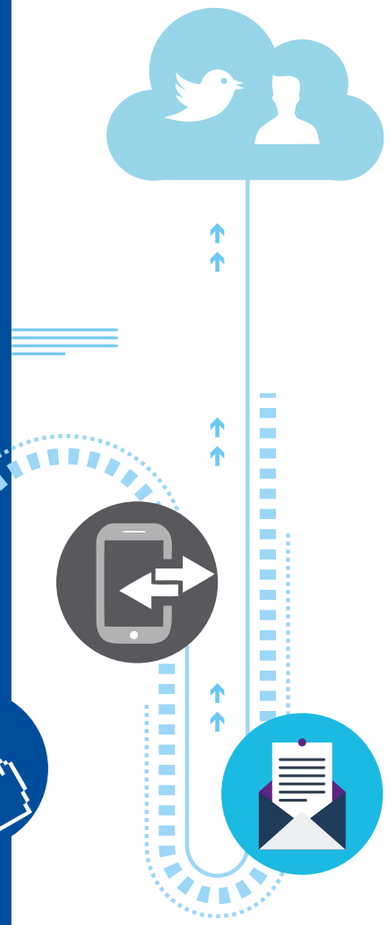
RGPD

LE COMPRENDRE ET L'APPLIQUER

Septembre 2018

CCI PARIS ILE-DE-FRANCE



SOMMAIRE

Pour plus de détails, cliquez sur les **mots en surbrillance**

Tous concernés !

Mon entreprise est-elle concernée ?

Depuis le 25 mai 2018, toutes les entreprises sont concernées par le Règlement européen sur la protection des données personnelles **(RGPD)** dès lors qu'elles « traitent » (collectent, enregistrent, conservent…) des **données personnelles**.

Être soumis au RGPD n'est pas une question de taille (TPE/PME, grande entreprise), d'activité ou de mode de **traitement** (fichier tenu manuellement ou automatisé). Tout dépend de la façon dont les données sont traitées et des objectifs poursuivis.

Le RGPD concerne également la relation de l'entreprise :

- avec ses salariés (ex : données RH, badgeage…) ;
- avec ses clients (ex : coordonnées, préférences, historiques d'achats, cartes de fidélité, prospects…) ;
- avec ses **sous-traitants** (ou tout simplement lorsqu'il s'agit de son « cœur de métier » : hébergeur, éditeur de logiciel…).

Il existe ainsi une gradation dans les obligations selon les cas de figure : par exemple, les PME employant moins de 250 salariés ne sont pas, en principe, soumises à l'obligation de tenir un **registre des activités de traitement** sauf si ce traitement est susceptible de présenter un risque pour les droits des personnes ou porte sur des données particulières.

Exemple : la nomination d'un **délégué à la protection des données (DPD)** est aussi obligatoire pour des petites structures à partir du moment où elles effectuent un traitement des données personnelles de manière régulière et systématique à grande échelle et/ou portant sur des données sensibles (opinions religieuses, politiques, données médicales, biométriques…).

QUELLES FORMALITÉS PRÉALABLES POUR VÉRIFIER QUE MA TPE/PME EST SOUMISE AU RGPD ?

- **Recenser les données détenues** (diversité des fichiers constitués : clientèle, nom et prénom, adresses, habitudes de consommation, situation familiale, catégorie socioprofessionnelle, revenus, salariés…) ;
- **Lister la nature des données concernées** (notamment s'il s'agit de données sensibles ou relatives à des condamnations pénales et à des infractions) ;
- **Lister les finalités des traitements effectués ou envisagés** (vente de produits, campagne de mailing, newsletter, vente du fichier à des partenaires commerciaux, transmission à des tiers à des fins de livraison, de maintenance ou de commercialisation).

Pourquoi est-il fondamental de protéger les données personnelles de son entreprise ?

Protéger les données personnelles n'est pas seulement une obligation légale, c'est aussi un moyen de développer une "hygiène informatique" indispensable, notamment pour se prémunir contre la cybercriminalité dont les conséquences peuvent être lourdes non seulement pour l'activité de l'entreprise mais aussi pour son image.

Surtout, se conformer au RGPD peut être un atout économique pour l'entreprise qui pourra ainsi :

- **gagner la confiance de ses clients**, **fournisseurs et partenaires** ;
- **découvrir de nouvelles opportunités d'activité** à partir du capital de données existant ;
- **obtenir plus facilement des fonds** ;
- **anticiper le développement de son entreprise** pour éviter une mise en conformité coûteuse et tardive.

L'entreprise peut estimer que les traitements qu'elle opère n'entrent pas dans ceux visés par le RGPD, elle devra alors pouvoir le démontrer.

VERBATIM D'UN CHEF D'ENTREPRISE

« Le RGPD, c'est un projet d'entreprise »

En cas d'infraction au RGPD, les sanctions peuvent être très lourdes, les amendes peuvent s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial.

Fiche 1 DÉSIGNER UN RÉFÉRENT ET MOBILISER SES ÉQUIPES

Quand désigner un délégué à la protection des données ?

Une entreprise doit obligatoirement nommer un Délégué à la Protection des Données **(DPD)** lorsqu'elle effectue un **traitement à grande échelle** de données personnelles qui implique :

- de réaliser un suivi régulier et systématique des personnes ;
- de traiter des **données sensibles** via ses activités de base (origine raciale ou ethnique, données biométriques, santé ...) ;
- de traiter des données relatives à des condamnations pénales et infractions.

La démarche RGPD engage toute l'entreprise, elle doit impliquer tous les collaborateurs via des programmes de sensibilisation et de formation pilotés par le délégué à la protection des données.

Qui choisir ?

Compte tenu de ses tâches, le DPD doit être un bon chef de projet et avoir de solides compétences tant en matière juridique, qu'informatique.

Dûment associé à toutes les questions relatives à la protection des données à caractère personnel, il doit aussi pouvoir bénéficier :

- de garanties d'indépendance, ce qui implique de ne pas soumettre le DPD aux directions effectuant elles-mêmes les traitements (comme la Direction des systèmes d'information) ;
- des ressources nécessaires à l'exercice de ses missions.

Quelle est sa tâche ?

Il a pour principales missions :

- d'informer et conseiller le **responsable du traitement**, ses collaborateurs internes et externes, et les sous-traitants ;
- d'évaluer et contrôler le respect du droit à la protection des données à caractère personnel y compris dans le partage des responsabilités, la sensibilisation et la formation du personnel ;
- faire office de point de contact pour la Commission nationale informatique et libertés **(CNIL)** qui doit disposer de ses coordonnées ;
- être joignable par les collaborateurs et les parties prenantes de l'entreprise : ses coordonnées doivent être publiées par le responsable du traitement ou le sous-traitant.

Pour déjouer les attaques en matière de cybercriminalité :

- **87% des entreprises misent sur la sensibilisation des collaborateurs et les formations internes ;**
- **80 % sur le renforcement des procédures de contrôle interne ;**
- **44% sur des audits de sécurité des systèmes d'information.**

(Etude Fraude Euler Hermès et la DFCG, 2018)

Comment faire à défaut de compétences en interne ?

L'absence de compétences spécifiques au sein de l'entreprise en matière de réglementation des données personnelles ne doit pas être un frein à la désignation d'un DPD dans les TPE-PME : il peut être externalisé ou encore désigné par et pour un groupe d'entreprises.

Comment mobiliser ses équipes autour du délégué à la protection des données ?

Le DPD n'agit pas seul, il est étroitement lié aux opérationnels. Il est par ailleurs en charge de la formation et de la sensibilisation afin que la protection des données à caractère personnel soit parfaitement intégrée dans tous les métiers de l'entreprise.

VERBATIM D'UN CHEF D'ENTREPRISE

« Le RGPD, c'est apprendre aux opérationnels à avoir une autre culture de la donnée... »

Fiche 2

ÉTABLIR SON PLAN DE CONFORMITÉ

Les 4 phases du plan de conformité

1 • Recenser ses données et ses traitements ;

2 • Mener une analyse d'impact lorsqu'elle est nécessaire ;

3 • Adopter les mesures techniques et organisationnelles propres à protéger les données ;

4 • Suivre régulièrement la conformité et la documenter.

Pourquoi et comment établir un registre des activités de traitement ?

Un registre recensant les activités de traitement est obligatoire pour les entreprises de plus de 250 employés.

En deçà de ce seuil, le registre reste obligatoire lorsque le traitement effectué :

- est susceptible de comporter un risque pour les droits et libertés des personnes concernées ;
- est non occasionnel ;
- concerne des données sensibles (origine ethnique, opinion religieuse, donnée biométrique...) et/ou relatives à des condamnations pénales et à des infractions.

Grâce au registre, l'entreprise va pouvoir cartographier l'ensemble des données :

- vérifier que leur collecte est nécessaire à la finalité poursuivie par le traitement ;
- savoir où elles sont stockées (Dans quel pays ? Un niveau adéquat de protection est-il garanti ?) ;
- cibler les données à purger (ex : mention de la religion des employés) ...

Le registre n'est pas figé et doit être tenu à jour régulièrement.

Comment établir le registre ?

Le registre est présenté sous forme écrite, y compris sous forme électronique.
La CNIL a publié **un modèle de registre ainsi qu'une fiche de registre.**

Quel est le contenu du registre ?

