CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE
DE MARTINIQUE

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'ASSISTANT TERRITORIAL QUALIFIE DE CONSERVATION DU PATRIMOINE ET DES BIBLITHEQUES PRINCIPAL DE 2ème CLASSE, SESSION 2022

Mardi 24 mai 2022

EPREUVE DE NOTE

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'une note à l'aide des éléments d'un dossier portant sur la spécialité choisie par le candidat au moment de l'inscription.
Durée : 3 heures Coefficient : 2

SPECIALITE : ARCHIVES

A LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

- ✓ Vous ne devez faire apparaître dans votre copie aucun signe distinctif tels que : paraphe, signature, initiales, numéro de convocation, votre nom ou nom fictif, nom de votre collectivité employeur, commune où vous résidez ou composez.
- ✓ Seul l'usage d'un stylo non effaçable à encre noire ou bleue est autorisé (bille ou feutre). L'utilisation d'une autre couleur pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- ✓ Les feuilles de brouillon ne seront en aucun cas prises en compte.

Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

Ce sujet comprend 20 pages, y compris celle-ci.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir un surveillant.

Vous êtes assistant territorial de conservation du patrimoine et des bibliothèques principal de 2ème classe au sein du service Archives de la ville de Cultureville.

Votre Directeur général des services vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note sur l'application du Règlement Général sur la Protection des Données Personnelles (RGPD) aux Archives de la collectivité.

Liste des documents :

Document 1 : « Protection des données : Adoptez les 6 bons réflexes » - *cnil.fr* - 18 septembre 2019 - 1 page

Document 2 : « Point complet sur le règlement européen relatif aux données personnelles » - *lagazette.fr* - 9 octobre 2019 - 5 pages

Document 3 : « Le délégué à la protection des données au sein de la collectivité locale : missions et désignation » - A. de La Mure - *courrierdesmaires.fr* - 19 mars 2019 - 2 pages

Document 4 : « 4. Comment concilier les durées de conservation et les archives ? » (extrait) - Guide de sensibilisation au RGPD pour les collectivités territoriales - *cnil.fr* - Septembre 2019 - 3 pages

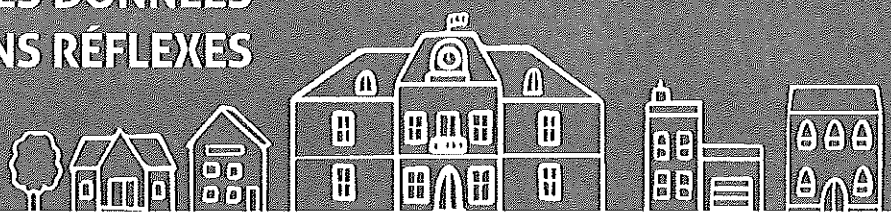
Document 5 : « La vie d'une donnée au regard des réglementations "CRPA", "RGPD" et "Patrimoine" » (extrait) - *reseau.supdpo.fr* - Juin 2019 - 1 page

Document 6 : « Vos données à caractère personnel : Tout savoir pour mieux archiver » - *archives.cotesdarmor.fr* - Janvier 2020 - 2 pages

Document 7 : « Le RGPD et les archives » - B. Ricard - *siafdroit.hypotheses.org* - 17 juin 2019 - 4 pages

DOCUMENT 1

PROTECTION DES DONNÉES
ADOPTEZ LES 6 BONS RÉFLEXES



1 NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF

Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.
Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».
Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

2 SOYEZ TRANSPARENT

Les administrés doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

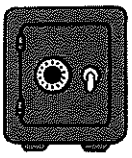
3 ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES ADMINISTRÉS

Vous devez organiser des modalités permettant aux administrés d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

4 FIXEZ DES DURÉES DE CONSERVATION

Vous ne pouvez pas conserver les données indéfiniment.
Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi.
Elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

5 SÉCURISEZ LES DONNÉES ET IDENTIFIEZ LES RISQUES



Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques.
Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données.
Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

6 INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE

La conformité n'est pas gravée dans le marbre et figée.
Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en œuvre. Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.

DOCUMENT 2

lagazette.fr
9 octobre 2019

Point complet sur le règlement européen relatif aux données personnelles

Le règlement européen sur la protection des données personnelles (RGPD) opère, à compter du 25 mai 2018, un changement de culture en passant du contrôle à la responsabilisation. Le premier versant de cette révolution culturelle tient dans l'affirmation des droits des personnes physiques relatifs à la protection des données personnelles. La mise en œuvre du RGPD implique également un renforcement des obligations des acteurs privés et publics.

« Toute personne a droit à la protection des données à caractère personnel la concernant », déclare l'article 8 §1 de la Charte des droits fondamentaux de l'Union européenne. Si depuis 1978, la loi Informatique et libertés affirmait déjà les grands principes traduisant ce droit, à compter du 25 mai 2018, le règlement européen sur la protection des données personnelles (RGPD) opère un véritable changement de culture en passant d'une logique de contrôle à une logique de responsabilisation des acteurs privés et publics. Cela se traduira par une mise en conformité permanente et dynamique de la part des collectivités.

