RGPD

# Gérer la durée de conservation des données, casse-tête des collectivités

Déterminer la durée de conservation des données personnelles est un élément central du RGPD, tant pour le respect des obligations légales du responsable de traitement que pour la protection de la vie privée des personnes. Pourtant, cette notion apparaît mal maîtrisée par les collectivités, du fait de sa complexité, des réticences et du manque d'accompagnement pratique de l'autorité de contrôle.

## 1 LA DURÉE DE CONSERVATION, ENJEU CENTRAL DE PROTECTION DE LA VIE PRIVÉE

La limitation des durées de conservation est prévue à l'article 5.1 e) du règlement général sur la protection des données («RGPD»). Celui-ci définit les grands principes des traitements de données à caractère personnel et précise que celles-ci seront conservées sous une forme permettant l'identification des personnes uniquement pour une durée n'excédant pas celle nécessaire au regard des finalités qui ont justifié sa collecte.

### Un cycle de vie des données et deux objectifs

En faisant le choix de lier la durée de conservation des données aux finalités poursuivies par le traitement, le législateur européen poursuit deux objectifs.

Le premier objectif est relatif à la protection de la vie privée des personnes dont les données sont collectées. Le législateur a voulu empêcher que les organismes ayant collecté des données personnelles gardent ces informations indéfiniment et constituent ainsi un patrimoine informationnel aux dépens des personnes qui ne disposeraient plus d'une maîtrise effective de leurs données.

Le deuxième objectif s'inscrit dans la continuité du premier mais sous un angle différent. En imposant une durée de conservation limitée, le législateur européen tente de réduire la gravité des risques subis en cas de violation de sécurité puisque ces données ne sont pas conservées plus que nécessaire.

### Utilisation courante, archivages intermédiaire et définitif : trois temps

Pour réaliser ces deux objectifs, tout en ayant conscience des besoins des administrations et des entreprises, la Cnil a organisé le cycle de vie des données à caractère personnel en trois temps :

– la phase d'utilisation courante ou durée d'utilisation courante (DUC) ;

– l'archivage intermédiaire ou durée d'utilisation administrative (DUA) ;

– l'archivage définitif.

S'agissant de la phase d'utilisation courante, la Cnil indique que cela correspond au temps pendant lequel les données sont utiles aux différents services de la structure et doivent être conservées en base active (1). Durant cette période, l'accessibilité aux données est entendue comme relativement large, puisqu'il s'agit des données utilisées fréquemment par les services d'une collectivité.

S'agissant de la durée de l'archivage intermédiaire, la Cnil rappelle qu'il ne s'agit pas de conserver l'intégralité des données mais seulement celles qui sont indispensables ou requises par une obligation légale (2). Durant cette période, l'accessibilité aux données est entendue comme réduite avec des modalités d'accès spécifiques et un encadrement strict des personnes pouvant avoir accès aux données.

S'agissant de l'archivage définitif, la Cnil rappelle que certaines données et documents présentant un intérêt historique doivent effectivement pouvoir être conservés et archivés, dans les conditions fixées par le code du patrimoine (3).

Cette articulation en trois temps matérialise la réflexion que l'ensemble des collectivités doit adopter pour l'ensemble de ses traitements. La conservation des données à caractère personnel doit être pensée par rapport à ce schéma et cela impose que, dès l'origine, la collectivité sache, pour chacune des catégories de données qu'elle va collecter, les durées de conservation qu'elle va lui appliquer en fonction des finalités qu'elle aura déterminées.

### Le principe d'une durée par catégorie de données

Au-delà de cette articulation en trois temps, une des particularités bien souvent méconnue sur la durée de conservation est que celle-ci ne se pense pas sur l'activité de traitement en elle-même mais sur les catégories de données collectées.

Par exemple, pour une collectivité ayant une activité de traitement relative à la gestion des accès et horaires, et comme l'indiquait l'ancienne norme simplifiée n° 42, la Cnil indiquait comme durée de conservation :
– 5 ans après le départ de l'agent pour les données identifiantes ;
– 3 mois pour les éléments relatifs aux déplacements ;
– 5 ans pour les données permettant (si existant) le contrôle du temps de travail ;
– 5 ans pour les données relatives aux motifs d'absence (sauf dispositions législatives contraires) ;
– 3 mois pour les données monétiques des données relatives au paiement des repas (ou 5 ans en cas de paiement par retenue sur salaire).

