Ximi by Xelya
MON EFFICACITÉ MULTIPLIÉE

Livre Blanc

Conformité des structures de services à la personne au RGPD : par quelles étapes devez-vous passer ?

Avril 2018

www.ximi.fr

LE RGPD APPLIQUÉ AUX STRUCTURES DE SERVICES À LA PERSONNE ET D'AIDE À DOMICILE

INTRODUCTION

Le nouveau règlement européen en matière de protection de la vie privée entre en vigueur le 25 mai 2018. Cette législation vient compléter l'ancienne loi « Informatique et Liberté » en fixant de nouvelles exigences concernant la protection de la vie privée.

Le RGPD - Règlement général sur la protection des données - (ou GDPR) définit un cadre autour des droits de chaque individu, de la sécurité et de la conformité relatifs à la protection des données.

Dans un contexte de Big Data, d'accroissement de données, de transmission et stockage de masse, le RGPD est une avancée majeure dans le respect de la vie privée et dans la manière dont les données doivent être utilisées.

Acteur du Cloud, Ximi est partie prenante de cette démarche. Depuis plusieurs mois maintenant, nous nous sommes appropriés le nouveau règlement et l'avons progressivement intégré à notre organisation et à l'ensemble de nos procédures.

Partant de notre expertise des systèmes d'information et de nos connaissances sur le RGPD, Ximi a décidé de mettre à disposition ce livre blanc pour vous permettre d'appréhender plus facilement les nouvelles obligations en matière de protection des données.

Dans le cadre de notre relation de partenariat, cet ouvrage a pour ambition de vous fournir des informations et de vous accompagner dans votre mise en conformité, il ne saurait se substituer aux conseils légaux d'un professionnel sur le sujet.
Nous ne garantissons pas que ce que nous communiquons est exhaustif. Suivre nos guidelines ne saurait garantir une conformité au RGPD qui relève in fine du responsable du traitement et de structure.

EDITO

Les grandes étapes du RGPD

Pour vous accompagner dans la mise en conformité au RGPD, Ximi vous propose de suivre pas à pas cette mise en conformité à travers huit étapes. Nous vous recommandons en parallèle de désigner une personne au sein de votre structure (cela peut être vous-même) responsable du pilotage de votre mise en conformité au RGPD.

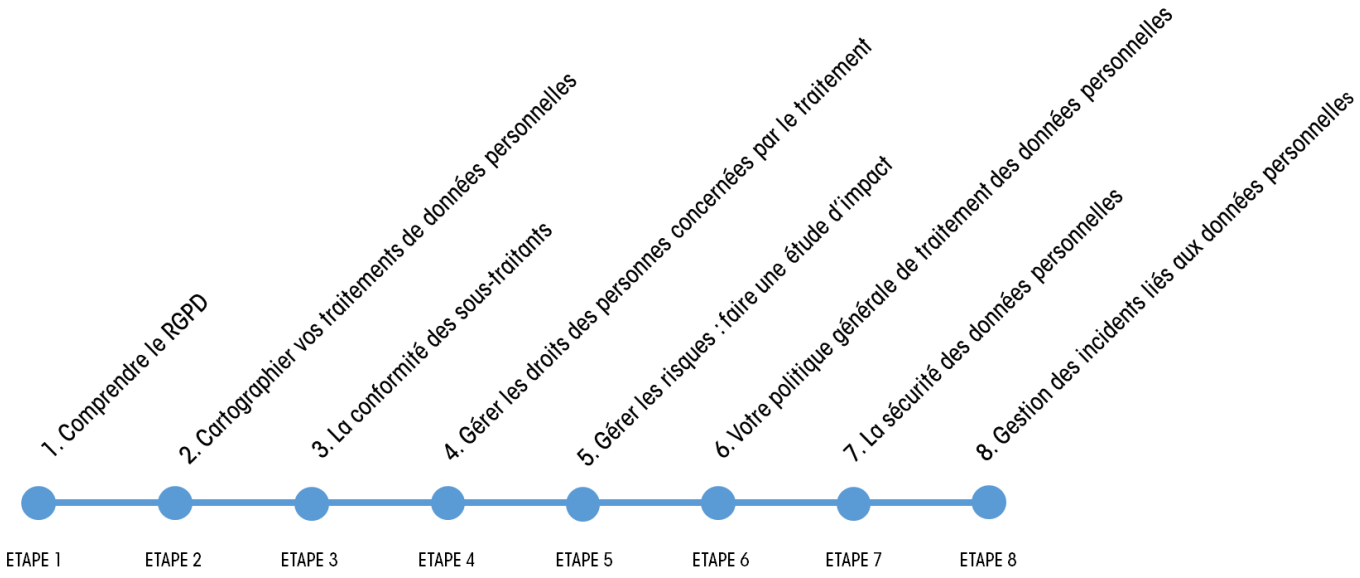

TABLE DES MATIÈRES

1. LES GRANDS PRINCIPES DU RGPD

La conformité au RGPD ne s'improvise pas. Pour bien vous préparer, la première étape consiste à faire un état des lieux de tous les acquis nécessaires pour atteindre au mieux l'objectif de la conformité, c'est-à-dire :

- Une connaissance des grands principes du RGPD
- Une vision claire des étapes clés qui amènent à la conformité de votre structure
- Une personne au sein de votre structure qui sera désignée comme référent RGPD

QU'EST-CE QUE LE RGPD ?