Il comporte, d'abord, le **nom** et les **coordonnées de l'entreprise** (qu'elle soit **responsable de traitement** ou **sous-traitant d'un responsable de traitement**) et de son DPD ainsi que la liste de toutes ses activités de traitement de données personnelles. Il contient, ensuite, une fiche sur chaque activité de traitement.

Informations à fournir par le responsable de traitement pour chaque activité de traitement

Identification et coordonnées du ou des responsables du traitement	**Finalité de chaque traitement**	**Catégorie des personnes concernées** (clients, prospects...) **Données concernées** (nom, prénom, coordonnées, adresse IP,....) **Présence de données sensibles**	**Flux des données** Destinataires des données Où sont-elles hébergées et transférées ? Dans l'UE ou en dehors de l'UE?	**Durée de conservation**	Moyens mis en œuvre afin de **garantir un niveau de sécurité adapté au risque**

Informations à fournir par le sous-traitant pour chaque activité de traitement

Identification et coordonnées du sous-traitant et du responsable du traitement pour le compte duquel il agit	**Catégories de traitements effectués** pour le compte de chaque responsable du traitement	**Flux des données**	**Moyens mis en œuvre afin de garantir un niveau de sécurité adapté au risque**

Le registre permet à l'entreprise de vérifier la pertinence de ses mesures de sécurité compte tenu des risques pesant sur les droits et libertés des personnes physiques du fait du traitement.

Quand faut-il mener une analyse d'impact?

Avant sa mise en œuvre, chaque **« traitement de données personnelles susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques »** doit faire l'objet d'une **analyse d'impact** sur la protection des données ou Privacy Impact Assessment (PIA).

Comment déterminer si un traitement de données personnelles est « susceptible d'engendrer des risques élevés pour les droits et libertés des personnes » ?

L'analyse d'impact est **obligatoire** en présence :

- d'une évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un **traitement automatisé**, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- d'un traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et à des infractions ;
- ou dans l'hypothèse d'une surveillance systématique à grande échelle d'une zone accessible au public.

La CNIL a indiqué qu'étaient également visés les traitements remplissant au moins deux des critères suivants :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Il faut consulter la CNIL ou l'autorité de contrôle compétente dans les pays de l'UE, préalablement au traitement, lorsqu'une analyse d'impact révèle un risque élevé.

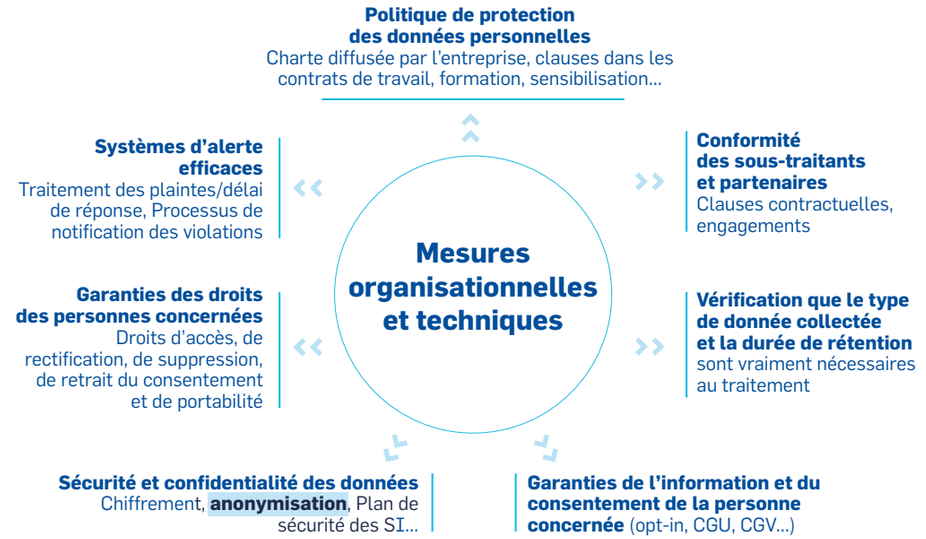
Exemple : la surveillance systématique des salariés implique une analyse d'impact.

L'historique des incidents rencontrés par l'entreprise permet d'alerter sur la nécessité de mener une étude d'impact :
exemple, le vol d'un ordinateur portable d'un commercial contenant le fichier client et ses effets sur les personnes concernées.

L'analyse permet d'évaluer l'impact des traitements de façon à minimiser les risques sur la vie privée et d'opter pour les modalités de traitement les plus adaptées.

Quelles mesures organisationnelles et techniques prendre pour se mettre en conformité ?

Le **registre des opérations de traitement** et l'analyse d'impact menée dans l'entreprise doivent conduire à mettre en place des mesures organisationnelles et techniques appropriées pour protéger les données personnelles et les faire évoluer, si besoin, pour répondre aux exigences du RGPD.



Comment organiser sa conformité dans le temps ?

Il est important de :

- mettre à l'épreuve et actualiser régulièrement le plan de conformité (par exemple une fois par an) pour vérifier la pertinence et l'efficacité des mesures en place (changement régulier des mots de passe, contrôle d'accès au registre concerné...) ;
- prévoir une sensibilisation et une formation du personnel à intervalles réguliers.

Penser à documenter tous les stades de la constitution du plan de conformité (registre, clauses contractuelles,...) et de sa mise en œuvre. Les supports écrits peuvent être demandés à n'importe quel moment par la CNIL et doivent pouvoir être transmis immédiatement.

VERBATIM D'UN CHEF D'ENTREPRISE

« Le risque réputationnel doit être transformé en atout. Avec le RGPD, l'entreprise montre qu'elle respecte ses clients »

Fiche 3

CONNAÎTRE LES MODES DE CERTIFICATION OFFICIELS : certification, label, code de bonne conduite

Le RGPD précise qu'un des moyens de prouver le respect de ses obligations en matière de protection des données est de faire valoir que l'on a fait l'objet d'une certification ou que l'on applique un code de conduite approuvé.

Certification ou label ?

La CNIL a mis fin à son activité de labellisation à la faveur de la certification.

Des **certifications** seront délivrées par des organismes certificateurs agréés par la CNIL ou accrédités par l'organisme national d'accréditation (COFRAC). Les certificateurs pourront utiliser des référentiels de certification en cours d'élaboration, qui seront approuvés et publiés par la CNIL.

S'agissant des labels déjà obtenus, la CNIL a précisé que, jusqu'à échéance de leur validité, seuls étaient garants de la conformité RGPD les labels Gouvernance (*www.cnil.fr/fr/labels-gouvernance)*) et Formation *(www.cnil.fr/fr/labels-formation)*, leurs référentiels ayant été mis à jour conformément au RGPD.

Les entreprises peuvent à travers ces démarches prouver leur volonté de se mettre en conformité.

Attention aux arnaques !

Beaucoup de prestations « clés en main » promettent de garantir une conformité au RGPD. Elles se déclarent labellisées ou certifiées par la CNIL. Il est impératif de vérifier cette affirmation. Le risque est double car au-delà de l'arnaque financière peut se cacher aussi un mécanisme visant à s'emparer des données de l'entreprise.

À cet effet, la DGCCRF et la CNIL ont formulé des recommandations *(www.cnil.fr/fr/pratiques-abusives-mise-en-conformite-RGPD-CNIL-DGCCRF)* rappelant que les pouvoirs publics n'ont jamais mandaté d'entreprises pour proposer à titre onéreux des prestations de mise en conformité au RGPD.

La DGCCRF et la CNIL ont listé les principaux réflexes à adopter en présence de telles sollicitations :

- demander des informations sur l'identité de l'entreprise démarcheuse permettant de faire des vérifications sur internet ou auprès des syndicats professionnels ;
- se méfier de communications prenant les formes d'une information officielle émanant d'un service public ;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;
- prendre le temps de la réflexion et de l'analyse de l'offre ;
- diffuser ces conseils de vigilance auprès des services et des personnels de l'entreprise qui sont appelés à traiter ce type de courrier ;
- ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse.

En cas de doute, ne pas hésiter à contacter la CNIL au 01 53 73 22 22

Comme l'ont rappelé la DGCCRF et la CNIL, les entreprises de moins de 5 salariés sont protégées par les dispositions du code de la consommation pour les contrats conclus hors établissement (possibilité de se rétracter...).

En cas de pratiques commerciales déloyales ou pratiques contractuelles abusives, il est possible de s'adresser à la Direction départementale de la protection des populations (DDPP) ou à la Direction départementale de la cohésion sociale et de la protection des populations (DDCSPP) du département de son siège social.

POUR ALLER PLUS LOIN **www.economie.gouv.fr/dgccrf/coordonnees-des-DDPP-et-DDCSPP**

Qu'est-ce qu'un code de conduite sectoriel ?

Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des **codes de conduite**, modifier ou proroger ceux déjà existants, aux fins de préciser les modalités d'application du RGPD. Ces codes doivent être soumis pour avis préalable et approbation à la CNIL. Si les activités en cause concernent plusieurs États membres de l'Union européenne, sont également saisis le **Comité européen** (regroupant l'ensemble des autorités de contrôles européennes) et la Commission.

Bonnes pratiques : il est recommandé de s'informer et de communiquer avec les parties prenantes du secteur pour mener à bien sa conformité en mutualisant les efforts et les outils.

Fiche 4 RECUEILLIR LE CONSENTEMENT

Faut-il toujours recueillir le consentement ?

Le traitement des données personnelles doit être licite, il repose notamment sur le **consentement** de la personne concernée et sur un fondement légitime.

