personnels**

   Tous les employés impliqués dans la gestion de renseignements personnels et confidentiels doivent se conformer aux exigences du processus d'anonymisation décrites dans la présente directive. Tout processus d'anonymisation doit être réalisé sous la supervision d'une personne compétente en la matière.

2. **Rédaction et application d'une méthodologie d'anonymisation**

   La FADQ, par l'intermédiaire d'une ressource compétente, doit rédiger, documenter et maintenir une méthodologie détaillée pour l'anonymisation des renseignements personnels et confidentiels. Cette méthodologie doit inclure les étapes suivantes :

   1. identification et suppression de tous les renseignements d'identification directs ;
   2. analyse préliminaire des risques de réidentification en considérant notamment les critères suivants :
      1. le critère d'individualisation ;
      2. le critère de corrélation ;
      3. le critère d'inférence ;
      4. les renseignements disponibles dans l'espace public.
   3. identification des techniques d'anonymisation appropriées, conformément aux meilleures pratiques généralement reconnues ;
   4. mise en œuvre de mesures de sécurité afin de diminuer les risques de réidentification ;

5. analyse du risque de réidentification.

L'analyse doit démontrer qu'il est, en tout temps, raisonnable de prévoir que les renseignements anonymisés ne permettent plus, de façon irréversible, d'identifier directement ou indirectement une personne.

3. Documentation et transparence

Tous les renseignements concernant le processus d'anonymisation doivent être consignés dans un registre incluant, mais sans s'y limiter :

1. une description des renseignements personnels anonymisés ;
2. les fins pour lesquelles les renseignements anonymisés seront utilisés ;
3. les techniques d'anonymisation appliquées et les mesures de protection et de sécurité mises en place ;
4. les dates des analyses de risques de réidentification effectuées et mises à jour.

Ce registre doit être accessible aux autorités compétentes et être maintenu à jour pour assurer la transparence et la conformité continue.

4. Revue et mise à jour périodique

Une évaluation périodique des renseignements anonymisés doit être réalisée pour s'assurer qu'ils demeurent anonymisés, la fréquence est déterminée selon l'évaluation du risque initiale.

5. Vigie

Les avancées technologiques et les nouvelles sources de données doivent être considérées lors de chaque réévaluation pour mettre à jour les techniques d'anonymisation et les mesures de protection.

6. Formation et sensibilisation

Tous les employés impliqués dans la gestion de renseignements personnels et confidentiels, plus particulièrement dans le traitement et l'anonymisation de tels renseignements, doivent recevoir une formation adéquate sur les meilleures pratiques d'anonymisation et les exigences réglementaires.

Annexe 3 — Méthodes de destruction

NIST 800-53 rev 5 National Institute of Standards and Technology (NIST). (2020) Security and Privacy Controls for Informations Systems and Organisations (NIST Special Publication 800-53, Revision 5). Gaiothersburg, MD : National Institute Standards and Technology.
doi :10.6028/NIST.SP.800-53r5.

NIST 800-88
National Institute of Standards and Technology (NIST). (2014) Guidelines for Media Sanitization (NIST Special Publication 800-88, Revision 1). Gaiothersburg, MD : National Institute Standards and Technology.
doi :10.6028/NIST.SP.800-88r1.

DoD 5220.22-M
U.S. Department of Defense. (1997) National Industrial Security Operating Manual (NISPOM) (DoD 5220.22-M). Washington, D.C, : Department of Defense

Safe Harbor du Health Insurance Portability and Accountability Act (HIPAA)
U.S Department of Health & Human Services (HHS). (2013) Standards for Privacy of Individually Identifiable Health Informationn(45 CFR 164.514(b)). Washington, D.C. : US Department of Health and Human Services.

Note : La méthode de destruction doit être adaptée au type de support et au niveau de confidentialité des documents et assurer la destruction définitive des renseignements personnels qu'ils contiennent.