LA PROTECTION
DES DONNÉES PERSONNELLES

GUIDE DE SENSIBILISATION

ADMINISTRATION DE LA POLYNÉSIE FRANÇAISE

INTRODUCTION

Dans notre grande majorité, nous recueillons les données de nos concitoyens ou avons accès à des renseignements et des documents à caractère personnel, dans l'exercice de nos missions.

Ces données sont variées. Même si elles peuvent parfois paraître «courantes », elles révèlent beaucoup sur la vie des personnes qu'elles concernent. C'est la raison pour laquelle les données personnelles doivent être protégées.

La protection de ces données est une obligation pour l'administration. Elle est imposée par la loi.

Mais surtout, cette protection fait partie intégrante du service que nous devons à nos concitoyens et de la confiance qu'ils placent en nous.

Le présent guide vous expose les règles qui encadrent la collecte et le traitement des données personnelles.

Il aide à mieux comprendre la réglementation, pour vous aider à la mettre en œuvre.

SOMMAIRE

01

QUELLE RÈGLEMENTATION S'APPLIQUE EN POLYNÉSIE FRANÇAISE ?

La protection des individus en matière informatique a été instaurée par la loi n°78-17 du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés.

Cette loi est applicable en Polynésie française depuis 1980 et beaucoup de ses modifications successives nous ont été étendues.

Cette loi posait déjà un grand nombre de principes et d'obligations. Elle prévoyait que les traitements informatiques devaient faire l'objet de formalités préalables auprès de la commission nationale de l'informatique et des libertés, la CNIL (selon le cas : des déclarations, des autorisations ou des demandes d'avis).

En 2018, le droit a évolué de manière importante. Le règlement UE 2016/679 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* (RGPD) est en effet entré en application le 25 mai 2018 dans l'Union européenne.

Pour tenir compte du RGPD, la loi de 1978 a été totalement réécrite, par une ordonnance n°2018-1125 du 12 décembre 2018.

En Polynésie française, la nouvelle réglementation nous est applicable, puisque l'ordonnance en prévoit l'extension dans notre collectivité. L'ordonnance a été publiée au JOPF du 21 décembre 2018.

C'est la loi du 6 janvier 1978, dans la version issue de l'ordonnance, qui nous est désormais applicable. La loi modifiée renvoie au RGPD à de nombreuses reprises.

Un décret d'application vient compléter ce dispositif.

Ces textes entrent en vigueur le 1er juin 2019.

02

QU'EST CE QU'UNE DONNÉE PERSONNELLE ?

Les textes définissent largement le concept de données à caractère personnel.

Selon la définition légale une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »

Une donnée personnelle est donc toute information, quelque en soit la forme (écrite, numérique, photographique, sonore…), qui permet, seule ou par combinaison avec d'autres informations, d'identifier quelqu'un.

Certaines données sont considérées comme « sensibles » et font l'objet de règles plus contraignantes.

La typologie suivante liste un certain nombre de données par grandes catégories.

DONNÉES COURANTES

État-civil, identité, données d'identification

Vie personnelle (habitudes de vie, situation familiale…)

Vie professionnelle (CV, scolarité, formation professionnelle, carrière, distinctions…)

Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…)

Données de connexion (adresses IP, journaux d'événements…)

Données de localisation (déplacements, données GPS, GSM…)

Données bancaires

DONNÉES SENSIBLES

Origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, biométriques, données concernant la santé, la vie sexuelle et l'orientation sexuelle

Numéro d'immatriculation au répertoire national d'identification des personnes physiques (NIR)

Infractions et condamnations pénales, mesures de sureté

Dans nos activités, ces informations sont collectées. Nous sollicitons par exemple :

- dans presque tous les cas : l'identité, la date de naissance, l'adresse, le téléphone, le courriel ;
- pour les demandes d'aides sociales ou les bourses : la composition du foyer familial, l'activité professionnelle, les revenus,
- pour les déclarations fiscales : les activités professionnelles, les revenus, les coordonnées bancaires,
- pour la prise en charge dans les établissements de santé : le numéro CPS, les résultats d'analyses médicales, le suivi des soins…

Une image de vidéosurveillance est également une donnée personnelle dès lors que l'on reconnait une personne ou que l'on sait de qui il s'agit.

Et pour les personnes morales ?