Il n'est donc pas exigé de recueillir le consentement si le traitement des données est nécessaire à l'exécution du contrat (vente, service, etc.) : par exemple, il n'est pas possible de livrer un bien sans traiter les adresses de livraison, de payer un salaire sans traiter les coordonnées bancaires ...

Faut-il demander à nouveau le consentement de mes clients/salariés pour les données récoltées avant l'entrée en vigueur du RGPD ?

Non, lorsque le traitement est fondé sur un consentement obtenu en vertu des règles antérieurement en vigueur (à savoir celles de la directive 95/46/CE) et notamment selon les principes de proportionnalité, de transparence et de finalité légitime, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement.

En revanche, tous les consentements présumés, c'est-à-dire ceux pour lesquels il n'existe pas de preuve qu'ils ont bien été donnés, seront automatiquement considérés comme ne remplissant pas les conditions requises par le RGPD et devront être renouvelés.

Le consentement préalable est l'une des conditions de licéité d'un traitement des données. Il doit être libre, éclairé, spécifique à une finalité et donné de manière non équivoque qu'il soit recueilli offline ou online.

Les 4 étapes à respecter :

1 • **Recueillir le consentement éclairé de la personne**

2 • **Conserver la preuve du consentement**

3 • **Informer la personne concernée de ses droits**

4 • **Mettre en place un processus de gestion des réclamations**

Comment recueillir le consentement ?

RECUEIL DES DONNÉES EN LIGNE

Pour chaque formulaire en ligne, qu'il s'agisse d'un formulaire de contact, de demande de téléchargement, de demande de devis, d'inscription à un événement, le consentement de l'internaute à l'utilisation de ses données personnelles doit être obtenu.

Remplir un formulaire ne suffit pas, une case à cocher doit être configurée dans un champ obligatoire pour que le consentement soit explicite : opt-in. Prévoir autant de cases à cocher que de traitement spécifique.
Les cases remplies par défaut sont interdites.

RECUEIL DES DONNÉES HORS LIGNE

Un formulaire papier doit être mis à disposition de la personne dont les données sont recueillies.

S'agissant des appels téléphoniques, une déclaration orale est valable à condition de recueillir l'identité de la personne par confirmation sur plusieurs éléments : date de naissance, adresse, mail...

CAS SPÉCIFIQUE DU PARRAINAGE PROMOTIONNEL

Les opérations de parrainage consistent, pour une entreprise/association de commerçants, à demander à une personne de fournir les coordonnées d'un tiers susceptible d'être intéressé par une offre, un article ou une annonce. La CNIL admet la possibilité de collecte et d'utilisation de l'adresse mail d'une personne sans son consentement préalable, dès lors que le premier message électronique de prospection envoyé comporte l'identité du parrain. Mais les données du parrainé ne pourront être utilisées qu'une seule fois, pour lui adresser l'offre/l'article/l'annonce suggéré par le parrain. L'entreprise ne pourra conserver les données du parrainé pour lui adresser d'autres messages que si elle a obtenu son consentement exprès.

CONSEILS DE RÉDACTION

- Employer des termes clairs : "Consentir" "Accepter" "Autoriser"
- Spécifier la finalité : *« pour permettre de vous recontacter » « pour vous envoyer la newsletter, dans le cadre de la relation commerciale qui découle de cette demande de devis », etc.*

Il n'est pas possible de recueillir les cartes de visite sous le prétexte d'un jeu concours, sans indiquer leurs réelles fins de prospection. Il faudra également conserver la date, le lieu et **la manière** dont ces données ont été recueillies.

Dans tous les cas, l'information selon laquelle la personne a le droit de retirer son consentement doit être également mentionnée au moment où son accord est obtenu.

LE CAS SPÉCIFIQUE DES MINEURS

La France a fixé la majorité numérique à 15 ans. Dès lors, les traitements concernant les mineurs de moins de 15 ans nécessitent l'accord préalable des titulaires de l'autorité parentale.

Le professionnel devra s'efforcer d'obtenir « raisonnablement » cette autorisation parentale.

Comment conserver la preuve du consentement ?

Si le consentement s'effectue par l'envoi d'un formulaire avec une case à cocher, il est indispensable de garder une trace de cet envoi, sa date et le contenu du consentement.

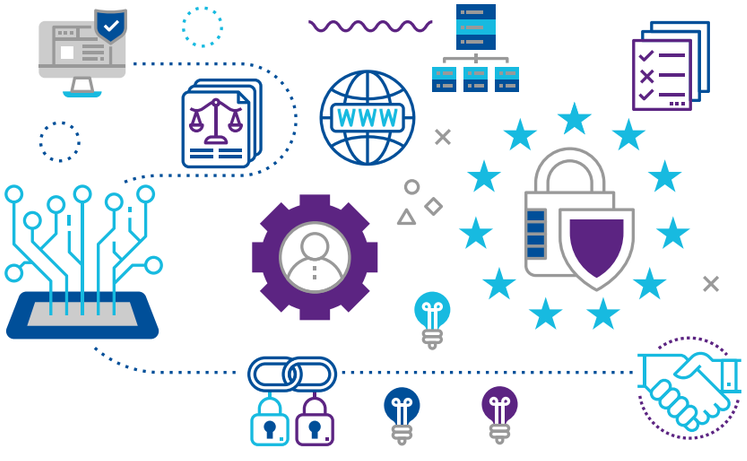
Quelles informations transmettre ?

Le RGPD exige qu'un certain nombre d'informations soient portées à la connaissance de la personne concernée lorsque les données personnelles sont collectées auprès d'elle.

Il s'agit notamment des informations suivantes :

- l'identité du Responsable de Traitement ;
- les coordonnées du Délégué à la Protection des Données ;
- la finalité des traitements ;
- les destinataires des données ;
- le type de données collectées et leur durée de conservation ;
- l'existence du droit de demander l'accès aux données, leur rectification ou leur effacement etc. ;
- la procédure pour exercer son droit d'accès, de rectification et d'effacement, de portabilité etc.

Attention, si les données sont obtenues auprès d'une autre source, toutes ces informations devront être portées à la connaissance de la personne concernée dans un délai raisonnable.



Comment mettre en place un processus de gestion des réclamations ?

La personne concernée peut faire valoir, à tout moment, les droits dont elle dispose sur ses données personnelles auprès du professionnel. Il s'agit du :

- droit d'accès ;
- droit de retirer son consentement ;
- droit de rectification ;
- droit **d'effacement** ;
- droit au déréférencement ;
- droit d'opposition ;
- droit à la **portabilité des données**.

Attention, le professionnel ne pourra pas toujours satisfaire ces droits en particulier lorsqu'il doit respecter un certain nombre d'obligations légales telles que la conservation de données en cas de contrôle fiscal ou des pièces à fournir dans l'hypothèse d'un contentieux...

DÉLAI DE RÉPONSE
Le professionnel devra répondre dans les meilleurs délais et au plus tard dans le délai d'un mois à compter de la réception de la demande.

Aucun paiement ne peut être exigé pour répondre à ces différentes demandes.

Il faut prévoir des mécanismes simples d'utilisation en envisageant plusieurs moyens de contact dont la **visibilité est suffisante sur les documents commerciaux** ou sur le **site internet** lorsqu'il existe :

- adresse électronique ;
- adresse postale ;
- et /ou numéro de téléphone.

VERBATIM D'UN CHEF D'ENTREPRISE

« Le RGPD est un défi qui amènera des générations d'entreprises au numérique éthique »

Fiche 5

ADAPTER SES CONTRATS ET CONDITIONS GÉNÉRALES

Vérifier la compatibilité des contrats de sous-traitance avec le RGPD : BtoB

Le prestataire qui gère les données pour le compte de son client doit s'interroger sur la conformité des produits qu'il développe avec le RGPD et s'ils ont éventuellement fait l'objet d'une analyse d'impact. Il doit pouvoir en faire état dans ses contrats et fournir les documents qui en attestent.

Il doit également s'assurer que les ressources tierces sur lesquelles il s'appuie ou qu'il intègre dans ses produits répondent à ces exigences.

Adapter les conditions générales de vente BtoC

COMMENT INFORMER SES CLIENTS SUR SA POLITIQUE DE GESTION DES DONNÉES PERSONNELLES ?

Les mentions sur les données personnelles peuvent par exemple être intégrées dans les conditions générales de vente (CGV) soit dans un article spécifique ou encore dans un document connexe type **charte** ou **politique de protection des données** personnelles. Aucun formalisme n'est imposé mais l'ensemble des obligations d'informations mentionnées dans le RGPD doit y figurer, notamment la liste des droits dont dispose le client quant à l'utilisation de ses données : droit de réclamation, demande de désabonnement... Ces informations doivent être rédigées clairement et être facilement accessibles.

Suggestions de clauses relatives à la protection des données à caractère personnel pouvant être incluses dans les CGV en matière de BtoC :

COLLECTE DES DONNÉES SUR UN SITE INTERNET

Les données à caractère personnel collectées sur notre site sont les suivantes :

- ouverture du compte utilisateur : les données recueillies concernent le nom, le prénom, l'adresse électronique, la date et lieu de naissance ;
- connexion : lors de la connexion de l'utilisateur à notre site, sont enregistrées ses coordonnées, la durée de connexion, la localisation et les données relatives au paiement ;
- profil : l'utilisation des services proposés par notre site internet permet de renseigner un profil qui peut inclure différentes informations dont l'adresse et le numéro de téléphone ;
- paiement : lors des transactions effectuées sur notre site, sont enregistrées les données liées au compte bancaire et à la carte de crédit de l'utilisateur.
- cookies : des cookies sont utilisés sur notre site, l'utilisateur a la possibilité de les désactiver à partir des paramètres de son navigateur.

