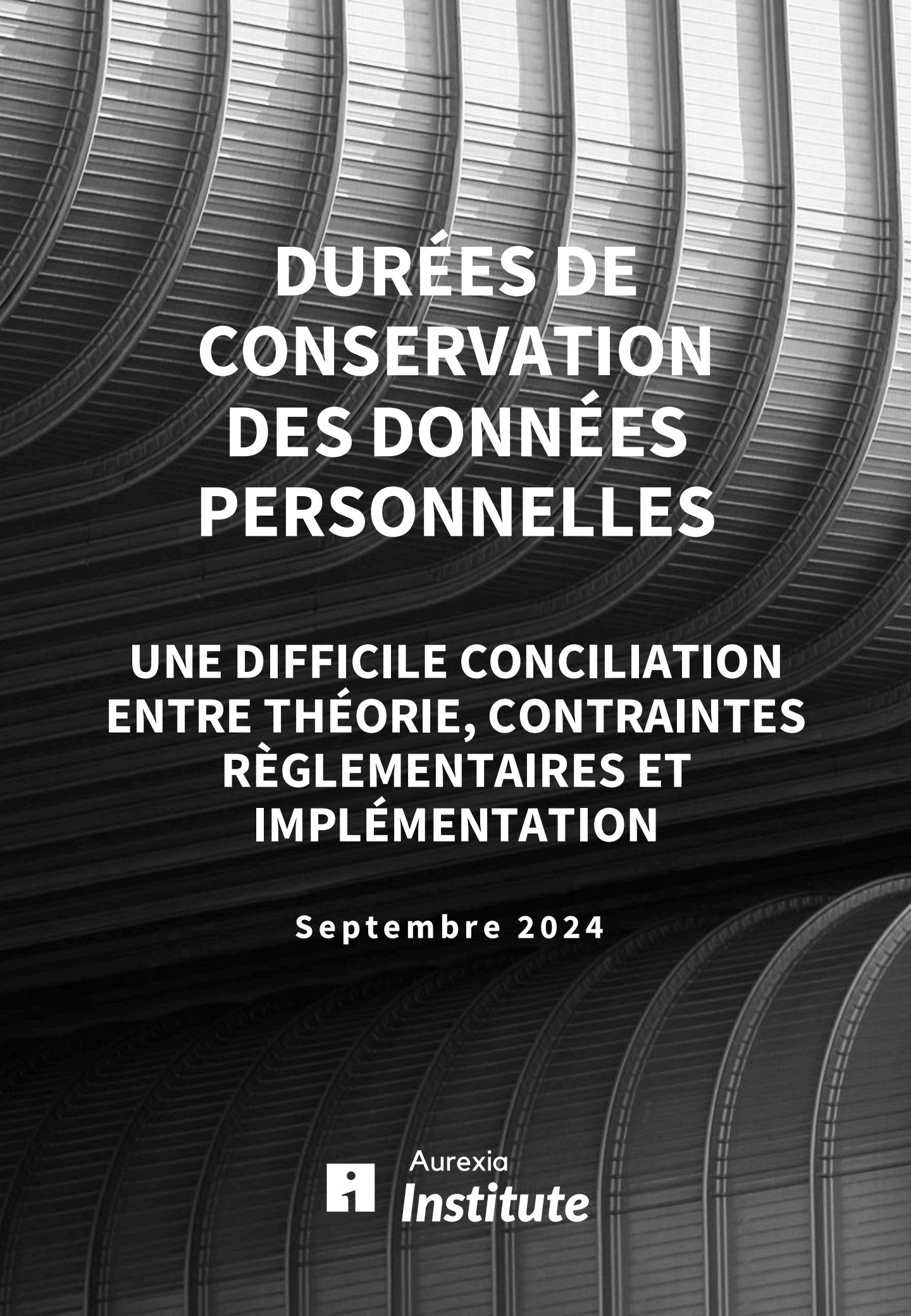

DURÉES DE CONSERVATION DES DONNÉES PERSONNELLES

UNE DIFFICILE CONCILIATION ENTRE THÉORIE, CONTRAINTES RÈGLEMENTAIRES ET IMPLÉMENTATION

Septembre 2024

Aurexia Institute

Les durées de conservation des données personnelles : une difficile conciliation entre théorie, contraintes règlementaires et implémentation

Entre la rigueur imposée par le RGPD et les réalités opérationnelles, les établissements financiers et/ou assurantiels se retrouvent à devoir concilier impératifs de conformité et contraintes pratiques en matière de gestion des durées de conservation des données personnelles.