Le champ d'application

Le RGPD protège les libertés et droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel. Il s'applique ainsi à tout responsable du traitement, personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données. Le traitement de données à caractère personnel est défini comme tout traitement automatisé en tout ou partie et appelé à figurer dans un fichier. Les données personnelles regroupent toutes les informations se rapportant à une personne physique identifiée ou identifiable par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou des éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Ce traitement doit s'entendre notamment par les opérations telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission de données. Le profilage de données se définit comme le traitement de données afin d'analyser et de prédire les éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. L'enjeu pour les collectivités est, pour l'essentiel, directement lié au développement de l'e-administration par les téléservices, l'open data, les systèmes d'information géographique, les réseaux sociaux, les compteurs intelligents, ou la lecture automatique de plaques d'immatriculation. « Les collectivités doivent s'interroger sur les personnes pouvant accéder à un fichier, la durée de conservation de celui-ci, son utilisation à des fins autres que celles prévues initialement et la pertinence des informations qui y sont contenues, mais aussi sur la protection des fichiers des cyberattaques de plus en plus nombreuses. »

L'enjeu se situe également pour les fichiers de ressources humaines, la sécurisation de leurs locaux, le contrôle d'accès par badge, la vidéosurveillance ou la gestion des différents services publics et activités dont elles ont la charge. Ainsi, un maire ne se servira pas du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra, en revanche, être utilisée à une telle fin. Seule la mention « personne en fauteuil roulant » sera enregistrée si la précision du handicap n'est pas nécessaire pour assurer une prise en charge adéquate de l'intéressé. Les agents doivent disposer d'un mot de passe individuel régulièrement changé et leurs droits d'accès aux fichiers sont définis en fonction de leurs besoins réels en lien avec l'exercice de leur mission.

Les droits des personnes physiques

Le RGPD précise huit droits qui sont autant d'outils à disposition des citoyens pour protéger leurs données personnelles. Le premier est le droit d'accès de la personne concernée aux données à caractère personnel détenues, ainsi que les Informations relatives à la finalité du traitement, aux catégories des données personnelles, la durée de conservation définie des données à caractère personnel et les destinataires auxquels les données ont été ou seront communiquées.

Le deuxième tient dans la possibilité de demander la rectification ou l'effacement de données personnelles au responsable du traitement.

Chaque personne physique peut aussi bénéficier de l'effacement des données personnelles, dit « droit à l'oubli », notamment lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées. La personne concernée pourra ainsi retirer son consentement ou s'opposer au traitement.

Le quatrième droit tient dans la possibilité de demander la limitation du traitement des données personnelles qui ne peuvent être traitées qu'avec le consentement de la personne concernée. Le RGPD crée également le droit à la notification de la rectification ou de l'effacement des données à caractère personnel ainsi que le droit à la portabilité des données à caractère personnel par le responsable du traitement, dans un format structuré couramment utilisé et lisible par une machine. Cela lui permet de les transmettre à un autre responsable du traitement.

Le septième droit est celui du droit d'opposition, à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel y compris un profilage. Le dernier droit tient dans la possibilité de demander à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques le concernant. Cela implique que la personne concernée a le droit d'obtenir une intervention humaine.

Le traitement des données à caractère personnel

- **Les principes du traitement**

Les obligations se fondent sur des principes qui doivent guider le responsable du traitement de données personnelles dans son action. Le premier principe rappelle que les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Cela implique que ladite personne a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. Ainsi, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.

Néanmoins, les données pourront être traitées sans le consentement si elles remplissent les conditions du principe de finalité, qui implique que les données sont collectées dans un but déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial comme, notamment, l'objectif nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Le règlement prévoit d'autres objectifs nécessaires :

- ✓ à l'exécution d'un contrat auquel la personne concernée est partie ;
- ✓ au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- ✓ à la sauvegarde des intérêts vitaux de la personne concernée ;
- ✓ aux fins des intérêts légitimes poursuivis par le responsable du traitement.

- **Le responsable de traitement**

Dans toutes ces hypothèses, le responsable du traitement devra informer la personne physique que son contentement n'est pas requis pour l'un des fondements sus-évoqués. Le principe de pertinence implique que seules les données strictement nécessaires à la réalisation de l'objectif poursuivi doivent être collectées. Le RGPD affirme aussi un principe de durée limitée de conservation des données personnelles au seul temps nécessaire à la réalisation de l'objectif poursuivi. Elles devront, au-delà de cette durée, être détruites ou archivées. Le dernier principe est celui de la sécurité de traitement de la collectivité qui doit prendre toutes les mesures utiles pour garantir l'intégrité et la confidentialité de ces données en s'assurant que les tiers non autorisés n'y auront pas accès.

Le responsable du traitement de données peut également avoir une obligation de réaliser une étude d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Elle est particulièrement requise en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, le traitement à grande échelle des catégories particulières de données (raciales, éthiques, relevant d'opinions politiques, de convictions religieuses, philosophiques, syndicales, génétiques, biométriques) et, en cas de surveillance systématique, à grande échelle d'une

zone accessible au public. L'analyse contient au moins une description systématique des opérations de traitement envisagées et des finalités du traitement, une évaluation de la nécessité et la proportionnalité des opérations de traitement au regard des finalités, et une évolution des risques pour les droits et libertés des personnes, ainsi que les mesures envisagées pour faire face aux risques. En cas de risque élevé, le responsable du traitement saisit l'autorité de contrôle pour avis afin de vérifier si le règlement communautaire est bien respecté. Chaque responsable du traitement devra tenir un registre des activités effectuées sous sa responsabilité comportant notamment le nom et les coordonnées du responsable du traitement, les finalités du traitement, une description des diverses catégories concernées (personnes, données à caractère personnel, destinataires auxquels les données à caractère personnel ont été ou seront communiquées), les délais prévus pour l'effacement des différentes catégories de données et une description générale des mesures de sécurité techniques et organisationnelles.