UTILISATION DES DONNÉES

Les données personnelles que nous collectons auprès des utilisateurs de notre site internet visent à permettre l'accès aux différents services de notre site, leur amélioration et leur sécurisation. L'utilisation des données porte sur :

- l'accès et l'utilisation du site internet ;
- la gestion du site internet ;
- l'identification/l'authentification des données ;
- l'assistance utilisateur ;
- la personnalisation des services en affichant des publicités en fonction de l'historique de navigation (si c'est le cas) ;
- la prévention et la détection des fraudes (logiciels malveillants) et la gestion des incidents de sécurité ;
- le traitement des éventuels litiges avec les utilisateurs ;
- l'envoi d'informations commerciales et publicitaires, en fonction des préférences de l'utilisateur (si c'est le cas).

PARTAGE DES DONNÉES AVEC DES SOCIÉTÉS TIERCES

Les données personnelles collectées peuvent être partagées avec des sociétés tierces dans les cas suivants :

- relations avec des sociétés bancaires et financières pour le paiement ;
- recours aux services de prestataires pour fournir l'assistance utilisateurs du site internet, à la publicité et aux services de paiement. Ces prestataires disposent d'un accès limité aux données de l'utilisateur dans le cadre de l'exécution de ces prestations et ont une obligation contractuelle de les utiliser en conformité avec les dispositions du RGPD ;
- quand la loi l'exige, les données peuvent être transmises pour faire suite à des réclamations exercées contre le professionnel afin de se conformer aux procédures administratives et judiciaires.

TRANSFERT DES DONNÉES AUX ÉTATS-UNIS (LE CAS ÉCHÉANT...)

Cette clause est pertinente lorsque le professionnel appartient à un groupe international ou lorsqu'il fait appel à un sous-traitant situé aux États-Unis. L'utilisateur autorise le professionnel responsable du site internet à transférer, stocker et traiter ses informations dans ce pays. Le professionnel est responsable des données personnelles qui sont partagées avec des tiers dans le cadre du Privacy Shield, bouclier de protection des données entre l'Union européenne et les États-Unis relatif à la collecte, l'utilisation et la conservation des données à caractère personnel transférées aux États-Unis depuis l'Union européenne. En cas de conflit entre les conditions de la clause et les principes du Privacy Shield, ceux-ci prévaudront.

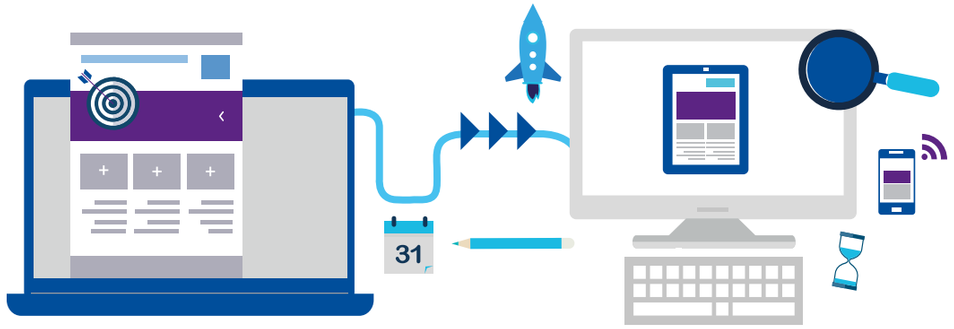
MISE EN ŒUVRE DES DROITS DES UTILISATEURS

Conformément aux règles applicables aux données à caractère personnel, les utilisateurs disposent des droits suivants :

- mettre à jour ou supprimer les données qui les concernent en se connectant à leur compte ;
- supprimer leur compte en cliquant sur le lien suivant : ....
- exercer leur droit d'accès pour prendre connaissance de leurs données personnelles en écrivant à l'adresse mail suivante.....ou en contactant le numéro suivant : .....
- corriger l'inexactitude des informations les concernant en écrivant à l'adresse mail suivante ou appelant le numéro suivant : .....
- demander la suppression de leurs données à caractère personnel en écrivant à l'adresse mail suivante...

Fiche 6

ORGANISER LA PORTABILITÉ DES DONNÉES



Le droit à la portabilité des données vise à faciliter le passage d'un prestataire de service à un autre et renforce la concurrence entre les divers prestataires de service. Il offre la possibilité de gérer et de réutiliser ses données. Par exemple : les titres de livres qu'une personne a achetés sur une librairie en ligne, les playlists qu'elle a constituées via un service de musique en streaming...

Le droit à la portabilité est limité aux données personnelles fournies par la personne concernée sur la base de son consentement ou pour la bonne exécution d'un contrat

Sous quel délai répondre à une demande de portabilité ?

La réponse doit se faire dans les meilleurs délais, au plus tard un mois à compter de la réception de la demande.

QUELLES DONNÉES SONT CONCERNÉES ?

Deux catégories de données sont visées :

- les données déclarées de manière volontaire : la date et lieu de naissance, l'adresse postale, l'e-mail ;
- les données produites lors de l'utilisation d'un service ou d'un appareil : une playlist constituée par l'abonné à un service de streaming, les achats listés sur une carte de fidélité, les mails envoyés et reçus, l'historique des recherches...).

PEUT-ON REFUSER DE PROCÉDER AU TRANSFERT DEMANDÉ ?

Tout dépend du degré d'action de l'utilisateur sur les données : une playlist proposée en fonction des préférences de l'utilisateur par un prestataire ne pourra pas être transférée car elle a été développée en fonction des algorithmes de la plateforme de musique en ligne.

Les données anonymisées sont exclues du droit à la portabilité mais pas les données pseudonymisées.

Seuls les fichiers automatisés sont concernés. Le responsable de ces traitements n'est donc pas obligé de dématérialiser ses fichiers pour réaliser la portabilité.

Modalités du transfert

Deux cas de figure :

- L'envoi direct aux personnes concernées : il est recommandé de les envoyer dans un format électronique approprié et notamment à travers un portail électronique ;
- L'envoi des données à un autre prestataire (sur demande de la personne).

BON À SAVOIR

Le professionnel devra garder une trace du transfert mais il n'est pas responsable de la façon dont les données seront utilisées par la suite.

Les données doivent être transmises à leur titulaire dans « un format structuré, couramment utilisé et lisible par la machine ». Ce dernier pourra à son tour les transmettre à un autre responsable de traitement sans que le professionnel puisse s'y opposer.
La personne concernée peut cependant préférer que ses données soient directement transmises d'un responsable de traitement à un autre. Cette condition suppose toutefois que les responsables de traitement aient mis en place des formats interopérables.
Si l'interopérabilité ne peut pas être mise en œuvre, les informations devront être envoyées dans un format électronique approprié et si cela ne fonctionne pas, les raisons techniques de cet empêchement devront être fournies au titulaire de droits.
Le Comité européen (ex G29), instance qui regroupe les autorités de contrôle européennes, invite toutefois les responsables de traitement à sélectionner un format réutilisable et lisible par d'autres systèmes pour une bonne réutilisation des données.

Sauf demande manifestement infondée ou excessive, le transfert des fichiers demandés doit être gratuit.

Conséquences pour le titulaire des données

Une demande de portabilité n'implique pas nécessairement que la personne cesse de bénéficier de son service ou que ses données soient effacées : par exemple, tout en continuant de bénéficier d'un service d'abonnement auprès d'un prestataire A, l'utilisateur peut décider de transférer ses données à un prestataire B auquel il s'abonne également.

Aucun format particulier n'a été imposé par le RGPD, il doit simplement être interopérable et peut être différent selon les secteurs d'activités.

Fiche 7

RÉAGIR A LA VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL

Qu'est-ce que la violation de données à caractère personnel ?

Suite à une faille de sécurité, des données traitées ou stockées permettant d'identifier une personne physique (salarié, client, prospect, fournisseur…), ont pu faire l'objet d'une destruction, d'une altération ou, le plus souvent, d'une communication à un tiers non autorisé (un hacker, un concurrent…).

Le responsable de traitement doit réagir rapidement et de façon appropriée en cas de **violation de données à caractère personnel**.

Le **sous-traitant** qui constate une faille de sécurité doit en informer **immédiatement** le responsable de traitement.

Que doit faire le responsable de traitement ?

1ère ÉTAPE

- **Déterminer la nature de la violation**
- **Évaluer les risques que la situation est susceptible d'engendrer pour les droits et les libertés**

› S'agit-il d'un vol de fichiers, d'une destruction, d'un problème de serveurs ?

› Cet incident est-il susceptible d'engendrer des risques pour la vie privée des personnes dont les données ont été violées : limitation de leurs droits, discrimination, vol ou usurpation d'identité, perte financière, atteinte à leur réputation, perte de confidentialité de données protégées par le secret professionnel ?

ex : une intrusion dans le serveur d'un prestataire en charge de campagnes de marketing direct peut entraîner une fuite de données qui doit inciter les personnes concernées à la prudence au regard des risques de phishing, d'escroquerie ou d'usurpation d'identité.