Le RGPD est le Règlement Général pour la Protection des Données entré en vigueur le 25 mai 2016 et dont l'application prendra effet le 25 mai 2018 dans tous les États-Membres de l'UE.

POUR QUOI ?

D'ici 2020, la quantité de données récoltées par les entreprises aura atteint 40 Zo (zettaoctets). Avec pareil déluge informationnel, elles ne savent plus quelles données elles détiennent, qui les contrôle et comment les traiter.
Le RGPD fixe un cadre renforcé et harmonisé de la protection des données personnelles en tenant compte des récentes évolutions technologiques (Big Data, Objets connectés, Intelligence Artificielle) et des défis qui accompagnent ces évolutions.

Le RGPD répond à 3 grands objectifs :

- Placer l'individu au cœur du dispositif légal et renforcer ses droits en matière de données personnelles.
- Responsabiliser les organisations quant à l'utilisation qu'elles ont des données personnelles
- Définir un cadre législatif commun à l'ensemble des pays européens

POUR QUI ?

Le RGPD s'applique à toutes les entités privées ou publiques qui traitent des données personnelles de citoyens européens.

Il s'adresse donc à vous en tant que structure de service à la personne et à l'ensemble de vos sous-traitants qui traitent vos données.

QUELLES CONSÉQUENCES EN CAS DE MANQUEMENT ?

À partir du 25 mai prochain, la CNIL sera en mesure de contrôler n'importe quelle organisation. C'est pourquoi il est important de se mettre en conformité avec le RGPD et de rester vigilant car une erreur ou négligence peut amener des conséquences importantes :

- La suspension du traitement sur les données
- De lourdes amendes administratives pouvant aller jusqu'à 20 millions d'euros d'amende ou 4% du chiffre d'affaires mondial de la structure.

Outre l'aspect financier, il est aussi important de comprendre que toute sanction, à plus forte raison si elle s'avère importante, risquerait de nuire énormément à la réputation et à l'image de votre structure, du fait d'un probable déficit de confiance de la part de vos clients ou bénéficiaires, salariés et partenaires.

QUEL IMPACT DANS VOTRE ACTIVITÉ QUOTIDIENNE ?

Qui dit règlement, dit obligations.

1) Pour être conforme au RGPD, vous devez être en mesure de cartographier l'ensemble de vos processus et de savoir où et à quel moment intervient le traitement des données.
2) Vous devez également assurer la conservation sécurisée des données utilisées.
3) Enfin, vous devez être en mesure de chercher, identifier, restaurer ou supprimer de manière définitive les données que vous détenez pour un individu.

Vous l'aurez compris, la conformité au RGPD passe par une (ré)organisation de votre système d'information avec la mise en place d'outils de gestion des données, la nomination d'un DPO (Data Protection Officer) et la mise en place de processus de sécurité.

Transformez vos obligations en opportunités !
Les conséquences du RGPD peuvent être vues comme très contraignantes pour le responsable du traitement (vous) et pour ses sous-traitants, mais elles sont aussi très positives.

Le RGPD donne la possibilité :

- À titre individuel, d'avoir la main sur ses données personnelles
- Au niveau de votre organisation, de gagner en transparence, en crédibilité et en confiance vis-à-vis de vos clients. Le RGPD c'est une nouvelle manière de créer du lien avec eux et de penser votre approche commerciale. Votre avantage concurrentiel ne sera plus de savoir traiter de la donnée en quantité mais d'avoir des échanges de qualité.

COMMENT ?

Le RGPD a été construit autour de 7 principes à respecter :

1/ Principe de responsabilité : La charge de la preuve de la conformité revient à l'organisation. Cela implique de documenter tous les processus et mesures mis en œuvre. **Ximi vous accompagne dans cette mise en conformité en tant que sous-traitant mais ne porte pas la responsabilité.**

2/ Principe de licéité : Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions du responsable du traitement .

3/ Principe de minimisation : Seules les données strictement nécessaires à la finalité du traitement peuvent être collectées.

4/ Principe de conservation limitée : les données personnelles ne peuvent être conservées que le temps nécessaire à l'exécution du traitement.

5/ Principe de sécurité par défaut : Toutes les mesures nécessaires à la sécurisation des données personnelles (confidentialité, intégrité, disponibilité) doivent être mises en place.

6/ Principe de sécurité dans la conception : La sécurité des données personnelles doit être prise en compte dès la phase de conception de toute activité.

7/ Principe d'information : Les personnes doivent être informées de leurs droits et consentir explicitement à la collecte et au traitement de leurs données personnelles. De plus, en cas de fuite de données, les personnes concernées ainsi que la CNIL doivent être prévenues dans un délai de 72h.

2. CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Il s'agit là de la première étape pour respecter vos nouvelles obligations et notamment vis-à-vis de vos clients. Pour ce faire, il s'agit de tenir une documentation interne complète sur vos traitements de données personnelles et de vous assurer que ces traitements respectent bien les nouvelles obligations légales.

Ce registre doit pouvoir être consulté à tout moment par la CNIL.

COMMENT FAUT-IL PROCÉDER ?