- **Un délégué à la protection des données**

A compter du 25 mai 2018, les collectivités territoriales devront désigner un délégué à la protection des données qui aura pour mission :

- ✓ d'informer et de conseiller le responsable de traitement de la collectivité ;
- ✓ de diffuser une culture « informatique et libertés » au sein de la collectivité ;
- ✓ de contrôler le respect du règlement et du droit national en matière de protection des données ;
- ✓ de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- ✓ de coopérer avec la Commission nationale de l'informatique et des libertés (Cnil) et d'être le point de contact de celle-ci.

Ce délégué devra disposer d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace, notamment sur les droits et pratiques en matière de protection des données, être associé aux questions « informatique et libertés » et bénéficier de ressources et formations nécessaires pour mener à bien ses missions,

Ce délégué peut être partagé entre plusieurs structures de mutualisation informatique ou au sein des EPCI.

L'article 32 du RGPD prévoit également une obligation de sécurisation des données. Il rappelle à cet effet que le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque comme le chiffrement des données à caractère personnel, les moyens garantissant la confidentialité, l'intégrité, la disponibilité des données, les moyens permettant de rétablir

La disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ainsi qu'une procédure visant à effectuer

des tests. Il devra aussi analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. L'objectif est de se prémunir contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises.

Les sanctions

Le responsable de traitement peut faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement. Les autorités de protection peuvent notamment :

- ✓ prononcer un avertissement ;
- ✓ mettre en demeure l'entreprise ;
- ✓ limiter temporairement ou définitivement un traitement ;
- ✓ suspendre les flux de données ;
- ✓ ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ✓ ordonner la rectification, la limitation ou l'effacement des données.

Les amendes administratives peuvent s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou dans le cas d'une entreprise, à 2 % et jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

L'article 82 du RGPD prévoit également un droit à réparation et responsabilité en précisant que toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. Cette disposition peut se combiner avec celle relative à une action de groupe en matière de protection des données personnelles ayant pour objet de faire cesser les manquements tenant à ce que plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la loi de 1978 par un responsable de traitement de données à caractère personnel ou un sous-traitant.

L'action est engagée par les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel, les associations de défense des consommateurs représentatives au niveau national et notamment les organisations syndicales de fonctionnaires. Cette action de groupe pourrait permettre de lutter contre le traitement des données personnelles qui viendrait porter atteinte à l'identité humaine, aux droits de l'homme, à la vie privée, aux libertés individuelles ou publiques. Si la Cnil a imposé ce changement de culture en passant d'une logique de contrôle à une logique de responsabilisation des acteurs privés et publics, alors une révolution pourrait bien naître dans les consciences des citoyens qui fournissent gratuitement leurs données personnelles à des algorithmes toujours plus puissants et intrusifs.

DOCUMENT 3

courrierdesmaires.fr
A. de La Mure
19 mars 2019

Le délégué à la protection des données au sein de la collectivité locale : missions et désignation

Depuis la rentrée en application du règlement général sur la protection dos données (RGPD), la désignation d'un délégué à la protection des données est obligatoire pour les collectivités. Il peut être interne, externe ou mutualisé pour plusieurs organismes. Le DPO joue un rôle essentiel dans la mise en conformité au RGPD et participe au développement de relations de confiance entre collectivités et administrés.

1 - Les missions du délégué

Informer et conseiller. C'est la première mission du DPO envers le responsable de traitement de la collectivité (maire, président de conseil régional et départemental, président d'EPCI), ainsi que les services opérationnels chargés de la mise en œuvre des traitements. Le délégué peut aussi, pour les utilisations les plus sensibles, conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution.

Contrôler le respect du règlement. Au DPO revient la charge de vérifier que le règlement et le droit national en matière de protection des données sont bien respectés. Dans la majorité des cas, le délégué prendra en charge la tenue et l'actualisation du registre des traitements. Ce registre lui offre une vue d'ensemble sur les finalités et conditions d'usage des données personnelles : quels objectifs, quelles données, quels destinataires, quelle durée de conservation, quelles mesures de sécurité, etc. Il est à géométrie variable suivant la taille de la collectivité. Celui des toutes petites communes pourra contenir moins d'une dizaine de fiches : état civil, liste électorale, cadastre, prêts à la bibliothèque, etc.

Une responsabilité non personnelle. Le DPO n'est pas personnellement comptable du respect de la réglementation. En cas de manquement aux obligations, il ne pourra être tenu juridiquement responsable en lieu et place de la collectivité publique et de son représentant légal.

Dans les petites communes, les secrétaires de mairie sont souvent pressentis pour occuper la fonction de DPO. Or, leur désignation peut parfois se heurter à des difficultés : manque de temps à y consacrer et risque de conflits d'intérêts. Ainsi, avant de procéder à la désignation, il faudra s'assurer qu'ils ne prennent pas part au circuit de décision concernant les fichiers mis en œuvre dans leur collectivité (objectifs et conditions de mise en œuvre, données traitées, destinataires, durées de conservation, mesures de sécurité, etc.).