Les informations relatives aux personnes morales *(sociétés, associations…)* ne sont pas concernées par la législation sur la protection des données personnelles. Mais il faut être vigilant car des données de personnes physiques sont parfois collectées à l'occasion des demandes formulées par les personnes morales. Par exemple, dans une demande de subvention, l'identité et les coordonnées d'un président d'association peuvent être sollicitées. Dans ce cas, il convient d'en assurer la protection.

Et pour les personnes décédées ?

Les droits prévus par les textes s'éteignent au décès de la personne. La personne peut toutefois, de son vivant, laisser des directives quant à la conservation, l'effacement ou la communication des données qui la concernent.

Il faut également être vigilant quand une information concernant une personne décédée est susceptible d'avoir un impact sur la vie privée de l'un de ses ayants droits vivant. Si tel est le cas, elle doit être protégée.

En Polynésie française il est plus facile d'identifier une personne à partir d'informations éparses, car la population y est peu nombreuse et beaucoup de personnes se connaissent ou entretiennent des liens amicaux, familiaux ou professionnels.

Des initiales, un prénom, une information sur le lieu de vie ou sur l'activité professionnelle peuvent suffire à identifier quelqu'un de manière quasi certaine. C'est ce que l'on appelle le risque de ré identification. La vigilance s'impose donc pour éviter une telle ré identification.

03 QU'EST-CE QU'UN TRAITEMENT ?

Le traitement est un concept largement défini. En réalité, tous les outils utilisés dans le cadre de nos activités sont concernés, dès lors qu'ils contiennent des données de personnes physiques.

A son origine, la législation ne visait que les « fichiers » automatisés.

Désormais elle vise « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, 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, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »

Un traitement peut donc être :

- une application métier développée pour votre service,
- une application de gestion électronique de documents,
- une application de gestion du courrier,
- un téléservice,
- un logiciel, quelqu'en soit l'objet,
- un site internet,
- un dossier numérique,
- des fichiers pdf classés ou archivés dans un répertoire sur le réseau interne,
- un fichier ou outil interne partagé ou non, de type fichiers word, excell ...
- une extraction de données,
- la captation d'images de vidéo-surveillance,
- mais également les dossiers papiers contenant les données des usagers.

Les traitements déployés par notre administration se fondent sur l'exécution de nos missions d'intérêt public ou, parfois sur une obligation légale ou règlementaire à laquelle nous sommes soumis. Dès lors, et sauf exceptions *(certains traitements dans le domaine de la santé par exemple)*, nous n'avons pas à recueillir le consentement des personnes lorsque nous les mettons en œuvre. Ceci étant, les personnes doivent être informées de leurs droits *(voir point 7. ci après)*.

ET LE RESPONSABLE DE TRAITEMENT ?

Le responsable de traitement est celui qui détermine les finalités et moyens des traitements.

En pratique, il s'agit de la personne morale représentée par son représentant légal. Pour notre administration, c'est la ministre en charge du numérique qui assume cette responsabilité, pour les services administratifs et ministères en vertu d'une délégation de pouvoir du Président de la Polynésie française, chef de l'administration.

Dans les établissements publics, c'est le directeur qui représente l'établissement.

04 QUELS PRINCIPES S'APPLIQUENT AUX TRAITEMENTS ?

Notre administration peut traiter des données personnelles dès lors qu'elle le fait dans le cadre de ses missions de service public. En réalité elle en a besoin pour remplir ses missions et satisfaire les demandes des usagers.

Mais elle doit veiller au respect de certains principes.

Tout d'abord, les données ne peuvent être collectées puis traitées que pour des finalités déterminées, explicites et légitimes.

Les données doivent servir pour un usage précis, conforme à nos missions et clairement expliqué à nos usagers. A chaque traitement doit correspondre une finalité. En quelque sorte, il faut pouvoir répondre à la question : à quoi sert le traitement ?

Par exemple, si un traitement sert à gérer les demandes de permis de construire, les renseignements récoltés dans ce cadre serviront à instruire ces demandes et ne pourront pas être utilisés pour d'autres besoins, à moins qu'ils n'aient un lien suffisant *(par exemple, une demande ultérieure portant sur une modification du permis de construire)* ou qu'un texte prévoit un droit de communication.

Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire.

Cela signifie que nous ne pouvons collecter que les données dont nous avons réellement besoin, dans le cadre de notre activité. Des informations superflues ou inutiles ne doivent pas être demandées.

Pour reprendre l'exemple du permis de construire, il n'est pas nécessaire de connaître le nombre d'enfants du foyer, pour traiter une telle demande. En revanche, cette information sera utile pour une demande de prestation sociale.