2ème ÉTAPE :

- **Prendre les mesures nécessaires pour remédier à cette faille de sécurité (par exemple : rétablir la disponibilité du serveur).**

3ème ÉTAPE :

- **Évaluer si cette faille de sécurité nécessite une notification à la CNIL, voire aux personnes dont les données ont été violées.**

1ère hypothèse

La violation des données **n'est pas susceptible d'engendrer un risque** pour les droits et les libertés des personnes physiques

le responsable de traitement n'est pas tenu de la notifier

Il doit pouvoir justifier cette abstention auprès de la CNIL si celle-ci le lui demande.

ex. : les données sont inexploitables car toutes les mesures ont été prises en amont pour les sécuriser (chiffrement…)

2ème hypothèse

La violation des données **est susceptible d'engendrer un risque** pour les droits et les libertés des personnes physiques

le responsable de traitement devra impérativement en informer la CNIL

Ce n'est pas une option : des sanctions pénales et administratives sont prévues.

3ème hypothèse

La violation des données **est susceptible d'engendrer un risque élevé** (risque réel de réutilisation non consentie des informations) pour les droits et les libertés des personnes physiques

le responsable de traitement devra également en informer toutes les personnes concernées

Le critère de risque élevé pour les droits et les libertés des personnes physiques est le même que celui retenu en matière d'étude d'impact obligatoire.

En cas de doute sur l'interprétation du « risque élevé », contacter la CNIL.

NB : Si la violation de données à caractère personnel porte sur des données qui ont été transmises par (ou à) un responsable de traitement établi dans un autre État membre de l'Union européenne, elle doit être notifiée à la personne concernée dans les meilleurs délais.

Comment notifier la violation des données à caractère personnel ?

QUELLES INFORMATIONS COMMUNIQUER ?

à la CNIL

1. La nature de la violation ;
2. Les catégories et le nombre approximatif de personnes concernées (si possible) ;
3. Le nombre approximatif d'enregistrements de données (si possible) ;
4. Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
5. Les conséquences probables de la violation de données à caractère personnel
6. Les mesures prises ou qui seront mises en œuvre :
   - pour remédier à cette violation de données à caractère personnel,
   - pour en atténuer les éventuelles conséquences négatives.

aux personnes dont les données ont été violées

QUEL EST LE DÉLAI DE NOTIFICATION ?

à la CNIL

Dans les meilleurs délais et, **si possible, 72 heures au plus tard** après avoir pris connaissance de l'incident

Si le délai de 72 h ne peut pas être respecté, il convient de :

- notifier le plus rapidement possible, en précisant les motifs du retard ;
- transmettre les informations, même de façon échelonnée, dès qu'elles sont à disposition.

Dans un délai aussi raisonnable que possible

aux personnes dont les données ont été violées

Dans certains cas, la communication aux personnes concernées pourra être retardée pour tenir compte d'éléments propres à l'incident de sécurité en cause.

Exemple : nécessité de mettre prioritairement en œuvre des mesures appropriées pour empêcher la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires, l'existence d'une enquête judiciaire qui pourrait être entravée par une divulgation prématurée…

COMMENT INFORMER ?

à la CNIL

Le téléservice de notification de violations de la CNIL est à la disposition des responsables de traitement concernés

La communication doit être faite en des termes clairs et simples

aux personnes dont les données ont été violées

Dans le cas où la notification exigerait des efforts disproportionnés, une communication publique peut être privilégiée.

COMMENT ÉVITER LES FAILLES DE SÉCURITÉ ?

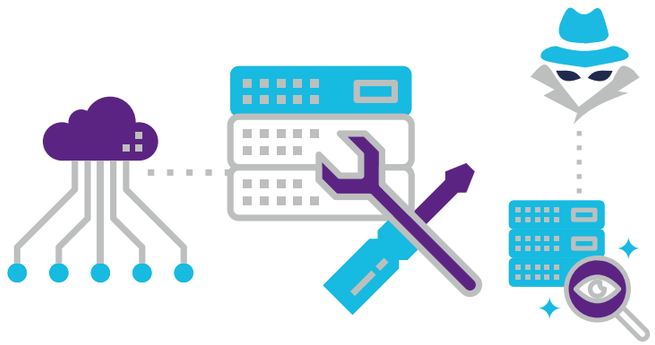
… en les anticipant !

C'est-à-dire en ayant pris des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (V. fiche n°2 « Établir son plan de conformité »).

Les obligations de sécurité décrites dans le RGPD doivent donc être regardées comme des pare-feux utiles face aux risques de failles informatiques.

VERBATIM D'UN CHEF D'ENTREPRISE

« Certes, la conformité a un coût mais il est proportionné à l'activité en matière de traitement et il doit être mis en balance avec celui des brèches de sécurité »



Fiche 8

SENSIBILISER LES PERSONNELS À LA PROTECTION DES DONNÉES

Sensibiliser, c'est protéger les données de l'entreprise

Les failles de sécurité portant sur des données traitées ou stockées sont causées dans 35% des cas par des personnes physiques (salarié, client, prospect, fournisseur...).

Des actions humaines sont le plus souvent à l'origine de la destruction de données, de leur altération, de leur communication à un tiers non autorisé (un hacker, un concurrent...) ou de leur perte accidentelle.

Quelles sont les failles vers les données de l'entreprise ?

Les failles dans la sécurité des données de l'entreprise ne sont pas seulement le fait d'attaques extérieures, elles sont parfois le résultat de négligences internes, voire d'erreurs dues à la méconnaissance des consignes et des enjeux liés à la sécurité ou à une violation des consignes de sécurité au sein de l'entreprise. Sont en cause :

- la multiplication des canaux de communication que l'entreprise a déployés dans le cadre de sa stratégie numérique (pages Facebook, LinkedIn, Viadeo, forums, sites web, Blog, Twitter, ...) ;
- les réseaux sociaux et toutes les informations personnelles permettant de passer les barrières de sécurité (type mot de passe et login) utilisés sur les appareils de l'entreprise ou non ;
- la perméabilité des appareils (ou devices) : la multiplication de nouveaux usages (BYOD/mobilité, télétravail, plateformes collaboratives, ...) impliquent de se connecter à des réseaux qui sont parfois insuffisamment protégés ;
- une tentative d'installation d'un logiciel par un salarié ou la méconnaissance des risques de *phishing* (hameçonnage).

Les attaques sur les données personnelles prennent des formes très diverses :

- la prise des données en otage ou *ransomware* (61 %) ;
- la défiguration de site web (23 %) ;
- le vol de données personnelles (18 %).

La plupart de ces intrusions sont le résultat d'une négligence humaine.

(3ème édition du Baromètre annuel du Club des Experts de la Sécurité de l'Information et du Numérique, CESIN)

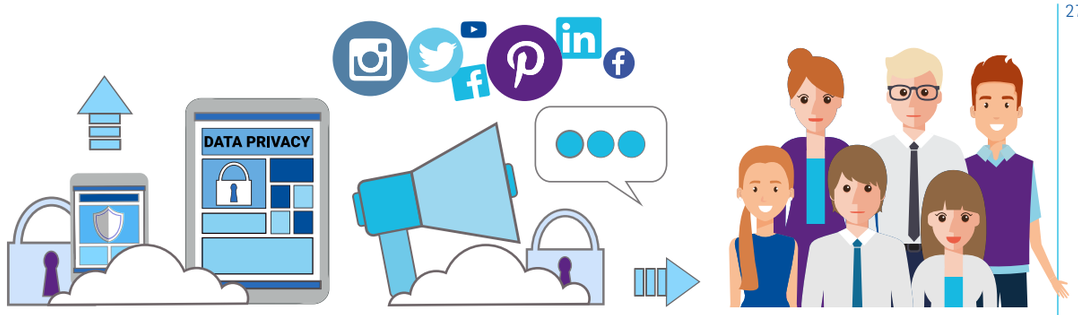
DEPUIS L'ENTRÉE EN VIGUEUR DU RGPD, 74% DES ENTREPRISES FRANCILIENNES ONT FORMÉ LEURS ÉQUIPES (ENQUÊTE D'OPINION DU CROCIS - JUIN 2018)

Quelles conséquences pour l'entreprise ?

Plus de 8 entreprises françaises sur dix ont été visées par une cyberattaque en 2015.

Une cyberattaque peut induire :

- Des pertes de fichiers importantes ;
- Un impact négatif sur l'image de l'entreprise vis-à-vis de ses clients, fournisseurs et prospects.



Comment sécuriser son système d'information ?

Plusieurs démarches doivent être mises en œuvre en interne pour protéger les données :

- sensibiliser son personnel aux pratiques élémentaires de sécurité informatique (règles de navigation sur internet, accès à la messagerie personnelle...) ;
- prévoir une charte relative à l'usage des réseaux sociaux, notamment si l'entreprise est présente sur ces réseaux ;
- identifier les données les plus sensibles (liste de clients, données RH, brevet...) et effectuer un inventaire des comptes bénéficiant de droits étendus sur ces données ;
- encadrer les règles permettant au personnel d'utiliser un équipement informatique personnel au sein de l'entreprise ;
- authentifier et contrôler les accès en évitant la configuration des systèmes d'information par défaut (exemple : nom d'utilisateur : admin, mot de passe : 12345) ;
- faire une information sur la configuration des mots de passe pour les rendre plus fiables tout en les changeant régulièrement ;
- sécuriser les postes de travail en interdisant par exemple le branchement des clés USB sur les ordinateurs.

Moyens de sensibilisation des salariés

DEVELOPPER UNE POLITIQUE DE SÉCURITÉ

Élaborer et codifier une politique de sécurité compréhensible par tous permet d'adapter sa stratégie.