Être le point de contact. C'est la troisième mission du DPO, interlocuteur privilégié de la Cnil, au contact des administrés et des agents dont les données sont traitées pour faciliter l'exercice de leurs droits.

2 - Compétences et statut du DPO

Le RGPD n'impose pas aux organismes de recourir à un profil particulier pour la désignation de leur DPO : aucun agrément n'est prévu, aucune exigence de diplôme ou condition statutaire n'est fixée ; il peut s'agir d'une personne issue du secteur juridique, technique ou de tout autre secteur (archives, communication, qualité, etc.), physique ou morale, interne ou externe (avocat, consultant, etc.).

Un expert libre de ses analyses. Le niveau d'expertise « informatique et libertés » du délégué doit être proportionné au niveau de protection qu'exigent le nombre, la taille et la complexité des traitements mis en œuvre par la collectivité. Le délégué doit être à l'abri des conflits d'intérêts, rendre compte au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté dans les analyses et actions qu'il décide

d'entreprendre.

3 - Désignation et mutualisation

La collectivité doit notifier à la Cnil la désignation de son délégué, par l'intermédiaire du téléservice de la Cnil.

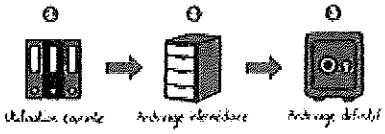
Mutualiser le DPO. Afin de limiter les coûts et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires, le délégué peut être mutualisé, au niveau par exemple :

- d'un EPCI agissant pour le compte des communes membres ;
- d'un centre de gestion de la fonction publique territoriale (CDG-FPT) proposant un tel service aux collectivités de son ressort territorial.

DOCUMENT 4

4 COMMENT CONCILIER LES DURÉES DE CONSERVATION ET LES ARCHIVES ?

Les données à caractère personnel doivent être conservées pour la durée de leur utilité. Mais une même donnée peut avoir parfois plusieurs utilités successives ce qui implique donc des durées de conservation différentes.



Le cycle de vie des données à caractère personnel peut se décomposer en trois phases successives :

- les données sont en cours d'utilisation (dossier « en cours ») ;
- les données sont mises de côté (le dossier est réglé) ;
- les données sont archivées (le dossier est réglé et archivé).

1ère phase : l'utilisation courante ou « base active » qui correspond à la durée d'utilisation courante (DUC)

C'est la durée d'utilisation courante des données ou, autrement dit, la durée nécessaire à la réalisation de l'objectif du traitement (établissement d'un acte d'état civil, gestion d'un bénéficiaire d'une prestation, inscription aux activités périscolaires, etc.).

Durant cette phase, les données sont généralement accessibles quotidiennement aux agents, selon leurs fonctions, au sein des services opérationnels (chargés de l'état civil, du cadastre, des établissements scolaires, etc.).

Il appartient au responsable du fichier de définir cette durée et de la respecter. Lorsqu'il fait appel à des sous-traitants et qu'il n'a pas directement la main sur les données, cette durée doit être définie contractuellement.

EXEMPLE D'UTILISATION COURANTE

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur accessible au sein d'un bureau placé dans un tiroir fermé à clé quand il n'est pas utilisé.

2e phase : l'archivage intermédiaire qui correspond à la durée d'utilisation administrative (DUA)

Après leur utilisation, les données personnelles peuvent parfois être conservées dans une base d'archivage intermédiaire, distincte de la base active, avec accès restreint, dans la mesure où :
- il existe une obligation légale de conservation de données pendant une durée fixée ;
- en l'absence d'obligation de conservation, ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables.

Il ne s'agit pas de conserver l'intégralité des données mais seulement celles qui sont indispensables ou requises par l'obligation légale.

Ces données ne peuvent plus être utilisées par les services opérationnels : elles sont désormais conservées dans un but précis et ne sont accessibles que de façon restreinte.

Le choix du mode technique d'archivage intermédiaire est laissé à l'appréciation du responsable du fichier. Ces données peuvent par exemple être archivées sur un support de conservation dédié avec des accès restreints aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple le service juridique).

La décision de recourir à un archivage intermédiaire doit être prise dès la sélection du sous-traitant pour une gestion optimale.

EXEMPLE D'ARCHIVAGE INTERMÉDIAIRE

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur rangé dans une salle d'archivage fermée à clé au sein des bureaux.

3e phase : l'archivage définitif

Certaines données et documents présentant un intérêt historique doivent pouvoir être conservées et archivées, dans les conditions fixées par le code du patrimoine.

Cette mission est celle du service des Archives de France. La décision ainsi que les modalités d'archivage définitif des documents des collectivités « sont définies par accord entre le service, l'établissement ou l'organisme intéressé et le service interministériel des Archives de France de la direction générale des patrimoines » (article R. 212-13 du code du patrimoine).

Il est recommandé de les conserver sur un support physique indépendant n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

Afin de vous renseigner sur vos obligations en matière d'archivage définitif, vous pouvez vous rapprocher des services d'archives concernés (dans la plupart des cas pour les communes les services d'archives départementales) et consulter le site francearchives.fr.

EXEMPLE D'ARCHIVAGE DÉFINITIF

À titre de comparaison avec des dossiers papier, il s'agirait d'un classeur transmis à un organisme d'archivage.

BONNE PRATIQUE

Les différentes durées de conservation doivent être inscrites dans le registre du délégué à la protection des données pour chacun des traitements concernés.