Tout dépend donc de la mission exercée et de la réglementation qui l'encadre.

Les données doivent être exactes et tenues à jour.

Dans ses prérogatives, l'administration doit s'assurer que les données qu'elle conserve ne sont pas fausses et prendre toute mesure pour les maintenir à jour. Si des données inexactes sont identifiées *(erreurs, oublis…)* elles doivent être rectifiées ou effacées sans tarder.

Enfin, les données doivent être protégées et conservées seulement pendant une durée déterminée.

Nous devons veiller à ce que les données soient sécurisées. Elles ne doivent pas être divulguées, sauf dans les cas prévus par un texte. Elles doivent être protégées contre les actes malveillants *(intrusion, vol)* mais aussi contre la détérioration, ou la perte.

Les données ne peuvent pas être conservées sans limitation. Passés certains délais, il convient soit de les archiver, soit de les détruire. Tout dépendra des besoins du domaine d'activité et des différents délais qui s'appliquent *(notamment délais de prescription, délais d'archivage…).*

05

COMMENT DOIT-ON TRAITER LES DONNÉES PERSONNELLES ?

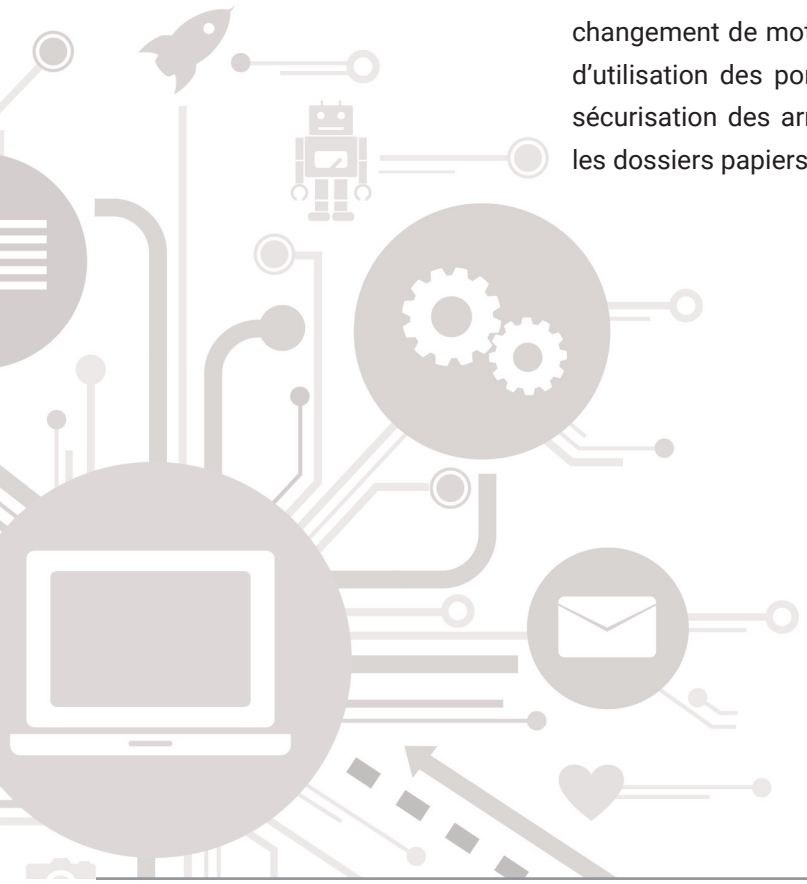
Les données récoltées doivent être traitées de manière à en garantir la confidentialité.

Cela passe par la définition de procédures internes déterminant les personnels habilités à accéder aux données, l'étendue de leurs droits d'accès, les modalités de stockage ou de transfert des données, éventuellement le cryptage des données. Plus les données sont sensibles, plus les procédures doivent être strictes.

Des bonnes pratiques doivent être adoptées : sauvegardes régulières, archivage dans certains délais, sécurisation des accès, politique de changement de mot de passe, règles d'utilisation des ports USB externes, sécurisation des armoires contenant les dossiers papiers….

Il faut garder à l'esprit que les données personnelles ne doivent être accessibles ni aux personnels qui n'en ont pas besoin dans l'exercice de leurs fonctions, ni a fortiori au public fréquentant les services.

Une note interne doit définir ces paramètres, au regard de l'organisation propre et des besoins et missions de chaque service. Et dans tous les cas, le bon sens et la précaution s'imposent.