En effet, le RGPD consacre un principe fondamental : la limitation de la conservation des données. Ce texte précise que la durée doit être strictement nécessaire par rapport à l'objectif initial de la collecte de la donnée personnelle.

Tel est donc le défi pour les entreprises : identifier les données qu'elles collectent concernant leurs employés, clients ou autres personnes concernées, déterminer leurs durées de conservation, puis implémenter techniquement les règles définies.

Le non-respect de ces obligations engendre un **fort risque opérationnel** car le RGPD prévoit des amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de la société, le montant le plus élevé étant appliqué.

Définition des périodes de conservation des données personnelles : qui porte cette responsabilité ?

La décision incombe au responsable du traitement, c'est-à-dire l'entité qui fixe les **finalités et les moyens du traitement**. Ce choix doit à la fois respecter les obligations légales, répondre aux besoins opérationnels et protéger les droits des individus.

Les durées doivent être identifiées avec précaution car le RGPD n'indique pas explicitement une durée qui doit être respectée. Cette réalité laisse une marge d'appréciation très (trop ?) importante au responsable de traitement, lui donnant ainsi une flexibilité d'adapter les périodes de conservation en fonction des spécificités de chaque traitement et de sa stratégie. Avec pour corollaire les risques afférents et évoqués plus haut en cas de « mauvais choix » (exemple : durée considérée comme trop importante par l'autorité de contrôle).

Quels facteurs doivent guider le responsable de traitement dans l'établissement des durées de conservation des données ?

Pour définir les durées de conservation des données personnelles, le responsable de traitement doit se baser sur plusieurs éléments, en complément de la finalité initiale du traitement des données en question. Il peut ainsi être nécessaire de prendre en compte les obligations légales et règlementaires **génériques** (conservation des documents comptables et des pièces justificatives pendant 10 ans selon les dispositions du code de commerce, durée de prescription civile etc.) ou **spécifiques** à chaque secteur d'activité et susceptibles de contrôles par les régulateurs compétents (AMF, BCE ou autres), comme les données KYC et celles relatives au blanchiment d'argent. Il peut être aussi crucial de prendre en considération aussi les durées légales locales applicables à chaque entité juridique et qui peuvent différer selon les territoires (au moins 5 ans pour les données KYC en France qui peut être prolongée sur demande du régulateur). Dans ces cas-là, il faut faire en sorte de concilier la période de stockage des données avec la demande du régulateur pour être en mesure de répondre à cette requête et/ou se baser sur des règles établies par le Groupe qui aura analysé le risque éventuel.

En outre, il est indispensable d'examiner les recommandations et délibérations de la Commission nationale de l'informatique et des libertés (CNIL) notamment en cas d'absence de texte règlementaire. La CNIL a publié sa doctrine en matière de prospection commerciale, de gestion des alertes professionnelles, etc. Selon ces règles, les données des clients utilisées à des fins de prospection peuvent être conservées jusqu'à trois ans après la fin de la relation commerciale. Pour les prospects non-clients, les données personnelles peuvent également être conservées jusqu'à trois ans après leur collecte ou le dernier contact établi par le prospect, comme une demande de documentation. Enfin, en cas d'absence de tout texte imposant une durée précise ou une délibération, l'entité financière, bancaire ou assurantielle, agissant en tant que responsable de traitement, doit vérifier les besoins des métiers à garder les données et définir une règle qui ne nuit pas au bon fonctionnement des opérations et consulter ses équipes juridiques et le Data Protection Officer pour avis.

La documentation des périodes de conservation des données

La CNIL vérifie effectivement la **documentation** des périodes de conservation des données lors de ses contrôles, qui est un aspect essentiel de la conformité au RGPD.

Voici ce qu'il faut retenir :

Le RoPA

Le fichier ou logiciel où figurent les durées de conservation des données est le RoPA (Register of Processing Activities) ou le registre des activités de traitement de données personnelles.