La notion de données personnelles est extrêmement large. Est considérée comme une donnée personnelle, toute information se rapportant à une personne physique identifiée ou identifiable.
Le Règlement ajoute qu'est ainsi réputée être une personne physique identifiable, une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant comme son 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.

À cela s'ajoute **la notion de données sensibles** qui sont des informations faisant référence aux origines raciales ou ethniques, à la religion, aux opinions politiques, philosophiques, syndicales, à la génétique, aux données biométriques, à la santé[1] ou à la sexualité des personnes.
Dans le cadre de cette étape, pour chaque donnée personnelle, vous allez devoir vous poser les questions suivantes :

- **QUI ?** Qui a accès aux données personnelles ? Cela signifie cartographier TOUS les acteurs, internes comme externes (liste des sous-traitants), qui ont accès à ces données.

- **QUOI ?** Comment sont utilisées les données personnelles ? Ici se posera la question des données sensibles comme les données relatives à la santé.

- **POURQUOI ?** Pour quoi faire ? Indiquer les finalités de la collecte de ces données. À titre d'exemple, pourquoi collectez-vous les numéros de Sécurité Sociale de certains de vos clients.

[1] *Les données de santé sont soumises à une réglementation particulière (Hébergement des Données de Santé, dit HDS).*

- **OÙ ?** Où sont ces données personnelles ? Il faut ici, déterminer les lieux physiques où sont hébergées les données personnelles et dans quel pays les données sont éventuellement transférées.

- **JUSQU'À QUAND ?** Il convient à ce stade, de préciser pour chaque catégorie de données, combien de temps vous souhaitez les conserver.

- **COMMENT ?** Comment sont traitées les données personnelles ? Quelles sont les mesures de sécurité que vous mettez en œuvre pour limiter les risques d'accès non autorisés à ces données. À titre d'exemple, l'une des premières mesures de sécurité est de mettre en place des mots de passe pour accéder aux ordinateurs.

3. LA CONFORMITÉ DES SOUS-TRAITANTS

En tant que structure de services à la personne, vous êtes le Responsable du Traitement et de ce fait responsable des données personnelles que vous avez collectées. Il est cependant rare de ne pas faire appel à un fournisseur pour l'hébergement et le traitement de ces données.

Dans votre démarche de mise en conformité au RGPD vous devez dès lors vous poser la question de vos sous-traitants. **Sont-ils eux-mêmes conformes ?**

Malheureusement, envoyer un mail laconique à son fournisseur en lui demandant qu'il vous confirme sa conformité n'est pas suffisant. En cas de contrôle, vous ne pourriez vous dédouaner en montrant que vous avez posé la question et n'avez pas reçu de réponse claire, voire pas de réponse du tout.

L'INVENTAIRE DES FOURNISSEURS

Il vous appartient de commencer par un recensement des fournisseurs concernés.
Les sous-traitants impliqués dans l'hébergement et le traitement des données peuvent être multiples. Si on pense en premier lieu à **l'éditeur du logiciel métier et au prestataire qui héberge et sauvegarde vos fichiers**, il ne faut pas oublier **l'hébergeur de vos mails**.
Qui n'a en effet jamais demandé à un client par mail des informations qui constituent des données personnelles.

- Vous demandez à votre client d'ultimes précisions le concernant pour évaluer ses besoins ? Votre boîte mail contient dès lors des données personnelles et vous devez vous poser la question de la conformité au RGPD de votre fournisseur.
- Vous stockez des fichiers sur des serveurs externalisés (Dropbox, Onedrive…) ? Vous transférez des données via une plateforme d'envoi (Wetransfer, Hightail, Free…). Il en va de même. Il vous appartient de vous assurer de la conformité de ces fournisseurs.

LE PRINCIPE DE CORESPONSABILITÉ

Le règlement européen instaure un **principe de coresponsabilité des sous-traitants** qui voient leurs obligations renforcées.
Ils doivent ainsi prendre en compte le principe de protection des données par défaut. Tout éditeur de logiciel digne de ce nom devra désormais dans la conception de nouvelles fonctionnalités inclure un volet RGPD dans sa réflexion.

Les sous-traitants sont également soumis à une **obligation de transparence et de traçabilité**.
Le temps du logiciel métier, boîte noire sur lequel vous ne disposez d'aucune information, est révolu. Vous êtes en droit de connaître et d'obtenir les mesures de sécurité appliquées par votre éditeur pour conserver et garantir l'intégrité des données que vous lui avez confiées.

Vos fournisseurs en lien avec les données personnelles ont également une **obligation d'assistance, d'alerte et de conseil**. Pas question qu'ils vous laissent seuls face à vos responsabilités. Ils sont désormais et plus que jamais acteurs à vos côtés avec le RGPD.

Les contrats en cours avec vos fournisseurs doivent-ils être modifiés ? La réponse est oui. Tous les contrats en cours d'exécution devront comprendre les clauses obligatoires prévues par le règlement européen.

Vous êtes client Ximi ? Pas d'inquiétude, nous avons tout prévu. Vous recevrez bientôt nos nouvelles Conditions Générales d'Utilisation des Services liées aux Données Personnelles qui intègrent ces nouvelles obligations.

