LETTRE SOCIALE N°4/18

13 avril 2018 – SECURISATION DES DONNEES PERSONNELLES INFORMATIQUES

LETTRE SOCIALE

Nous contacter

Maître Stéphane FABING
245, rue d'Epargnemailles
02100 SAINT-QUENTIN
☎ 03.23.05.78.40
✉ maitre.fabing.avocat@wanadoo.fr

Le règlement européen sur la protection des données personnelles **(RGPD)** entrera en vigueur le 25 mai 2018. Ce règlement précise que la protection des données personnelles nécessite de prendre des *« mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »* (règlement 2016/679 du 27 avril 2016, art. 32).

En réalité, la loi « Informatique et libertés » impose déjà cette obligation : *« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »* (loi 78-17 du 6 janvier 1978, art. 34).

Si le RGPD ne crée pas ici une règle nouvelle, il alourdit la sanction encourue en cas de non-respect de la règle. Ainsi, à compter du 25 mai 2018 le responsable du traitement de données personnelles qui n'aura pas pris les mesures nécessaires pour garantir leur sécurité encourra une amende allant jusqu'à 10.000.000 Euros, voire jusqu'à 2 % de son chiffre d'affaires annuel mondial (règlement 2016/679 du 27 avril 2016, art. 83, § 4). Actuellement, le plafond de la sanction pécuniaire est de 3.000.000 Euros (loi 78-17 du 6 janvier 1978, art. 47), ce qui n'est déjà pas rien.

Les thématiques traitées par ce règlement européen sont les suivantes :

- transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée,
- informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée,
- informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée,
- droit d'accès de la personne concernée au traitement informatisé de ses données personnelles,
- droit de rectification,
- droit à l'effacement (« droit à l'oubli »),
- droit à la limitation du traitement,
- obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement,
- droit à la portabilité des données,
- droit d'opposition et prise de décision individuelle automatisée,

I. Rédiger une charte informatique

- *Informations à donner aux salariés*

Bon nombre d'entreprises ont d'ores et déjà adopté une charte informatique mais, ainsi que la CNIL le souligne, celles qui ne l'ont pas fait doivent franchir le pas.

Il faut également penser à donner à cette charte une force contraignante, en l'intégrant ou l'annexant au règlement intérieur.

La charte informatique a la même valeur que le règlement intérieur si elle est adoptée en respectant les formalités et les règles de fond applicables au règlement intérieur (par exemple, consultation préalable des représentants du personnel). Si elle est insérée au règlement intérieur, cela implique que celui-ci soit modifié suivant les prescriptions du Code du travail.

Selon la CNIL, cette charte devrait, au moins, comporter les informations suivantes :

- le rappel des règles de protection des données et les sanctions encourues en cas de non-respect ;
- les modalités d'intervention des équipes chargées de la gestion des ressources informatiques dans l'entreprise ;
- les moyens d'authentification utilisés par l'entreprise ;
- les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition (poste de travail, équipements nomades, espaces de stockage individuel, réseaux locaux, Internet, messagerie électronique et téléphonie) ;
- les conditions d'utilisation des dispositifs personnels ;
- les conditions d'administration du système d'information et l'existence, le cas échéant, de systèmes automatiques de filtrage, systèmes automatiques de traçabilité et gestion du poste de travail ;
- les sanctions encourues en cas de non-respect de la charte.

- *Obligations et interdictions à imposer aux salariés*

La charte doit préciser les obligations imposées aux salariés au titre de la protection des données personnelles. La CNIL cite l'obligation de :

- signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
- verrouiller son ordinateur dès que l'on quitte son poste de travail ;

- respecter certaines procédures (par exemple, demander l'accord d'un supérieur hiérarchique) afin d'encadrer certaines opérations (par exemple, la copie de données sur des supports amovibles).

La charte listera également les interdictions faites aux salariés, et la CNIL mentionne, à ce titre, l'interdiction de :

- confier ses identifiant et mot de passe à un tiers ;
- copier, installer, modifier ou détruire des logiciels sans autorisation ;
- supprimer des informations si cela ne relève pas des tâches incombant au salarié.

II. Prévoir une clause de confidentialité dans les contrats de travail

La CNIL demande aux entreprises de faire signer aux salariés un engagement de confidentialité lorsqu'ils sont amenés à manipuler des données personnelles et pour laquelle nous restons à votre disposition.

III. Insérer une clause de sécurité dans les contrats de maintenance

Les opérations de maintenance doivent être encadrées pour maîtriser l'accès aux données par les prestataires.

La CNIL souligne que les interventions de maintenance doivent être enregistrées dans une main courante et qu'une procédure de suppression sécurisée des données doit être mise en place.

Par ailleurs, la CNIL engage les entreprises à prévoir une clause de sécurité dans leurs contrats de maintenance.