Dans chacune des phases, le responsable du fichier doit prévoir des mesures techniques et organisationnelles pour protéger les données (destruction, perte, altération, diffusion ou accès non autorisés, etc.). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données considérées. Par exemple, les données des destinataires de la lettre d'information de la collectivité n'appellent pas les mêmes mesures que la gestion des prestations sociales octroyées par la collectivité ou le fichier de gestion des activités de la police municipale).

Une personne qui exerce son droit d'accès doit obtenir la communication de l'intégralité des données qui la concernent, qu'elles soient stockées en base active ou archivées.

Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

POUR ALLER PLUS LOIN

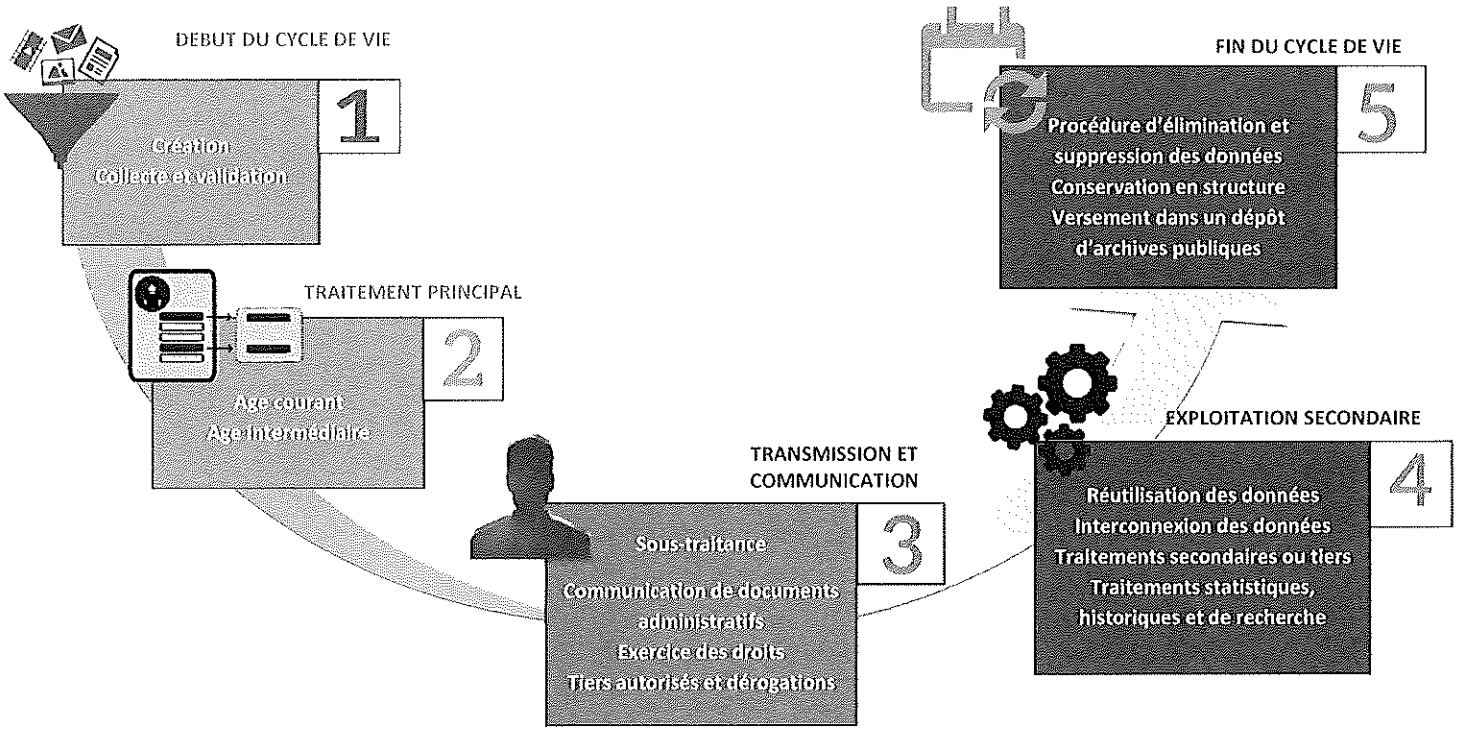
Des préconisations relatives au tri et à la conservation des archives produites par les communes et les structures intercommunales ont été faites dans l'instruction DGP/SIAF/2014/006.