Pour vous aiguiller dans votre conformité et si vos sous-traitants n'ont pas pris les devants, voici un avant-goût de questions que vous pourriez leur soumettre :

- Disposez-vous d'un registre des catégories d'activités de traitements réalisés pour le compte de vos clients ?
- Disposez-vous d'un DPO (Data Protection Office / Délégué à la Protection des Données) ?
- Faites-vous appel vous-même à des sous-traitants en lien avec les données que nous vous avons confiées ?
- Quelles garanties pouvez-vous nous apporter concernant leur conformité au RGPD ?
- Quelle information pouvez-vous me fournir pour réaliser mon étude d'impact ?
- Quelles sont vos procédures en cas de violation des données ?
- Quelle est votre Politique de Sécurité des Systèmes d'Information ?

4. GÉRER LES DROITS DES PERSONNES CONCERNÉES PAR LE TRAITEMENT

Comme nous l'avions introduit dans l'étape 1, le but du RGPD est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles. Autrement dit, ces derniers pourront désormais porter réclamation contre l'utilisation abusive de leurs données auprès d'une autorité unique. Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées.

LE DROIT À L'INFORMATION SUR LA COLLECTE DES DONNÉES

Avant même le traitement des données, il convient d'informer les personnes concernées du traitement de leurs données à caractère personnel. Une liste d'informations doit leur être obligatoirement communiquée et cette dernière peut figurer sur différents supports, comme notamment les documents contractuels, les documents de présentation de votre structure, au sein d'un courrier papier ou électronique, à travers des mentions dans le formulaire de contacts de votre site web, etc…
Vous devez alors obtenir le consentement explicite des personnes concernées par le traitement des données. Plus encore, la charge de la preuve du consentement vous revient. Enfin, la personne dont les données sont collectées peut retirer son consentement à tout moment.

Nous vous conseillons dans cette étape de :

- Formaliser un process qui sera utilisable pour tout nouveau projet nécessitant une collecte de données à caractère personnel
- Rédiger une bibliothèque de mentions d'information type afin de disposer de modèles uniformes et réutilisables
- Identifier les supports permettant de communiquer l'information aux personnes concernées par la collecte

En résumé : vous informez de l'existence d'un traitement, vous obtenez le consentement express des personnes concernées par le traitement et vous êtes capables d'en apporter la preuve.

LES DROITS D'ACTIONS SUR LA COLLECTE DES DONNÉES

Une fois le traitement mis en œuvre, vous devez pouvoir répondre aux demandes des personnes concernées. En effet, au-delà du droit à l'information que nous avons abordé ci-dessus, les personnes disposent du droit de vous demander d'effectuer certaines actions à leur profit.

Les droits dont disposent l'ensemble de vos clients sont les suivants :

- **Le droit d'accès** auxdites données, par la communication d'une copie.
- **Le droit d'obtenir** la rectification des informations inexactes ou incomplètes.
- **Le droit à l'oubli** c'est-à-dire le droit d'obtenir l'effacement de ses données, notamment lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles avaient été collectées.
- **Le droit à la limitation du traitement** c'est-à-dire le droit à la suspension du traitement, par exemple dans le cas d'une contestation par la personne concernée sur l'exactitude des données, vous permettant d'effectuer les vérifications adéquates.
- **Le droit à la portabilité** c'est-à-dire que la personne concernée a le droit d'obtenir les données qu'elle vous a fournies, dans un format structuré et couramment utilisé, et a le droit de transmettre ces données à un autre responsable de traitement.
- **Le droit d'opposition** au traitement qui permet à la personne concernée de vous demander de ne plus traiter ses données (exemple = droit d'opposition à la prospection).

COMMENT TRAITER CES DEMANDES ?

Toute demande doit faire l'objet d'une réponse respectant certaines modalités :

- **Délai :** un mois maximum à compter de la réception de la demande. La personne concernée pourra introduire une réclamation auprès d'une autorité de contrôle en cas de refus de réponse de votre part.
- **Format :** la réponse doit être concise, transparente, compréhensible, en des termes clairs et simples. Elle peut être apportée par écrit ou par voie électronique.

Nous vous conseillons de formaliser une procédure de gestion et de traitement des demandes d'exercice de leurs droits par les personnes concernées.

5. GÉRER LES RISQUES EN RÉALISANT UNE ANALYSE D'IMPACT

Dans le cadre de votre activité, le traitement des données est susceptible d'engendrer un risque élevé pour les droits et liberté des personnes, et ce, compte tenu de la nature, de la portée et du contexte des finalités du traitement.
C'est pour cette raison que la réalisation d'une analyse d'impact est nécessaire. Il faut toutefois garder en tête que la réalisation de l'analyse d'impact relève d'un processus continu et n'est pas un exercice ponctuel.

EN QUOI CONSISTE L'ÉTUDE D'IMPACT ?

L'analyse d'impact vise à évaluer la probabilité et la gravité du risque afin de déterminer, à partir du résultat de cette dernière, les mesures appropriées à prendre afin de prouver que le traitement des données à caractère personnel est conforme au RGPD.
En résumé, elle vise à assurer la conformité aux règles et à pouvoir en apporter la preuve.

QUE CONTIENT CETTE ANALYSE ?