Ces étapes d'élaboration des procédures de sécurité doivent cependant se faire sur un mode collaboratif, voire en réseau. Tous les acteurs de la chaîne de résolution de crise numérique doivent être impliqués.

DIALOGUER ET FAIRE DE LA PÉDAGOGIE

L'édiction de règles n'en garantit pas le respect. Il faut responsabiliser les communautés d'utilisateurs, qu'ils soient clients, prestataires, salariés ou sous-traitants. Cette responsabilité individuelle est une des clés de la protection des données car une carence humaine dans ce domaine peut entraîner la contamination de toutes les filiales d'un groupe.

La pédagogie doit être constante, renouvelée et accessible. Par exemple, la diffusion de l'historique des accidents déjà survenus, leur cause, les démarches à suivre pour qu'ils ne surviennent plus peut être utile.

ADOPTER DES PROCÉDURES DE CYBER-RÉSILIENCE

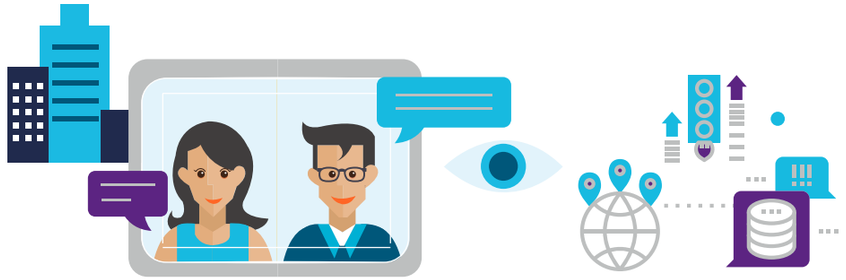
La cyberésillience vise à anticiper une attaque et non à l'éviter. Il s'agit de favoriser la continuité de l'activité en cas de fermeture des vitrines numériques, de rupture des moyens de communication ou d'entraves à l'exercice normal de l'activité.

Les règles d'or à diffuser en entreprise

- Maintenez vos logiciels à jour
- Ayez une bonne politique de mot de passe
- Méfiez-vous de certains mails
- Protégez-vous par un bon anti-virus
- Chiffrez vos disques
- La sécurité, ce n'est pas tabou : échangez
- Sauvegardez
- Sécurisez votre accès Wifi
- Soyez attentif lors de vos déplacements
- Pensez au Cloud

Fiche 9

GÉRER LES RELATIONS DE L'ENTREPRISE AVEC SES SALARIÉS



Employeurs et recruteurs ont fréquemment recours à la collecte de données personnelles dans le cadre de la gestion des ressources humaines. Elle commence dès le recrutement, avec les curriculum vitae et les tests d'évaluation, et se poursuit ensuite tout au long de la carrière du salarié via par exemple, les déclarations sociales et fiscales, les arrêts maladie, ou encore les échanges de correspondance.

Quelles données l'employeur peut-il collecter ?

L'employeur ne doit collecter que les données nécessaires au regard des finalités pour lesquelles elles ont été collectées.

Dans le cadre d'un recrutement, les données collectées doivent donc être limitées à celles strictement nécessaires à l'évaluation des capacités du candidat à occuper le poste proposé (diplômes, emplois précédents, etc.).

Il est ainsi interdit de collecter des informations sur sa famille, ses opinions politiques ou encore son appartenance syndicale.

A l'embauche du candidat, l'employeur peut collecter des informations complémentaires. Celles-ci doivent être soit nécessaires au respect d'une obligation légale (par exemple, les déclarations sociales obligatoires), soit utiles :

- **à la gestion administrative du personnel** (type de permis de conduire détenu, coordonnées de personnes à prévenir en cas d'urgence, numéro de sécurité sociale, informations bancaires, etc.). Attention le numéro de sécurité sociale ne peut-être traité, sauf cas très spécifiques, que pour la paye et les déclarations sociales obligatoires.
- **à l'organisation du travail** (photographie du salarié pour les annuaires internes et organigrammes, etc.)
- **à l'action sociale prise en charge par l'employeur** (informations concernant les ayants droit du salarié, etc.).

Les données collectées doivent être adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Quelles formalités pour le traitement de données personnelles ?

Les salariés doivent être informés du traitement de leurs données personnelles de façon claire et précise. Cette information peut se faire sur différents supports comme le règlement intérieur de l'entreprise ou encore le contrat de travail.

Elle doit notamment inclure :

- l'identité ;
- les coordonnées du Délégué à la Protection des Données (DPD) ;
- la durée de conservation des données ;
- la finalité du traitement ;
- les droits du salarié (droit d'accès, de rectification ou d'effacement, droit d'introduire une réclamation, etc.).

Par exemple, l'information du salarié est obligatoire en cas d'instauration d'un dispositif de vidéosurveillance, de contrôle des horaires, de géolocalisation des véhicules, ou encore d'enregistrement et écoute téléphonique.

La collecte de certaines données, comme des photos d'identité, impose l'obtention préalable du consentement du salarié, qui doit être recueilli de façon explicite et non équivoque.

Combien de temps conserver les données personnelles ?

Les données personnelles des salariés ne peuvent être conservées que pour la durée nécessaire :

- à l'exécution de leur contrat de travail ;
- ou/et au respect d'obligations légales (fiscales et sociales) ;
- ou/et à l'accomplissement de l'objectif qui était poursuivi lors de la collecte.

Quelques illustrations :

- les données relatives à un candidat doivent être effacées au plus tard 2 ans après le dernier contact ;
- la conservation des données relatives aux accès aux locaux est limitée à 3 mois après leur enregistrement ;
- la conservation des données relatives à la gestion de la paie ou au contrôle des horaires des salariés est limitée à 5 ans ;
- la conservation des données figurant dans un dossier médical peut aller jusqu'à 10 ans à compter de la consolidation du dommage.

Comment garantir la sécurité et la confidentialité des données ?

Toute entreprise doit garantir la protection des données personnelles de ses salariés ainsi que leur confidentialité. Le responsable du traitement, autrement dit l'employeur, doit déterminer et mettre en place les mesures techniques et organisationnelles nécessaires pour assurer la confidentialité des données personnelles des salariés afin d'éviter toute divulgation. Il doit à ce titre :

- **garantir la sécurité physique des lieux ou des serveurs et des dispositifs informatiques ;**
- **limiter l'accès aux données personnelles** en définissant clairement les données auxquelles chaque personne a légitimement accès. Par exemple, dans l'hypothèse où la personne chargée de la paie et celle chargée du recrutement sont deux personnes distinctes, elles ne devront pas avoir accès aux mêmes données personnelles, des informations différentes étant nécessaires à l'exercice de leurs fonctions ;
- **contrôler l'accès aux données personnelles** afin de s'assurer que seules les personnes habilitées en prennent connaissance. Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées afin de savoir qui se connecte à quoi, quand et pour faire quoi.

  L'employeur ne peut exiger qu'un salarié tenu au secret professionnel par ses fonctions signe une clause de confidentialité. Le salarié reste toutefois tenu d'une obligation générale de discrétion et de loyauté inhérente au contrat de travail et peut à ce titre être sanctionné en cas de divulgation à des tiers (salariés compris) d'informations confidentielles dont il a eu connaissance dans l'exercice de ses fonctions.

Bonnes pratiques : Pour davantage de prudence encore, la CNIL encourage les employeurs à prévoir une charte dédiée à la protection des données en annexe du règlement de l'entreprise qui préciserait que les données personnelles sont des informations confidentielles ne devant pas être communiquées à des personnes non autorisées sous peine de sanction.

Rappelons que certaines données des salariés sont accessibles aux représentants des salariés. Les délégués du personnel peuvent consulter les données figurant dans le registre unique du personnel (nom, nationalité, fonction occupée, date d'entrée dans l'organisme, etc.).

Le Comité social et économique (CSE) peut, après information des salariés et en l'absence d'opposition, avoir accès à certaines données, afin de proposer des activités et des prestations adaptées

Quels droits pour les salariés ?

DROIT D'ACCÈS

Un salarié peut obtenir communication de l'ensemble des données personnelles le concernant, qu'elles aient fait l'objet d'un traitement automatisé ou non. Il a notamment le droit d'accéder aux données relatives à :

- son recrutement ;
- son historique de carrière ;
- sa rémunération ;
- l'évaluation de ses compétences professionnelles ;
- son dossier disciplinaire ou encore tout élément ayant servi à prendre une décision à son égard (mutation, promotion, augmentation...).

Ce droit peut s'exercer :

- sur place, auquel cas la réponse de l'employeur doit être immédiate (si cela relève du champ du possible),
- ou par écrit sur présentation d'un justificatif d'identité, auquel cas l'employeur devra répondre dans les meilleurs délais et dans un maximum d'un mois. Toutefois ce délai peut être prolongé de 2 mois compte tenu de la complexité et du nombre de demandes.

Bon à savoir : L'employeur peut s'opposer aux demandes manifestement abusives. Il lui reviendra toutefois de démontrer ce caractère abusif. Le refus doit être écrit, motivé et doit mentionner les voies et délais de recours.

DROIT À L'EFFACEMENT OU À L'OUBLI

Les données des salariés, comme tous les autres types de données personnelles, sont sujettes au droit à l'oubli de leurs titulaires. Ce droit n'est cependant pas absolu. Il est conditionné par la vérification d'un des motifs suivants :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées,
- le consentement de l'intéressé est retiré et lui-seul justifiait le traitement,
- le traitement initial est illicite.