06 QUELS SONT LES RISQUES PESANT SUR LES DONNÉES PERSONNELLES ?

Les données personnelles représentent un capital intéressant, notamment pour les opérateurs économiques. Elles sont, par exemple, utilisées par les sociétés proposant des services ou des produits en ligne pour cibler les consommateurs. Elles sont cédées entre entreprises. Elles sont donc convoitées.

Par ailleurs, les données font, de plus en plus fréquemment, l'objet de violations. Ces violations peuvent résulter de négligences *(absence de sécurisation des postes de travail, perte de ports USB contenant des données…)* ou d'actes malveillants *(copies non autorisées de données ou de dossiers, divulgation délibérée d'informations personnelles à des tiers, piratage informatique …).*

Les piratages qui visent les données détenues par les entreprises et les administrations sont un phénomène en forte augmentation. Ils sont souvent le fait de « hackers » qui s'introduisent dans les systèmes d'information à la faveur de failles ou de négligences de sécurité.

Les données ainsi subtilisées peuvent être utilisées contre les personnes qu'elles concernent, de manière malveillante.

Dès lors, toutes les mesures utiles doivent être prises pour que les données ne soient pas accessibles à des tiers.

07

QUELS SONT LES DROITS DES CITOYENS ?

Les citoyens disposent de droits renforcés qui doivent être portés à leur connaissance. L'information s'exerce par des mentions figurant sur les sites internet, sur les téléservices, ou sur les formulaires.

Le droit à l'information

Un certain nombre d'informations doit être porté à la connaissance des citoyens, telles que par exemple, l'identité et les coordonnées du responsable de traitement, les coordonnées du délégué à la protection des données, les finalités du traitement, les catégories de données à caractère personnel traitées, les destinataires des données, la durée de conservation des données, les droits et les modalités selon lesquelles ils peuvent être exercés.

Le droit d'accès et le droit de rectification

Tout citoyen peut demander la communication des données qui le concernent. Il peut également en demander la rectification, c'est-à-dire la modification ou la correction.

Le droit d'opposition

Le droit d'opposition permet à la personne concernée de s'opposer, pour des motifs légitimes tenant à sa situation particulière, à ce que ses données soient traitées.

Pour les traitements répondant à une obligation légale, ce droit n'est pas applicable. Il peut également être écarté par une disposition expresse de l'acte instaurant le traitement, pour certains motifs importants d'intérêt public, notamment en matière financière, économique, monétaire, budgétaire, fiscal, de santé publique et de sécurité sociale, ou encore pour l'exercice de missions de contrôle ou d'inspection.

Le droit à l'effacement (ou suppression)

Ce droit permet à toute personne d'obtenir l'effacement des données qui la concernent.

Sauf exception, ce droit ne s'exerce pas pour les traitements mis en œuvre par notre administration car ils sont fondés sur l'exécution d'une mission d'intérêt public.

Le droit à la limitation

Ce droit permet à la personne concernée de demander que ses données soient conservées, mais non traitées. Les cas dans lesquels le droit à la limitation du traitement peut être exercé, sont limités. Ce droit s'applique si la personne concernée exerce son droit de rectification, dans l'attente de cette rectification, ou bien si le traitement est illicite, ou si la personne concernée souhaite que ses données soient conservées pour exercer un droit en justice.

Le droit à la portabilité

Toute personne peut demander la restitution de ses données sous un format structuré couramment utilisé et lisible par machine, ou le transfert de ses données vers une autre entité.

Ce droit ne s'applique pas aux traitements nécessaires à l'exécution d'une mission d'intérêt public.

La mise en œuvre des droits des personnes

Ces droits peuvent être exercés à tout moment, en justifiant de son identité.

L'usager doit être informé de la manière dont il peut exercer ses droits. Les mentions d'information doivent donc préciser l'adresse *(postale et électronique)* à laquelle il peut envoyer sa demande.

Le délai maximum pour répondre à une demande est d'un mois éventuellement prolongé de deux mois pour tenir compte de la complexité ou du nombre de demandes. La personne doit alors être informée de cette prolongation et de ses motifs.

La délivrance des données se fait par voie postale ou électronique, ou directement à l'usager s'il est présent.

Le responsable du traitement n'est pas tenu de donner suite aux demandes manifestement infondées ou excessives, à charge pour lui d'en démontrer le caractère infondé ou excessif.

L'obligation de notification d'une violation de données

Si une violation de données survient et que cette violation fait peser un risque pour les droits et libertés d'une personne, une notification à la CNIL doit être effectuée *(voir point 8)*.