- La description systématique du traitement envisagé, sa finalité
- L'étude des mesures existantes ou prévues, d'une part pour respecter les exigences légales et d'autre part, pour traiter les risques sur la vie privée
- L'évaluation des risques pour les droits et les libertés des personnes concernées
- Les mesures envisagées pour remédier aux risques

COMMENT RÉALISER CETTE ANALYSE ?

- La description systématique du traitement envisagé

Il convient à ce stade de décrire les traitements considérés, les responsabilités liées aux traitements et de décrire les supports des traitements

Pour illustrer ce point, vous trouverez ci-dessous des exemples de DCP par catégorie :

- Données à caractère personnel courantes : État civil, identité, vie personnelle (habitudes de vie, situation familiale …), revenus, données de connexion, données de localisation

- Données à caractère personnel sensibles : Numéro de sécurité sociale, données bancaires, opinions religieuses, vie sexuelle, données de santé, origine raciale, infractions, condamnations …

Il faut savoir que les supports de données à caractère personnel sont les composants du système d'information sur lesquels reposent les données à caractère personnel, à titre d'exemple :

- Système informatiques : Matériel (PC, clés USB), Logiciels (Systèmes d'exploitation, messagerie, base de données, applications métier), Canaux informatiques (Câbles, Wifi …)
- Organisations : Personnes (utilisateurs par exemple), Supports papier (Impressions, photocopies etc…), Canaux de transmission papier (envoi postal …)

- L'étude des mesures

Il convient de présenter les mesures de nature juridique (droits des personnes et informations à leur fournir) existantes ou prévues pour respecter les exigences légales ainsi que les mesures destinées à traiter les risques.

Exemples :

- Mesure de nature juridique => Comment obtenez-vous le consentement des personnes concernées ?
- Mesure organisationnelle => Comment gérez-vous votre supervision ? (Audits, tableaux de bord …)
- Mesure de sécurité logique => Comment sont gérés les postes de travail ?
- Mesure de sécurité physique => Comment sont sécurisés les documents papier dans vos agences ?

- L'étude des risques

Pour une meilleure identification et analyse, il faut décomposer le risque en deux parties :

- D'un côté on évalue ce que l'on craint sur les traitements (perte, divulgation …) et le niveau de gravité de ces évènements
- De l'autre on évalue les menaces et leur source ciblant les supports des traitements et pouvant mener aux évènements redoutés

Il existe plusieurs types de sources de risques :

- Les sources humaines internes agissant accidentellement ou de manière délibérée,
- Les sources humaines externes (Les prestataires, les anciens collaborateurs, les confrères, les clients …) agissant accidentellement ou de manière délibérée,
- Les sources non humaines (virus, catastrophes naturelles, animaux …) internes et externes.

À partir de là, se pose alors la question des évènements redoutés :

- L'accès illégitime aux DCP avec, par exemple, l'exploitation de ces dernières à d'autres fins que celles prévues (ex : fins commerciales, usurpation d'identité …)
- La modification non désirée des DCP dans un objectif d'exploitation (ex : changement de la relation entre l'identité des personnes et les données biométriques d'autres personnes …)
- La disparition des DCP avec pour conséquence un blocage (ex : impossibilité de plaider à cause de la disparition des conclusions…)

- La décision

Cela consiste à valider le choix des mesures existantes et prévues permettant de traiter les risques. Cela sous-entend que si les mesures ne sont pas suffisantes, un plan d'actions est alors défini pour en proposer des nouvelles. L'analyse est alors révisée pour prendre en compte ces nouveaux paramètres, et ce, jusqu'à ce que les niveaux de risques permettent de prendre la décision de les accepter.

6. LA POLITIQUE GÉNÉRALE DE TRAITEMENT DES DONNÉES PERSONNELLES

En matière de politique générale de traitement des données personnelles, le RGPD énonce plusieurs grands principes.

LE PRINCIPE DE MINIMISATION

Vous ne devez collecter que ce qui est strictement nécessaire.
Le principe est très simple d'application, notamment si vous faites un audit de votre existant : pouvez-vous justifier de la finalité des informations que vous avez demandées ? La réponse est non ? Il est temps de supprimer ces données.

LE PRINCIPE DE LIMITATION DE L'ACCÈS AUX DONNÉES :

Ce sujet est rarement adressé dans sa globalité.
Si les salariés d'une organisation ont le réflexe de limiter l'accès aux données financières de leur organisation il est rare qu'une politique interne globale de droits d'accès aux données soit mise en place. Le RGPD vous y contraint.

Par exemple : en quoi les documents originaux de vos clients sont-ils utiles une fois que le dossier est classé ? En rien justement.
Ou encore les accès aux coordonnées financières de vos clients sont-ils bien limités dans votre logiciel métier ? Si votre réponse est incertaine alors vous devez vous mettre en conformité.

Ximi, via sa fonctionnalité de gestion des permissions vous facilite cette conformité. Nous proposons la mise en place de profils type (gérant, chargé de planning, assistante, etc).
Au prochain recrutement, il suffira de sélectionner le profil de permissions adéquat et tout sera en place et homogène.

LE PRINCIPE DE PROTECTION PAR DÉFAUT

Toutes les organisations sont soumises à ce principe, y compris votre prestataire de logiciel métier. Ximi, en tant qu'éditeur, ne développe plus de fonctionnalité sans s'interroger au préalable sur sa conformité au RGPD.
De votre côté, Vous avez l'habitude de laisser vos dossier papiers sur votre bureau le soir en partant ? Maitrisez-vous vraiment qui accède à votre bureau ? Quels sont les engagements de confidentialité de la personne qui vient faire le ménage ?