IV. Gérer la sous-traitance

- *Garanties à exiger*

Les données communiquées à (ou gérées par) des sous-traitants doivent bénéficier de garanties suffisantes.

La CNIL insiste auprès des entreprises pour qu'elles ne fassent appel qu'à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources) et qu'elles exigent du sous-traitant la communication de sa politique de sécurité des systèmes d'information.

Nous contacter

Maître Stéphane FABING
245, rue d'Epargnemailles
02100 SAINT-QUENTIN
☎ 03.23.05.78.40
✉ maitre.fabing.avocat@wanadoo.fr

De plus, les entreprises doivent prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données. Ces garanties incluent notamment :

- le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées ;

- le chiffrement des transmissions de données (ex. : connexion de type HTTPS, VPN, etc.) ;

- des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.

Vous en souhaitant bonne réception, veuillez agréer, Madame, Monsieur, l'expression de mes sentiments dévoués.

Stéphane FABING

ANNEXE

REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES PERSONNELLES

Se préparer en 6 étapes

Etape 1 : Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données.

La désignation d'un délégué à la protection des données est obligatoire en mai 2018 si :

- vous êtes un organisme public,
- vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et à des infractions.

Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne, disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.

Le rôle du délégué à la protection des données

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés,
- de contrôler le respect du règlement et du droit national en matière de protection des données, de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution,
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

- informer sur le contenu des nouvelles obligations,
- sensibiliser les décideurs sur l'impact de ces nouvelles règles,
- réaliser l'inventaire des traitements de données de votre organisme, concevoir des actions de sensibilisation,
- piloter la conformité en continu.

Etape 2 : Cartographier vos traitements de données personnelles

Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point.

Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du règlement sur votre activité et de répondre à cette exigence, vous devez au préalable recenser précisément :

- les différents traitements de données personnelles,
- les catégories de données personnelles traitées,
- les objectifs poursuivis par les opérations de traitement de données,
- les acteurs (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants,
- les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Etape 3 : Prioriser les actions

Sur la base du registre des traitements de données personnelles, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement.

Points d'attention quels que soient les traitements de données

- Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées,
- Identifiez la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale),
- Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement,
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées,
- Prévoyez les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement…),
- Vérifiez les mesures de sécurité mises en place.

Points d'attention nécessitant une vigilance particulière

Vous traitez certains types de données :

- des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- des données relatives à la santé ou l'orientation sexuelle,
- des données génétiques ou biométriques,
- des données d'infraction ou de condamnation pénale,
- des données concernant des mineurs.

Votre traitement de données personnelles a pour effet :

- la surveillance systématique à grande échelle d'une zone accessible au public,
- l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Vous transférez des données hors de l'Union européenne ?

- vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne,
- dans le cas contraire, encadrez vos transferts.

Etape 4 : Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

L'étude d'impact sur la protection des données permet :

- de bâtir un traitement de données personnelles ou un produit respectueux de la vie privée,
- d'apprécier les impacts sur la vie privée des personnes concernées,
- de démontrer que les principes fondamentaux du règlement sont respectés.

Quand mener une étude d'impact sur la protection des données (PIA) ?

- avant de collecter des données et de mettre en œuvre le traitement,
- sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

Que contient une étude d'impact sur la protection des données (PIA) ?

- une description du traitement et de ses finalités,
- une évaluation de la nécessité et de la proportionnalité du traitement,
- une appréciation des risques sur les droits et libertés des personnes concernées,
- les mesures envisagées pour traiter ces risques et se conformer au règlement.

Les outils pour vous aider

La CNIL met à votre disposition sur son site les guides PIA, catalogues de bonnes pratiques qui vous aident à déterminer les mesures proportionnées aux risques identifiés.

Etape 5 : Organiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles (par exemple : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire etc.).

Organiser les processus implique notamment de :

- prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durées de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données) ; pour cela, appuyez-vous sur les conseils du délégué à la protection des données,

- sensibiliser et d'organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs,
- traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen),
- anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

Etape 6 : Documenter la conformité

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les mesures organisationnelles et techniques sont réexaminées et actualisées si nécessaire.

Votre dossier devra notamment comporter les éléments suivants :

La documentation sur vos traitements de données personnelles

- le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants),
- les analyses d'impact sur la protection des données (PIA ; *voir étape 4*) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes,
- l'encadrement des transferts de données hors de l'Union européenne (notamment les clauses contractuelles types ou les BCR).

L'information des personnes

- les mentions d'information,
- les modèles de recueil du consentement des personnes concernées,
- les procédures mises en place pour l'exercice des droits des personnes.

Les contrats qui définissent les rôles et les responsabilités des acteurs

- les contrats avec les sous-traitants,
- les procédures internes en cas de violations de données,
- les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.