Si le risque que fait peser cette violation sur les droits et libertés de la personne est élevé, la violation doit également être notifiée à la personne. Dans le cas où la violation concerne un nombre important de personnes, l'information peut être effectuée par une communication plus générale.

08 QU'EST CE QUE LE RGPD IMPLIQUE POUR NOTRE ADMINISTRATION ?

La nouvelle réglementation impose à chaque entité qui déploie des traitements de données personnelles de mettre en œuvre une organisation interne et les mesures permettant de garantir la protection des données personnelles.

En application de ce principe de responsabilité *(ou accountability)*, le responsable des traitements devra pouvoir justifier à tout moment des mesures prises, en tenant une documentation spécifique décrivant les mesures diligentées.

Diverses obligations lui sont imposées :

- nommer un délégué à la protection des données *(DPD ou DPO pour « data protection officer »),* chargé d'informer, de conseiller et de contrôler le respect du RGPD ; cette désignation est obligatoire pour les autorités et organismes publics ;
- tenir un registre des traitements à jour, cartographie exhaustive des traitements à caractère personnel mis en œuvre au sein de la structure ; identifier les traitements présentant un risque élevé ;
- réaliser, pour tout traitement identifié comme présentant un risque élevé, une analyse d'impact sur la protection des données *(AIPD ou PIA pour « privacy impact assessment »)* à même d'évaluer la conformité d'un traitement et de déterminer le cas échéant les mesures nécessaires pour assurer la protection des données ;
- intégrer dès la conception d'un traitement, et par défaut, les mesures appropriées pour protéger les données personnelles *(« protection dès la conception » et « protection par défaut »)* ;
- redéfinir ses relations contractuelles en précisant les obligations respectives du responsable de traitement et de ses éventuels sous-traitants, ces derniers assumant désormais une responsabilité propre ;
- sensibiliser et former ses personnels, adopter des codes de conduite, rédiger des procédures, faire réaliser des audits pour s'assurer de la bonne conformité de leurs pratiques avec le RGPD.

Le responsable des traitements a également l'obligation de notifier les violations de données à la CNIL et à la personne concernée *(si la violation fait peser un risque sur ses droits et libertés)* dans un délai de 72 heures.

09 ET LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES, QUEL EST SON RÔLE ?

Le délégué à la protection des données (DPD ou DPO pour data protection officer, selon le sigle anglais) est chargé d'une mission d'information et de conseil du responsable de traitement et des personnels qui procèdent aux opérations de traitement. Il est chargé de contrôler le respect du RGPD et des règles internes en matière de protection des données. A cet effet, il est consulté, donne son avis et formule des recommandations.

Il impulse la démarche en proposant toutes les mesures utiles au responsable de traitement, notamment en termes de sensibilisation et de formation des personnels.

Il fait office de point de contact avec la CNIL et coopère avec cet organisme le cas échéant.

Il rend compte de l'accomplissement de ses missions au responsable de traitement.

10 QUELLES SONT LES CONSÉQUENCES EN CAS DE NON RESPECT DE CES RÈGLES ?

Le non respect des règles de protection des données personnelles expose l'administration à des sanctions.

Ces sanctions sont de deux ordres.

Des sanctions administratives peuvent être prononcées par la CNIL. Elles dépendent de la gravité de la violation de données et peuvent atteindre 20 millions d'euros. La CNIL peut être saisie par les usagers ou agir de sa propre initiative.

Des sanctions pénales existent également. Elles font l'objet des articles 226-16 et suivants du code pénal.

Notamment, le fait de détourner des données de leur finalité, ainsi que le fait de divulguer à un tiers des informations qui pourrait porter atteinte à la considération d'une personne ou à l'intimité de sa vie privée sont punis de 5 ans d'emprisonnement et de 300 000 euros d'amende. La divulgation de données est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende si elle commise par négligence ou imprudence.

L'administration, personne morale, peut voir sa responsabilité engagée sur le fondement de l'article 131-38 du code pénal. Elle encoure alors une peine d'amende égale au quintuple de la peine prévue pour les personnes physiques.

Enfin, les agents publics peuvent également voir leur responsabilité engagée, suite à une plainte sur le terrain pénal tel qu'évoqué, ou sur le fondement disciplinaire si une faute professionnelle est caractérisée.

Pour contacter le DPO :
dpo@informatique.gov.pf

SERVICE DE L'INFORMATIQUE
DE LA POLYNESIE FRANCAISE

Déléguée à la protection
des données