LA DURÉE DE CONSERVATION DES DONNÉES

Un autre sujet primordial à adresser est la durée de conservation des données. La loi ne précise aucune durée en tant que telle mais pose un principe général. La durée de conservation que vous définissez doit pouvoir être justifiée au regard de la durée du traitement et de sa finalité. Si l'un de vos salariés ne fait plus partie de vos effectifs, vous allez évidemment conserver les données de paie le concernant pour toute la durée sur laquelle un contrôle URSSAF pourrait porter.

Sachez que la CNIL a édité une matrice des durées de conservation en fonction des données concernées. Une fois votre politique de durée de conservation définie, encore faut-il la mettre en œuvre.

LA CHARTE INFORMATIQUE

Enfin, la mise en conformité au RGPD est l'occasion de mettre en place une charte informatique si vous n'en avez pas déjà. Vous définirez ainsi les bonnes pratiques attendues en interne. Si le projet de mise en conformité au RGPD doit être porté par un chef de file, il ne peut ni ne doit agir seul.
Le RGPD doit se vivre au quotidien et est l'affaire de tous. Organiser en interne une sensibilisation au sujet et une formation aux process de travail adéquats avec une feuille de présence émargée que vous pourrez présenter en cas de contrôle fait partie de la démarche de mise en conformité.

7. LA SÉCURITÉ DES DONNÉES PERSONNELLES

Avant même l'arrivée du RGPD, la sécurité des données personnelles a toujours été un volet essentiel de la conformité à la loi Informatique et Libertés. Mais aujourd'hui, nous sommes face à un renforcement des obligations avec le RGPD qui nous oblige à accentuer nos précautions élémentaires en terme de sécurité.

Pour information, l'article 32 du règlement européen indique que : « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

En tout, la CNIL référence une liste d'actions à mener en termes de sécurité, dont :

SENSIBILISER LES UTILISATEURS

En tant que responsable de traitement des données personnelles, vous devez informer les utilisateurs des mesures prises pour traiter les risques.

Comment ?
En documentant les procédures d'exploitation et en rédigeant une charte informatique.

AUTHENTIFIER LES UTILISATEURS

Il est primordial de cloisonner les accès aux données et de les maîtriser.

Comment ?
En vous assurant qu'un utilisateur est doté d'un identifiant qui lui est propre et qu'il doit obligatoirement s'identifier avant toute utilisation des moyens informatiques. Il est également préconisé de limiter le nombre de tentatives d'accès aux comptes utilisateurs sur les postes de travail et d'imposer un renouvellement du mot de passe.

GÉRER LES HABILITATIONS

Ce point est central dans votre politique de sécurité des données. Il s'agit de limiter les accès aux seules données dont un utilisateur a besoin.

Comment ?
Les précautions de base à prendre sont de définir les profils d'utilisation afin de limiter les accès des utilisateurs aux seules données strictement nécessaires à leurs missions, et

également de supprimer les permissions d'accès des utilisateurs notamment dès la fin de leur contrat.
Attention : il ne faut jamais laisser un nouvel arrivant utiliser la licence d'accès de quelqu'un qui vient de partir.

TRACER LES ACCÈS ET GÉRER LES INCIDENTS

Vous avez pour responsabilité de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles.
Comment ?
En mettant en place un dispositif de gestion des traces et des incidents. Il faut alors prévoir un système de journalisation des activités des utilisateurs, des anomalies et des évènements liés à la sécurité.

SÉCURISER LES POSTES DE TRAVAIL

L'infogérance des postes de travail de l'ensemble de vos collaborateurs doit être au cœur de la réflexion de mise en conformité RGPD. En effet, les risques d'intrusion dans les systèmes informatiques sont importants et le principal point d'entrée est le poste de travail.

Comment ?
Certaines précautions élémentaires sont à prendre : mécanisme de verrouillage automatique de session, installation d'un « pare-feu », anti-virus et mises à jour régulières, sauvegarde régulière des espaces de sauvegarde et limiter la connexion de supports mobiles.

SÉCURISER L'INFORMATIQUE MOBILE

Les utilisateurs de nos jours multiplient les outils de communication (PC portables, clés USB, Smartphones) ce qui rend indispensable l'anticipation des vols ou pertes de ces équipements.

Comment ?
En sensibilisant les utilisateurs à ces risques via des procédures liées à l'utilisation d'outils informatiques mobiles, en mettant en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades et en prévoyant des moyens de chiffrement de ces derniers.

PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE

Vous devez impérativement protéger votre réseau informatique interne et autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

Comment ?
En limitant les accès Internet, en gérant vos réseaux Wi-Fi et en imposant un VPN pour les accès à distance.

SÉCURISER LES SERVEURS

Il faut avoir conscience que les serveurs centralisent un grand nombre de données. C'est pour cette raison que la sécurité de ces derniers doit être votre priorité.

Comment ? En limitant l'accès aux outils d'administration aux seules personnes habilitées, en adoptant une politique spécifique de mots de passe pour les administrateurs, en installant des mises à jour et en effectuant des sauvegardes.