DOCUMENT 5

Juin 2019

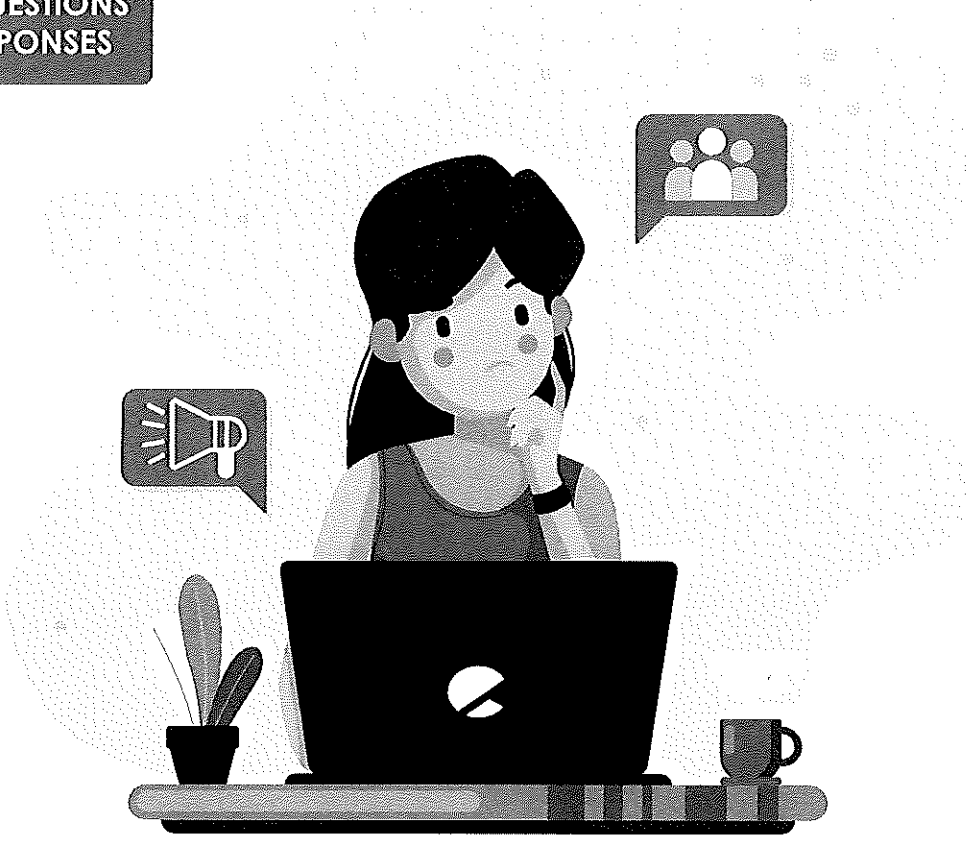
LA VIE D'UNE DONNÉE

AU REGARD DES RÉGLEMENTATIONS
« CRPA », « RGPD » et « Patrimoine »



DOCUMENT 6

QUESTIONS RÉPONSES



VOS DONNÉES À CARACTÈRE PERSONNEL

Tout savoir pour mieux archiver

Janvier 2020

Direction de la citoyenneté

Archives départementales des Côtes d'Armor
archives.cotesdarmor.fr

Côtes d'Armor le Département

QUESTIONS RÉPONSES

Le RPGD[1] : quels sont les effets de ce texte sur la gestion des documents contenant des données à caractère personnel ?

Question : je collecte ou manipule des données à caractère personnel, que dois-je faire ?

Réponse : pensez à vous rapprocher de votre délégué à la protection des données.

Q : un usager me demande de supprimer des données le concernant, que dois-je faire ?

R : ne le faites pas systématiquement, tout dépend du contexte. Dans la plupart des cas, le droit à l'oubli ne s'applique pas[2].

Q : les données personnelles que je gère sont à conserver longtemps avant destruction. Comment peut-on les mettre à l'abri d'éventuels usages malveillants ?

R : des solutions de conservation des données sécurisées existent. Il faut se rapprocher de la direction informatique et du délégué à la protection des données.

Q : les données personnelles que je gère sont à conserver définitivement. Dois-je les anonymiser pour garantir le droit à l'oubli ?

R : non, les archives à vocation historique ne doivent pas être anonymisées.
En fin de durée d'utilité administrative, elles doivent être versées sans avoir été modifiées. Leur versement dans un système d'archivage électronique garantit la sécurité des données conservées. On peut cependant conserver les données dans le système d'informations, après leur versement aux Archives, à condition de les anonymiser.

Q : j'ai eu recours à un dossier conservé aux Archives départementales, puis-je faire rectifier les données erronées relatives à une personne ?

R : les archives historiques ne peuvent être modifiées. Ce sont des originaux qui perdraient cette valeur si des modifications y étaient apportées. Le droit de rectification ne s'applique pas dès lors que la durée d'utilité administative[3] est écoulée.

[1] Le Règlement Général de la Protection des Données
Le Règlement européen 2016/679 relatif à la protection des données à caractère personnel (ou RGPD) est entré en vigueur le 25 mai 2018 dans tous les États membres de l'Union européenne.

[2] Le droit à l'oubli
Ce droit ne s'applique pas lorsque le traitement est nécessaire pour respecter une obligation légale ou pour exécuter "une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement" (art. 17 du RGPD).

[3] La durée d'utilité administrative
Le RGPD et l'article 36 de la loi Informatique et Libertés révisée confirment la possibilité de conserver les données au-delà de la durée de conservation dans le traitement initial (durée qui correspond habituellement à la durée d'utilité administrative – DUA) "à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques".

Côtes d'Armor le Département

DOCUMENT 7

siafdroit.hypotheses.org
A. Ricard
17 juin 2019

Le RGPD et les archives

Le Règlement européen 2016/679 relatif à la protection des données à caractère personnel ou RGPD est entré en vigueur le 25 mai 2018 dans tous les Etats membres de l'Union européenne. La plupart de ses dispositions sont d'application directe.

Le RGPD est complété par la loi du 6 janvier 1978, dite loi Informatique et Libertés modifiée à plusieurs reprises. Elle l'a été en 2018 par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, qui a servi à « implémenter, le RGPD en droit national et porte transposition de la directive européenne 2016/680 relative aux données pénales », puis par l'ordonnance n° 2018-1125 du 12 décembre 2018 qui a restructuré la loi Informatique et Libertés pour la rendre plus lisible et procéder à des mises en cohérence, entrée en vigueur le 1er juin 2019.