Un employeur peut ainsi, par exemple, légitimement refuser de faire droit à la demande d'un ancien salarié d'effacer ses données personnelles si les périodes de prescription relatives aux contentieux ne sont pas encore écoulées. Il doit en revanche, s'agissant plus particulièrement du recrutement, supprimer les informations sur les candidats non retenus (CV, lettre de motivation, etc.), sauf si ces derniers acceptent expressément de rester dans le « vivier » de l'entreprise.

DROIT À LA PORTABILITÉ

Le droit à la portabilité permet à un salarié de récupérer les données le concernant pour son usage personnel. Il s'applique dès lors que les données sont traitées de manière automatisée et que le traitement est fondé sur la base de l'exécution d'un contrat de travail ou sur la base du consentement.

Le droit à la portabilité ne concerne pas les données des salariés traitées par les employeurs sur la base d'un intérêt légitime ou d'obligations légales.
Les demandes en matière de gestion des ressources humaines doivent donc être analysées au cas par cas.

Fiche 10 ÉVALUER LA DURÉE DE CONSERVATION DES DONNÉES

La **durée de conservation** des données varie selon leur nature et les objectifs poursuivis. Elle peut être librement déterminée par le responsable de fichiers, sauf contraintes légales :

La loi impose, par exemple, de conserver :

- 3 ans maximum les coordonnées d'un prospect qui ne répond à aucune sollicitation ;
- 5 ans les données relatives à gestion de la paie ou le contrôle des horaires des salariés ;
- 10 ans un dossier médical ;
- 1 mois des images dans le cas d'un dispositif de vidéosurveillance poursuivant un objectif de sécurité des biens et des personnes ;
- le temps de réalisation de l'opération de paiement lors d'un achat sur internet s'agissant des coordonnées de la carte bancaire du client, puis pendant 13 mois en archivage intermédiaire en cas de contestation du paiement. ;
- tous les 13 mois, il faudra redemander le consentement des visiteurs pour le traitement des cookies.

Les données présentant un intérêt historique, scientifique ou statistique ne sont pas concernées par la limitation de conservation.

Ainsi, au terme de la réalisation de l'objectif poursuivi (par exemple, l'achat d'un produit), les données doivent être :

- effacées ;
- ou archivées (voir ci-dessous) ;
- ou faire l'objet d'un processus **d'anonymisation**, afin de rendre impossible la « ré-identification » des personnes. Ces données n'étant plus considérées comme des données à caractère personnel, elles peuvent ainsi être conservées librement et valorisées notamment par la production de statistiques.

POUR ALLER PLUS LOIN

www.cnil.fr/fr/limiter-la-conservation-des-donnees

Fiche 11 FAIRE FACE À UN CONTRÔLE DE LA CNIL

Que contrôle la CNIL ?

La CNIL s'assure que le responsable de traitement ou le sous-traitant respecte, les dispositions relatives à la protection des données personnelles.

Les quatre catégories de contrôle :

- **sur place** : dans les locaux professionnels du responsable du traitement et/ou du sous-traitant avec accès aux serveurs et ordinateurs où sont stockées les données ;
- **sur pièces** : il concerne la demande de communication de documents ;
- **sur convocation** : elle parvient à la personne auditionnée au moins 8 jours avant la date du contrôle ;
- **en ligne** : il s'effectue au sein de la CNIL à partir d'une plateforme et d'une connexion internet dédiée. Il porte sur la consultation de données librement accessibles ou rendues accessibles, y compris par imprudence, négligence ou du fait d'un tiers. Généralement ces contrôles s'effectuent sur le dépôt de cookies et autres traceurs, les mentions d'information à l'attention des utilisateurs, la sécurité du site internet...

Ces différents modes de contrôle peuvent se combiner.

Constituent un délit d'entrave sanctionné d'un an de prison et de 15 000 euros d'amende :

- le refus de communiquer, la dissimulation, la destruction des renseignements et documents nécessaires au contrôle ;
- la communication d'informations non conformes au contenu initial des enregistrements ;
- la présentation d'un contenu sous une forme qui n'est pas directement accessible...

Comment anticiper un contrôle ?

Il est conseillé de prévoir une procédure interne en cas de contrôle inopiné de la CNIL et de la diffuser sur l'intranet de l'entreprise.

Le DPD aura également pour mission de former les salariés sur le déroulement d'un contrôle « Informatique et Libertés ».

Cette formation visera notamment à lister les points de vigilance suivants :

Prévenir le DPD en cas de contrôle : nom + coordonnées, vérifier l'identité des agents de contrôle de la CNIL en l'absence du DPD, lire attentivement l'ordre de mission de ces agents, cadrer l'objet du contrôle et identifier les documents demandés, conserver une copie de tout ce qui est remis aux dits agents, vérifier le PV à signer par le DPD ou le représentant légal de l'entreprise.

Etendue d'un contrôle sur place ?

Les membres et agents habilités de la CNIL peuvent recueillir sur place tout renseignement juridique ou technique, toute justification leur permettant d'apprécier le respect des dispositions légales. Ils peuvent demander copie de contrats (tels que les contrats de sous-traitance informatique), de formulaires, de dossiers papier, de bases de données...

Quelles sont les suites d'un contrôle ?

En fin de contrôle, un procès-verbal (PV) est dressé par les agents de la CNIL.

Le PV est ensuite notifié au chef d'entreprise et au responsable des traitements par lettre recommandée avec demande d'avis de réception. Ce dernier devra rassembler les documents demandés et fournir des explications supplémentaires par courrier, notamment s'il était absent, ou clarifier une situation.

1ère hypothèse : le contrôle est clôturé

Si les constatations effectuées ne suscitent pas d'observations ou lorsque les manquements observés ne justifient pas une procédure contentieuse, il est procédé à la clôture du contrôle. Il est toutefois très fréquent qu'un courrier d'observations accompagne le courrier de clôture.

2ème hypothèse : une mise en demeure est adressée à l'entreprise pour les manquements constatés

Si l'instruction du dossier montre que le responsable de traitement n'a pas répondu ou a fourni des réponses qui démontrent un manquement, une procédure de mise en demeure peut être prononcée par le président de la CNIL : celle-ci précise le ou les manquements constatés et indique le délai à respecter pour se mettre en conformité.

Si l'entreprise concernée prend des mesures pour se conformer à la loi dans le délai imparti, le dossier sera clos et la CNIL pourra être amenée à le mentionner sur son site.

Si les manquements constatés sont importants, le dossier sera transmis à la formation restreinte de la CNIL qui pourra prononcer des sanctions administratives.

Le chef d'entreprise ou son représentant (DPD) peut émettre des observations ou réserves en cas de contrôle sur place ou sur convocation.

Les contrôles de la CNIL sont réalisés à 62 % à sa propre initiative et à 17 % dans le cadre de l'instruction de plaintes.

73 % des contrôles de la CNIL sont effectués dans le secteur privé.

(Rapport annuel d'activités 2017 de la CNIL)

Fiche 12 PRÉVENIR LES SANCTIONS

A quelles sanctions s'expose une entreprise non conforme au RGPD ?

DES AMENDES ADMINISTRATIVES

Ces sanctions sont assez lourdes : elles relèvent de deux catégories en fonction de la gravité du manquement.

1er niveau de gravité : les défauts ou carences du plan de conformité de l'entreprise

Il s'agit de l'insuffisance ou l'inadaptation de mesures de sécurité ou des défauts :

- de désignation du DPD ou de tenue du registre lorsqu'ils sont obligatoires ;
- de mise en œuvre d'une analyse d'impact alors qu'elle apparaît nécessaire ;
- de notification à l'autorité de contrôle ou à la personne concernée de la violation de données à caractère personnel.

Les amendes peuvent atteindre **10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total.**

2ème niveau de gravité : les violations les plus sérieuses telles que :

- la violation des principes fondamentaux du traitement des données à caractère personnel (loyauté, transparence, minimisation du consentement non valide des mineurs...) ;
- le défaut de licéité du traitement ;
- la méconnaissance des droits des personnes concernées (droits à rectification, à l'oubli, à la portabilité des données ...) ;
- les transferts non conformes de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale.

Les amendes peuvent atteindre **20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.**

À ces sanctions s'ajoute également pour l'entreprise le fort impact réputationnel d'une faille dans la protection des données !

DES SANCTIONS PÉNALES

Elles peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.

DES DOMMAGES ET INTERETS

Un responsable du traitement est responsable du dommage qu'il a causé en cas de violation du RGPD. Un sous-traitant est également responsable du dommage causé s'il n'a pas respecté les obligations prévues par le RGPD ou s'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Comment les personnes dont les droits ont été violés peuvent-elles agir ?

Auprès de la CNIL :

- Dépôt d'une réclamation auprès de la CNIL ;

À l'encontre du responsable du traitement ou du sous-traitant :

- Recours juridictionnel contre le responsable du traitement ou le sous-traitant. La personne concernée peut agir seule ou mandater un organisme, une organisation ou une association. L'entité introduit alors une réclamation au nom de la personne y compris pour obtenir réparation ;
- L'action de groupe : procédure de poursuite collective, elle permet aux personnes victimes d'un même préjudice de la part d'un professionnel, de se regrouper et d'agir en justice.

Désormais, cette action de groupe inclura, en France, l'indemnisation des personnes concernées.