SÉCURISER LES SITES WEB

Votre rôle est de vous assurer des bonnes pratiques appliquées aux sites web.
Comment ?
En mettant en œuvre le protocole TLS[2] sur tous les sites web, en limitant les ports de communication et si des cookies non nécessaires au service sont utilisés, il faut recueillir le consentement.

SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ

La limitation de l'impact d'une disparition non désirée des données doit être au cœur de votre politique de sécurité.

Comment ?
Pour cela, vous devez réaliser et tester régulièrement des sauvegardes et des copies de ces dernières : ces sauvegardes doivent être fréquentes, stockées sur un site extérieur et protégées au même titre que les serveurs d'exploitation. Nous vous conseillons de tester régulièrement la restauration des sauvegardes.

ENCADRER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES

Vous devez vous assurer que les opérations de maintenance sont encadrées pour être en maîtrise de l'accès aux données par les prestataires externes.

Comment ?

[2] TLS : protocole de sécurisation des échanges internet très largement utilisé

Il est nécessaire d'enregistrer les interventions de maintenance dans une main courante et de supprimer de façon sécurisée les données des matériels avant leur mise au rebut.

GÉRER LA SOUS-TRAITANCE

Ce point a été abordé au chapitre 3 de ce livre blanc, à savoir la rédaction d'un contrat avec les sous-traitants qui définit l'objet, la durée, la finalité du traitement et les obligations des parties.

PROTÉGER LES LOCAUX

Dans le cadre de votre politique de sécurité, la question de la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux se pose. Il faut que l'accès aux locaux soit contrôlé.

Comment ?
En installant des alarmes anti-intrusion et en mettant en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies. Il est également vivement conseillé de protéger physiquement le matériel informatique par des moyens spécifiques comme la redondance d'alimentation électrique par exemple.

ENCADRER LES DÉVELOPPEMENTS INFORMATIQUES

Si vous êtes amenés à effectuer des développements informatiques, la sécurité et la protection de la vie privée doivent être intégrés au plus tôt dans les projets, c'est-à-dire dès la conception.

Comment ?
En effectuant ces développements et tests dans un environnement informatique distinct de celui de la production (par exemple sur une réplication) et sur des données fictives ou anonymisées.

Comme vous pouvez le constater, la sécurité des données personnelles demande un certain nombre de précautions à prendre. En tant que partenaire, Ximi peut vous faciliter la tâche en vous proposant une offre d'infogérance complète :

- Contrôleur de domaine
- Gestion des mots de passe avec règles de sécurité
- Connexion par tunnels encryptés (VPN IPSec)
- Anti-virus
- Gestion des mises à jour Windows
- Firewall

8. LA GESTION DES INCIDENTS LIÉS AUX DONNÉES PERSONNELLES

Le RGPD prévoit également une obligation d'informer les autorités compétentes en cas d'incidents sur les données collectées (CNIL, ANSSI, agences régionales de santé). Pour cela, il est indispensable de se préparer à cette éventualité et mettre en place des bonnes pratiques au sein de votre organisation.

QU'EST-CE QU'UN INCIDENT ?

Un incident de sécurité se caractérise par tout événement qui ne fait pas partie du fonctionnement normal d'une organisation et qui entraine une réduction ou une interruption de la qualité de service ou qui peut compromettre la sécurité informatique.
Dans le cadre du RGPD, il peut être identifié comme une opération de fuite ou de perte de données personnelles.

POURQUOI METTRE EN PLACE UNE GESTION DES INCIDENTS ?

En règle générale, la gestion des incidents informatiques permet d'assurer la reprise de l'activité le plus rapidement possible et garantit que l'impact sur le business soit réduit au minimum pour une organisation.
Pour le RGPD, l'enjeu est aussi de protéger au maximum les individus dont les données personnelles auraient été utilisées.

La gestion des incidents donne lieu à la mise en place d'un (ou de plusieurs) processus qui doit/doivent être réfléchi(s), testé(s) et amélioré(s) en amont d'une éventuelle difficulté.
C'est dans cet outil que l'obligation d'informer les autorités de régulation doit figurer.

COMMENT METTRE EN PLACE UNE GESTION DES INCIDENTS ?

Au sein de votre organisation, vous devez être en mesure de définir une gestion des incidents tenant compte des ressources et des outils techniques dont vous disposez.

Il conviendra de respecter 5 étapes clés :

- **Planifier et préparer**

Cette étape consiste à identifier l'ensemble de vos ressources internes et externes qui pourraient être impliquées dans la gestion des incidents, de formaliser cette liste et de la tenir à jour.

Par exemple, il peut s'agir des salariés de votre organisation, de la personne en charge de la sécurité des systèmes d'information, de vos prestataires de services informatiques, des personnes en charge de la communication etc.

- **Détecter et signaler**

À cette étape, il est nécessaire de définir les moyens de veille et les outils d'alerte qui permettent de détecter et d'avertir sur l'arrivée d'un incident.
À travers un dispositif de veille, les menaces actuelles sont analysées via des sources internes ou externes (fournisseurs, ANSSI, ASIP, IRT, CERT[3]) ou des fils RSS.
À travers un dispositif de détection et de remontée d'alertes, les activités anormales, suspectes ou malveillantes sont identifiées.