Le cadre général

Comme le rappelait Aude Roelly dans son billet du 18 mai 2016 publié à l'occasion de l'adoption du RGPD, « le règlement a pour but de redonner aux citoyens le contrôle des données qui les concernent. (...) Il s'inscrit dans le contexte de la lutte contre le profilage des personnes et pour le contrôle de l'utilisation des données à caractère personnel par les grands acteurs du web (Facebook, Google, etc.) ».

Le RGPD et la loi Informatique et Libertés révisée renforcent en conséquence les droits des personnes et accroissent les obligations des responsables de traitements. Ils s'appliquent aux traitements de « données à caractère personnel », c'est-à-dire aux informations se rapportant à des personnes physiques identifiées ou identifiables, directement ou indirectement. Le RGPD et la nouvelle loi concernent tous les organismes, qu'ils soient publics ou privés, les personnes physiques comme les personnes morales, et tous les secteurs d'activités. Ils s'appliquent aux acteurs européens, mais aussi aux responsables de traitements établis hors de l'Union européenne lorsque les données qu'ils traitent concernent des personnes résidant dans l'Union.

Le RGPD et la nouvelle loi Informatique et Libertés concernent aussi bien le numérique que le papier : les bases de données, les listes de contacts, les listes d'invités à des manifestations, les dossiers de personnel, les données générées par les outils de contrôle d'accès, les registres, fichiers ou applications de gestion des usagers d'un service d'archives ou d'une bibliothèque, etc., entrent dans leur champ d'application.

Si ces deux textes visent toutes les données à caractère personnel, ils identifient en leur sein, comme les textes précédemment en vigueur, une catégorie particulière de données : les « données sensibles ». Il s'agit des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la vie sexuelle ou à l'orientation sexuelle et à la santé, ainsi que des données génétiques et biométriques. Ces données sensibles, de même que les données à caractère personnel relatives aux infractions et aux condamnations, sont soumises à des conditions de traitement très strictes (art. 9 et 10 du RGPD et dispositions complémentaires dans les législations nationales).

Il convient aussi de préciser que le RGPD s'applique seulement aux données relatives aux personnes vivantes, sauf extension par les Etats membres aux données relatives aux personnes décédées (considérant 27 du RGPD). La France n'a fait usage de cette option que de manière marginale, dans le champ des données de santé (art. 16 de la loi relative à la protection des données personnelles) et, antérieurement, dans le cadre de la loi pour une République numérique du 7 octobre 2016, notamment en octroyant le droit à « toute personne [de] définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès », disposition à laquelle dérogent les archives publiques (art. 63 de la loi pour une République

numérique, art. 85 de la loi Informatique et Libertés).

Le nouveau cadre juridique de la protection des données à caractère personnel consacre ou renforce plusieurs grands principes :

- Le principe de licéité, de loyauté et de transparence. La licéité répond à un certain nombre de conditions alternatives au rang desquelles figure le consentement explicite de la personne.
- Le principe de limitation des finalités : les données doivent être « collectées pour des finalités déterminées, explicites et légitimes ».
- Le principe de « minimisation des données » : les données doivent être « adéquates », « pertinentes », « limitées à ce qui est nécessaire au regard des finalités ».
- Le principe d'exactitude : les données doivent être exactes et à jour.
- Le principe de limitation de la conservation : la conservation des données doit être limitée dans le temps.
- Le principe de sécurité : les données doivent être traitées de manière à en garantir l'intégrité et la confidentialité.

A ces principes s'ajoute celui de la « responsabilité du responsable du traitement ». Ce principe de responsabilité se substitue au régime des « formalités préalables » (déclarations, autorisations) auprès des autorités de contrôle (la Commission nationale de l'informatique et des Libertés - CNIL - en France), régime qui ne subsiste que pour quelques catégories de traitements (notamment données génétiques et biométriques et données de santé). Les organismes doivent désormais s'assurer eux-mêmes de la conformité de leurs traitements au nouveau cadre juridique et pouvoir la démontrer. Ils doivent notamment appliquer le privacy by design, concept qui impose de réfléchir à la protection des données à caractère personnel en amont de la conception d'un traitement de données. Ils doivent également, dans certains cas, procéder à une « analyse d'impact » lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, analyse d'impact suivie, le cas échéant, d'une « consultation préalable » de la CNIL. Les organismes doivent aussi désigner un délégué à la protection des données ou data protection officer (DPO), chargé de conseiller l'organisme, mais aussi de contrôler la conformité de ses traitements au RGPD. Le DPO - qui peut être mutualisé entre plusieurs organismes - a plus de pouvoir que les anciens correspondants Informatique et Libertés (CIL). Le RGPD impose également de tenir un « registre des opérations de traitement », dont la CNIL propose un modèle.

Contrepartie de la responsabilité, les textes alourdissent les sanctions en cas de non-respect, jusqu'à 20 millions € ou, s'agissant d'une entreprise, 4 % de son chiffre d'affaires mondial. A ces grands principes - licéité, loyauté, transparence, limitation des finalités, etc. - sont associés des droits pour les personnes concernées par un traitement de données : « droit à l'oubli » ou « droit à l'effacement », droit d'opposition, droit de rectification, droit à la limitation du traitement, droit d'accès. Elles bénéficient aussi d'un « droit à la portabilité des données » qui permet de récupérer les informations fournies sous une forme réutilisable, afin, par exemple, de les transférer à un tiers.