### Le besoin d'outils informatiques automatisés

Cet exemple illustre bien la finesse de l'analyse que doivent déployer les collectivités responsables de traitement dans la gestion des données qui seront collectées. De plus, cela sous-entend bien que le triptyque « finalités/objectifs poursuivis, données collectées et durée de conservation pour chaque catégorie de donnée » doit être pensé dans son entièreté et ce, dès l'origine. Bien souvent, seule la partie relative à la détermination des finalités et du besoin en matière de données est abordée.
Ensuite, cela démontre l'importance d'avoir développé et d'utiliser des outils informatiques automatisés capables d'archiver ou d'effacer les données une fois que la durée indiquée dans l'outil aura été atteinte. On retrouve ici le concept des outils by design et by default promus par le RGPD (4).

## 2 LES COLLECTIVITÉS À LA PEINE POUR GÉRER LA DURÉE DE CONSERVATION

### Papier et numérique : différences de pratiques

Dans le cadre de marchés de mise en conformité ou au travers d'un accompagnement des délégués à la protection des données, l'on constate que les sujets autour de la conservation des données à caractère personnel sont souvent mal maîtrisés ou délaissés au profit d'une gestion par des services des données personnelles à l'occasion de laquelle ceux-ci archivent de manière extrêmement parcellaire ou sans réflexion globale au niveau de la collectivité. Il s'agit, bien souvent, d'un manque de sensibilisation autour des enjeux relatifs à la durée de conservation alors que ces services peuvent mettre en place leurs propres systèmes de gestion ad hoc de durée de conservation des données alors que d'autres peuvent stocker les documents sans avoir réellement mis en place de politique dédiée.
Au-delà, une différence de pratiques semble perdurer entre la gestion des documents papiers et des éléments numérisés. Bien souvent, l'on constate que les habitudes d'archivage ou de suppression des documents numérisés sont mieux ancrées que celles des documents papiers.

**Il n'est jamais aisé de déterminer une durée de conservation adaptée à la finalité du traitement et l'autorité de contrôle n'offre qu'un soutien très limité et théorique.**

### Déterminer la durée de conservation, exercice périlleux

Ensuite, une des principales difficultés pour les collectivités est de bien comprendre et bien déterminer les durées de conservation des données. Le RGPD a opéré une bascule entre les obligations antérieures de déclaration auprès de l'autorité de contrôle et la responsabilisation des utilisateurs de la donnée en leur imposant de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Ainsi responsabilisées, les collectivités territoriales ont eu l'obligation de construire leur conformité au règlement et par ce biais de déterminer les durées de conservation des données qu'elles collectaient toutes seules. Toutefois, il n'est jamais aisé de déterminer une durée de conservation adaptée à la finalité du traitement et, sur ce point, l'autorité de contrôle n'offre qu'un soutien très limité et uniquement théorique.

### Un manque de soutien de l'autorité de contrôle

A titre d'exemple, dans son guide RGPD à l'égard des collectivités, une fiche pratique n° 4 intitulée « comment concilier les durées de conversation et les archives ? » est bien présente et explique les différents stades du cycle de vie des données. Cependant, cet apport est toujours très abstrait et, en dehors des normes simplifiées aujourd'hui dépourvues de valeur juridique, rien ne vient aider les collectivités dans le choix d'une durée de conservation adaptée. Par exemple, une liste avec 45 activités de traitement les plus évidentes pour les collectivités a été publiée à l'issue ●●●

## RÉFÉRENCES


- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

du guide. Il aurait été possible de faire exactement la même chose pour les durées de conservation des données des activités de traitement présentées. Cela aurait permis aux collectivités de trouver un point d'équilibre entre la durée qu'ils estiment être nécessaire pour l'accomplissement de leurs missions et les souhaits de la Cnil en la matière puisque, comme on va le voir, ceux-ci peuvent largement diverger.