Cette analyse, automatisée, a pour objectif de définir la typologie de l'incident avant de réagir.

- **Évaluer et décider**

Une fois la détection et l'analyse faites et l'incident avéré, la troisième étape du processus consiste à qualifier l'incident pour ainsi déterminer quelle(s) autorité(s) devra/devront être sollicitée(s) entre les agences régionales de santé, l'ANSSI ou la CNIL.

En cas de violation de données personnelles, le RGPD oblige à documenter l'incident, c'est-à-dire l'intégrer dans un registre dans lequel seront consignés les faits de la violation, ses conséquences et les actions prises pour y remédier.

- **Répondre**

L'incident doit être résolu le plus vite possible pour que les conséquences soient minimes. Votre organisation doit alors mettre en place des actions de secours quitte à ce que les mesures prises soient temporaires.
Vous devez notifier l'incident (en fonction de sa typologie) aux autorités compétentes à travers les formulaires de notification mis en place[4].

Dans le cadre du RGPD et si une violation de données est confirmée, votre structure doit systématiquement informer la CNIL en lui fournissant les éléments suivants :

- La description de la nature de la violation de données à caractère personnel ;
- Les catégories de données ;
- Le nombre approximatif de personnes concernées par la violation ;
- Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

[3] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), ASIP (Agence des Systèmes d'Information Partagés de santé), IRT (Incident Response Team), CERT (Computer Emergency Response Team)
[4] CNIL : https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf
ANSSI : https://www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf
ARS : formulaire en ligne bientôt disponible

- Le nom et les coordonnées du référent qui dans votre structure est en charge de la protection des données ;
- La documentation liée à l'incident (faits, conséquences et actions réalisées)

Vous devez également informer les personnes concernées par l'incident.

- **Tirer les enseignements**

Enfin, comme dans chaque gestion d'incident, une dernière étape de prévention est requise. Le but est de faire en sorte que l'incident ne se reproduise plus en corrigeant les failles du système qui ont permis que l'incident arrive et en optimisant les mesures prises pour les rendre encore plus efficaces.

9. ETES-VOUS CONFORME ?

Nous avons bien conscience que la conformité au RGPD est un processus long. Pour autant, nous vous conseillons de l'inscrire dans une réelle démarche d'amélioration continue. Le RGPD vous demande une remise en question permanente sur votre politique de traitement des données personnelles.

Si vous n'êtes pas encore entièrement conforme, il n'est pas trop tard.
La mise en conformité au RGPD est un processus continu. Dans tous les cas, il faudra donc l'entretenir et mettre à jour les documents et les processus de sécurité en fonction de la vie de votre organisation et des évolutions technologiques ou réglementaires.

Et après le 25 mai ?
La CNIL ne s'annonce pas lorsqu'elle contrôle une entreprise ou une association. Pour prouver votre conformité, tenez votre documentation à portée de main pour pouvoir la présenter à tout moment :

- Registre de traitements
- Étude d'impacts
- Contrats avec les sous-traitants concernés
- Modèles de recueil de consentement des personnes concernées
- Procédures mises en place pour l'exercice des droits des personnes concernées
- Procédures internes de sécurisation et de communication en cas de violation des données

N'oubliez pas que le RGPD est une véritable opportunité pour développer votre activité !
Dans une société connectée, où les échanges sont dématérialisés, la protection des données est un moyen de remettre l'individu au cœur de sa stratégie. L'effort notable de mise en conformité avec la législation que vous effectuerez doit être communiqué auprès de vos clients, de vos salariés et de vos partenaires.
C'est la garantie d'une meilleure protection de leurs droits et d'échanges plus transparents et sécurisés. C'est un véritable atout !
Ceci dit, le grand public n'étant pas encore très familiarisé avec le RGPD, ne vous contentez pas d'ajouter une mention « conforme au RGPD », au contraire : valorisez les démarches accomplies en termes de processus de recueil des données, de sécurité, de droits d'accès, etc.

D'autre part, La conformité au RGPD est aussi un moyen pour vous de reprendre le contrôle sur les données que vous collectez et utilisez. Vous maîtrisez mieux désormais le type de données collectées, ainsi que leur stockage. Il va donc être plus facile de les utiliser à bon escient.

BESOIN D'UN CONSEIL PERSONNALISÉ ?

Matinée Ximi – Microsoft

Inscrivez-vous à la matinée consacrée au RGPD appliqué aux structures de services à la personne et d'aide à domicile.

Table ronde :
Le RGPD et la sécurité dans le cloud : quelle approche doivent avoir les structures de services à la personne ?

Intervenants :

Diane Bouchet (DPO – Xelya)
Maxime Legas (RSSI – Xelya)
Olivier Péraldi (DF – FESP)
Sylvain Denis (DSI – APEF)
Carelle Robinet (Chef produit sécurité – Microsoft)

LE VENDREDI 15 MAI 2018
– DE 9H À 13H –
Chez Microsoft
39 Quai du Président Roosevelt
Issy les Moulineaux, 92130

Inscription contact@xelya.com

Renseignements :

Anaïs Panhkham

Responsable Communication
au **01 73 28 33 48**
ou par mail **anais.panhkham@xelya.com**

ou rendez-vous sur **http://www.ximi.fr/evenement-microsoft-sap-2018/**