La politique de conservation des données

Les durées doivent aussi être regroupées dans un document spécifique, souvent appelé "politique de conservation des données". Ce document doit préciser principalement : les catégories de données concernées, les durées de conservation en base active, les éventuelles durées d'archivage et les justifications de ces durées (obligations légales, besoins opérationnels, etc.). Cette politique a vocation à être diffusée aux personnes concernées, en vue de respecter l'obligation d'information du responsable de traitement à leur égard. Cela passe souvent par la « Data Protection Notice » ou « Politique Vie privée » présente sur le site Internet de l'entreprise.

Les guides de la CNIL

La CNIL a élaboré des outils pour aider les responsables de traitement, notamment : un **Guide pratique sur les durées de conservation**, des **référentiels sectoriels** ou **thématiques** proposant des durées recommandées pour certains traitements courants tels que les traitements RH. La CNIL se positionne également sur les aspects de sécurité et de stockage des données et vérifie systématiquement, lors de ses contrôles, l'existence de cette documentation, la pertinence des durées définies par rapport aux finalités du traitement et leur intégration conforme et concrète dans les systèmes d'information.

Attention : même après avoir défini les périodes de conservation des données et accompli ces démarches de documentation, le processus de conformité du responsable de traitement doit être pérennisé via des audits réguliers en interne (LOD1, LOD2 et LOD3) pour corriger des éventuels écarts constatés et éviter une sanction financière et publique.

La mise en pratique des durées de conservation définies : un enjeu majeur pour les entreprises

Un point indispensable lors d'un contrôle se manifeste par la mise en œuvre effective de ces durées. L'absence de documentation ou le non-respect des périodes définies peuvent entraîner des sanctions, dont des amendes administratives.

Des exemples de sanctions rendues publiques :

- En novembre 2020, la CNIL a infligé des sanctions à **Carrefour Banque (800 000 euros)** et **Carrefour France (2,25 millions d'euros)** en raison d'une durée supérieure à celle recommandée par la CNIL, et sans justification (conservation pendant quatre ans au lieu de trois ans).

  - La CNIL a aussi estimé qu'un client n'ayant pas effectué d'achat depuis plusieurs années ne devait plus être considéré comme tel, qualifiant ainsi cette durée de conservation d'excessive.

  - La CNIL a constaté que le programme d'effacement des données de Carrefour était insuffisant, laissant subsister des informations sur des centaines de milliers de clients dont les achats dataient de plus de cinq ans.

- En mars 2024, l'autorité de protection des données finlandaise a imposé une amende de 856 000 euros à un détaillant en ligne pour violation du principe de limitation des données :

  - Dans cette affaire, il a été jugé que Verkkokauppa.com a enfreint le RGPD en ne définissant pas une période de conservation appropriée pour les données personnelles des clients. Le site demandait aux clients de créer un compte afin de réaliser un achat, ce qui signifiait que les données étaient conservées pendant une période indéfinie jusqu'à ce que le client les supprime.

Pour limiter tout risque opérationnel, il est donc indispensable de réussir à concilier théorie et pratique. Cela nécessite la collaboration étroite entre les équipes Data Office, Risk, Legal, business et IT afin de mettre en œuvre des solutions adaptées telles que l'archivage intermédiaire à l'issue de la conservation en base active, la suppression ou l'anonymisation effective des données. Organiser des ateliers de travail avec les différentes parties prenantes permet d'insuffler des réflexes sur ces sujets au sein des équipes et de s'assurer que les politiques de conservation des données définies seront effectivement appliquées au sein de l'entreprise.

Comment Aurexia vous accompagne ?

Pour rester conforme aux exigences du RGPD, Aurexia, fort de ses **experts et de ses consultants en services financiers** et de son **activité de veille** autour des sujets de protection des données, accompagne au quotidien et concrètement les banques et les établissements financiers dans leurs projets de Data Retention.

Exemples de missions :

- revue et mise à jour des RoPAs en définissant les durées de conservation de données adéquates, en coordination avec le métier, le DPO et le Legal
- adaptation des procédures et des politiques internes et externes des durées de conservation
- création de référentiels de durées de conservation de données et implémentation des règles
- sensibilisation continue des équipes
- déploiement auprès des entités locales

Vos contacts

Frédéric ALCARAS
Partner Aurexia
Tel : + 33 (0) 6 47 58 27 39
frederic.alcaras@aurexia.com

Sarah VELTÉ
Manager Data Regulation
Tel : + 33 (0) 6 75 66 74 98
sarah.velte@aurexia.com

Léa FRANCIS
Consultante
lea.francis@aurexia.com

Aurexia

Bringing value, together