Ce cadre général admet des exceptions et dérogations, prévues pour concilier le droit à la protection des données à caractère personnel avec d'autres droits comme la liberté d'expression ou encore le droit d'accès aux documents officiels.

Et les archives ?

Tel est le cas des archives qui bénéficient d'un statut spécifique, dérogatoire au régime de droit commun, statut justifié par la finalité de la conservation des archives (apporter des preuves, documenter l'histoire) qui implique la conservation d'archives intègres.

Ce régime dérogatoire n'est toutefois pas applicable à toutes les archives : il ne concerne que les archives définitives et il est de nature différente selon qu'il s'agit d'archives traitées par des services publics d'archives ou d'archives privées détenues par des personnes physiques ou morales de droit privé (entreprises, associations, Églises, etc.).

Les archives définitives conservées par les Services publics d'archives

Le RGPD et les articles 4 (2° et 5°) et 78 de la loi Informatique et Libertés révisée confirment la possibilité de conserver les données au-delà de la durée de conservation dans le traitement initial (durée qui correspond habituellement à la durée d'utilité administrative - DUA) « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ».

Les « traitements à des fins archivistiques dans l'intérêt public » sont, au sens du RGPD (considérant n° 158), ceux qui sont mis en œuvre par les services qui ont une obligation légale de collecte. De conservation et de communication d'archives définitives, c'est-à-dire en France, les services publics d'archives.

En application de l'article 78 de la loi Informatique et Libertés et des articles 17 et 89 du RGPD, les traitements mis en œuvre par les services publics d'archives dérogent à certains droits des personnes concernées par les traitements dans la mesure où ces droits seraient susceptibles de rendre impossible ou de compromettre gravement les finalités de ces traitements. Il s'agit des dérogations au droit à l'oubli ou droit à l'effacement, au droit d'opposition, au droit de rectification, au droit à la limitation du traitement, au droit à la portabilité des données, au droit d'accès de la personne concernée - au sens Informatique et Libertés - et de la dérogation à l'obligation de notification « en ce qui concerne la rectification ou l'effacement des données ou la limitation du traitement ».

Ces dérogations s'appliquent également aux archives définitives encore conservées par les producteurs, dans l'attente de leur versement dans le service public d'archives compétent. Elles s'appliquent aussi, le cas échéant, aux archives conservées par les services d'archives dont la DUA ne serait pas échue, mais dont, nécessairement puisqu'il y a eu versement, la durée de conservation dans le traitement initial est expirée.

Ces dérogations aux droits des personnes ont été obtenues en contrepartie de « conditions et garanties appropriées » constituées, s'agissant des archives publiques, par le très riche corpus normatif qui encadre leur gestion en France (code du patrimoine, code des relations entre le public et l'administration, décret à paraître sur les modalités de diffusion en ligne des archives, normes en matière d'archivage électronique, etc.).

Les archives courantes et intermédiaires

Les archives courantes et intermédiaires relèvent du régime de droit commun du RGPD et de la loi Informatique et Libertés, c'est-à-dire que le droit à l'effacement, le droit de rectification, le droit d'opposition, etc. peuvent s'exercer à leur égard. Ces droits sont cependant limités dans certains cas, limitations précisées dans chacun des articles du RGPD qui leur sont dédiés. Le droit à l'effacement, par exemple, ne s'applique pas lorsque le traitement est nécessaire pour respecter une obligation légale ou pour exécuter « une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (art. 17 du RGPD).

Les archives définitives de la sphère privée

Les archives du secteur privé ne peuvent pas bénéficier des dérogations associées aux « traitements à des fins archivistiques dans l'intérêt public » dans la mesure où les personnes ou organismes en cause n'ont pas d'obligation légale de collecte, de conservation, de traitement et de communication de leurs archives.

Mais comme leur traitement a pour finalité la recherche historique, ces archives bénéficient du régime spécifique accordé aux traitements à des fins de recherche scientifique ou historique ou à des fins statistiques. Ces traitements dérogent au droit à l'oubli dans la mesure où ce droit serait susceptible de rendre impossible ou de compromettre gravement la réalisation de leurs finalités et l'article 23 du décret n° 2018-687 du 1er août 2018 modificatif du décret n° 2005-1039 (dispositions aujourd'hui inscrites à l'article 116 du décret n° 2019-536 du 29 mai 2019) a défini l'étendue des autres dérogations dont ils peuvent bénéficier et des conditions et garanties appropriées qui doivent être mises en œuvre par leurs responsables.

Quel que soit le type d'archives conservées, les services d'archives auront l'obligation d'alimenter le « registre des opérations de traitement » de l'organisme dont ils relèvent, ou d'en constituer un

spécifique à leur service, selon la taille de celui-ci et le mode d'organisation de l'administration ou de la collectivité à laquelle ils sont rattachés.

Ils devront aussi engager un dialogue étroit avec leur DPO, qui pourra être un allié dans la sensibilisation des services producteurs à la légalité d'une deuxième vie pour les données à caractère personnel, à l'issue de la durée de conservation dans le traitement initial, et à la légitimité des traitements archivistiques.