## Les enseignements des mises en demeure de deux grandes entreprises

Par deux délibérations en date du 20 janvier 2020 (5 et 6) , la Cnil a rendu publique deux mises en demeure prises à l'encontre des sociétés Engie (7) et EDF (8) le 31 décembre 2019 autour de deux thématiques centrales du RGPD : la manière dont le consentement a été recueilli et les durées de conservations pendant lesquelles les données ont été sauvegardées.

Au-delà du débat sur le recueil du consentement, la Cnil a constaté que les durées de conservation des données à caractère personnel étaient trop longues au regard des finalités pour lesquelles celles-ci avaient été traitées.

## EDF : du zèle dans la précision et la conservation des données

A l'encontre d'EDF, la Cnil a constaté que l'entreprise conservait en base active les consommations quotidiennes et à la demi-heure pour une durée de cinq ans après la résiliation du contrat alors qu'aucune procédure d'archivage n'était par ailleurs prévue.

A ce propos, la Cnil indique que « les données de consommation à la demi-heure ne sont pas nécessaires pour établir la facturation et n'ont dès lors pas à être conservées cinq ans après la résiliation du contrat. Ensuite, les fournisseurs d'électricité ne sont tenus de mettre à disposition des clients leur historique de consommation que pendant une durée de trois années suivant la date de recueil du consentement (art. D. 224-26 du code de la consommation) » (9).

## Engie : la prospection commerciale ne légitime pas tout

A l'encontre d'Engie, la Cnil a constaté que les données de consommation mensuelles de ses clients étaient conservées à l'issue de la résiliation de leur contrat pendant une durée de trois ans en base active, puis pendant une durée de huit ans en archivage intermédiaire (10). Or, selon elle, « si les coordonnées du client peuvent être conservées en base active pendant trois ans à l'issue de la résiliation du contrat pour que la société puisse effectuer de la prospection commerciale, les données de consommation mensuelles ne sont pas nécessaires pour cet objectif, de sorte que leur conservation ne saurait être justifiée par cette finalité. Par ailleurs, la conservation des données de consommation mensuelles à l'issue de la résiliation du contrat n'est pas non plus justifiée par la mise à disposition de ces données dans l'espace client de l'usager dans la mesure où cette mise à disposition n'est effective que pour une durée d'un an à l'issue de la résiliation du contrat » (11).

## La défi de définir une durée de conservation proportionnée

Ces deux décisions illustrent bien la difficulté de déterminer une durée de conservation cohérente qui satisfera la Commission. On peut légitimement penser que les équipes dédiées aux questions de données à caractère personnel au sein de ces deux entreprises sont particulièrement au fait de toutes les problématiques présentées.

Pourtant, cela n'a pas empêché la Cnil d'estimer qu'il y avait eu un manquement à l'obligation de définir une durée de conservation proportionnée à la finalité du traitement alors que les conséquences d'une conservation excessive sont une violation de l'article 5, paragraphe 1, e), du RGPD et peuvent donc entraîner la mise en jeu de la responsabilité de l'organisme avec des sanctions administratives extrêmement élevées.

**(1)** www.Cnil.fr/comment-concilier-les-durees-de-conservation-et-les-archives.

**(2)** Idem.

**(3)** Idem.

**(4)** Article 25 du RGPD.

**(5)** Délibération du bureau de la Cnil n° MEDP-2020-002 du 20 janvier 2020 décidant de rendre publique la mise en demeure n° MED 2019-036 du 31 décembre 2019 prise à l'encontre de la société Engie.

**(6)** Délibération du bureau de la Cnil n° MEDP-2020-001 du 20 janvier 2020 décidant de rendre publique la mise en demeure n° MED 2019-035 du 31 décembre 2019 prise à l'encontre de la société EDF.

**(7)** Décision n° MED 2019-036 du 31 décembre 2019 mettant en demeure la société Engie

**(8)** Décision n° MED 2019-035 du 31 décembre 2019 mettant en demeure la société EDF.

**(9)** www.Cnil.fr/edf-et-engie-mises-en-demeure-pour-non-respect-de-certaines-conditions-de-recueil-du-consentement.

**(10)** www.Cnil.fr/edf-et-engie-mises-en-demeure-pour-non-respect-de-certaines-conditions-de-recueil-du-consentement.

**(11)** www.Cnil.fr/en/node/119648

**Par David Conerardy et Aloïs Ramel,** avocats à la cour, SCP Seban et associés