GLOSSAIRE

Analyse d'impact : document d'analyse des risques en matière de protection des données. Il permet de définir les mesures appropriées lorsqu'un risque élevé est susceptible d'exister pour les droits et les libertés des personnes concernées.

Anonymisation : processus par lequel des données personnelles sont irréversiblement altérées de telle façon que la personne concernée ne puisse pas être identifiée, directement ou indirectement, que ce soit par le responsable de traitement seul ou en collaboration avec une quelconque autre partie. Les techniques d'anonymisation consistent à transformer des données pour qu'elles ne se réfèrent plus à une personne réelle et/ou à les généraliser de façon à ce qu'elles ne soient plus spécifiques à une personne mais communes à un ensemble de personnes.

POUR ALLER PLUS LOIN

www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation
www.cnil.fr/sites/default/files/atoms/files/wp216_fr.pdf

Certification : mécanismes de certification pouvant être utilisés par les responsables du traitement ou les sous-traitants pour fournir des garanties appropriées, notamment dans le cadre des transferts de données à caractère personnel vers un pays-tiers ou une organisation internationale. Une certification ne diminue pas la responsabilité du responsable de traitement ou du sous-traitant mais peut l'aider à apporter la preuve des mesures techniques et organisationnelles prises pour se mettre en conformité. La certification peut être délivrée par un organisme de certification ou par l'autorité de contrôle (à savoir la CNIL).

Code de conduite : les associations et autres organismes représentant des catégories de responsables de traitement ou de sous-traitants peuvent élaborer des codes de conduite afin de préciser les modalités d'application du RGPD telles que le traitement loyal et transparent des données à caractère personnel, les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques, la collecte des données à caractère personnel, les mesures de sécurité et de confidentialité, les informations communiquées au public et aux personnes concernées, l'exercice des droits, la protection des données des enfants, le transfert des données à des pays tiers ou des organisations internationales ou les procédures extra-judiciaires et autres procédures de règlement des litiges. Le projet de code de conduite doit être soumis à la CNIL qui l'approuvera s'il offre des garanties appropriées suffisantes au regard du RGPD.

Comité européen de la protection des données (CEPD) : l'autorité européenne de la protection des données dont le rôle est de surveiller et garantir la bonne application du Règlement général sur la protection des données, de publier des lignes directrices, recommandations et bonnes pratiques. Créé en 2018, le CEPD remplace le G 29 (ancienne appellation). Il se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données ou de leurs représentants respectifs.

Commission Nationale de l'Informatique et des Libertés (CNIL) : autorité administrative indépendante de régulation. Elle dispose du pouvoir de mener des enquêtes, adopter des mesures correctrices, infliger des sanctions, émettre des avis, accompagner et conseiller le public.

POUR ALLER PLUS LOIN

www.cnil.fr/professionnel

Consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement :

- s'il est donné par écrit, le consentement ne doit pas avoir été noyé sous d'autres questions ;
- la personne concernée a le droit de retirer son consentement à tout moment ;
- concernant les services en ligne adressés aux enfants, le traitement est licite s'il est consenti par un mineur de plus de 15 ans ou par le titulaire de l'autorité parentale ;
- le responsable de traitement doit pouvoir prouver que la personne concernée a donné son consentement.

Données à caractère personnel (ou données personnelles) : toute information se rapportant à une personne physique identifiée ou identifiable. Cette identification peut être directe ou indirecte, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, une photo, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données sensibles : données à caractère personnel, qui, par nature, sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux et méritent donc une protection spécifique. Il s'agit des données qui révèlent :

- l'origine (raciale, ethnique) ;
- des convictions ou pratiques (les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, la vie sexuelle) ;
- l'état de santé (données génétiques, données concernant la santé, données biométriques).

DPD (ou Data Protection Officer – DPO -) : le Délégué à la protection des données est la personne chargée de s'assurer que les dispositions du RGPD sont bien mises en œuvre dans l'entreprise qui l'a désignée. Il peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

POUR ALLER PLUS LOIN **www.cnil.fr/fr/designation-dpo**

Droit à la limitation du traitement :

- lorsque l'exactitude des données personnelles est contestée (pendant une durée permettant la vérification par le responsable de traitement) ;
- lorsque le traitement est illicite et la personne concernée s'oppose à leur effacement ;
- lorsque le responsable de traitement n'a plus besoin des données personnelles qui sont toujours nécessaires à la personne concernée ;
- lorsque la personne concernée a fait valoir son droit d'opposition, pendant la période de vérification de l'existence motifs légitimes dans l'intérêt public.

Droit à la portabilité des données : droit de récupérer et/ou de transmettre les données personnelles à un autre responsable de traitement quand le traitement est fondé sur le consentement et qu'il est effectué à l'aide de procédés automatisés.

Droit à l'effacement[1] : possibilité pour la personne concernée d'obtenir l'effacement de ses données lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées :

- lorsque la personne concernée retire son consentement (et qu'il n'existe pas d'autres fondements juridiques au traitement) ;
- lorsque la personne concernée s'oppose au traitement de ses données personnelles dans l'intérêt public en l'absence de motif légitime impérieux ;
- lorsque les données personnelles ont fait l'objet d'un traitement illicite ;
- lorsque les données personnelles ont été collectées auprès d'un enfant dans le cadre de l'"offre de services de la société de l'information".

Limitation de la conservation : les données personnelles doivent être conservées sous une forme permettant l'identification pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées sauf finalité archivistique, de recherche, statistique.

Objet du traitement : le fichier a pour finalité la gestion clients, la gestion de ressources humaines et de lutter contre la fraude.

Personne concernée : Personne dont les données sont recueillies à des fins de traitement.

Pseudonymisation : processus par lequel les données à caractère personnel sont traitées de telle façon qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Registre des activités de traitement : outil permettant aux responsables du traitement et sous-traitants de recenser sous forme écrite y compris électronique, les traitements effectués et de prouver, le cas échéant, le respect des obligations imposées par le RGPD. Il doit être mis à disposition de l'autorité de contrôle sur demande.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Il peut s'agir d'un représentant légal de l'entreprise qui prend l'initiative de constituer un fichier.

RGPD : règlement [UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données appelé, plus communément, le règlement général sur la protection des données. Il s'applique au traitement des données à caractère personnel, automatisé en tout ou en partie, au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Il ne s'applique pas au traitement des données à caractère personnel effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ou par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites par les États membres dans les domaines de politique étrangère et de sécurité commune.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Il s'agit du prestataire informatique qui va, pour le compte du responsable de traitement, collecter des données, assurer des mailings lors d'une opération marketing (voire sous-traiter la prestation demandée) sur instruction du responsable de traitement.

** Sauf si le traitement est nécessaire pour :*
- *l'exercice de la liberté d'expression*
- *respecter une obligation légale*
- *des motifs d'intérêt public de santé*
- *les archives, la recherche ou les statistiques*
- *l'exercice d'un droit en justice*

Traitement de données à caractère personnel : 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, contenues ou destinées à être contenues dans un fichier 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. Les procédés utilisés peuvent être très sophistiqués (un progiciel spécifique destiné à gérer les ressources humaines ou lutter contre la fraude, par exemple) ou rudimentaires (un tableur ou même la constitution de dossiers papier pour autant qu'ils soient structurés selon des critères déterminés).

Traitement à grande échelle : traitement qui vise à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational et qui peut affecter un nombre important de personnes.

Traitement automatisé : toute opération aboutissant à la constitution informatique de fichiers ou de bases de données, et ce quel que soit le moyen ou le support informatique, ainsi que toute procédure de consultation, de télétransmission d'informations nominatives, quel que soit le moyen de télécommunication utilisé.

Violation des données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

La CCI Paris Ile-de-France représente et informe les entreprises. Dans le cadre de ces missions, elle encourage et soutient les projets destinés à accompagner celles-ci, afin de leur permettre de se mettre en conformité avec un nouvel environnement juridique, dans le souci essentiel de préserver leur compétitivité.

Ont rédigé ce guide :

Céline Delacroix, *Secrétaire générale de la Commission commerce, CCI Paris Ile-de-France*
Nathalie Huet, *Expert en droit des affaires, CCI Paris Ile-de-France*
Florence Jacquemot, *Expert en droit public, CCI Paris Ile-de-France*
Aurélie Marseille, *Expert en droit social, CCI Paris Ile-de-France*
Pierre-Arnaud Moreau, *Chargé de mission, CCI Paris Ile-de-France*

Remerciements pour leur éclairage :

Joël Thiery, *membre élu de la CCI Paris Ile-de-France*
Pascal Beaudoin, *membre élu de la CCI Paris Ile-de-France*
Eric Delisle, *Juriste, CNIL*
Jean-Noël de Galzain, *Président de Wallix*
Emmanuel Poidevin, *Président de e-attestations.com*
Amandine Pepers, *Responsable Inforeg, CCI Paris Ile-de-France*
Rémy Tingaud, *Juriste à Inforeg, CCI Paris Ile-de-France*

Contact presse
Isabelle de Battisti
tél. : +33 1 55 65 70 65
idebatisti@cci-paris-idf.fr

Conception : CCI Paris IDF / Cicero 3511-2018 - Juin 2018 - Photos © : AdobeStock - IStock-GettyImages

CCI PARIS ILE-DE-FRANCE

27 avenue de Friedland
75382 Paris cedex 08

www.cci-paris-idf.fr

www.cci-paris-idf.fr/etudes et sur Twitter (@CCIParisIDF_Vox)