Niveau 3

Implémentation : violation de données, transferts et contrat de sous-traitance

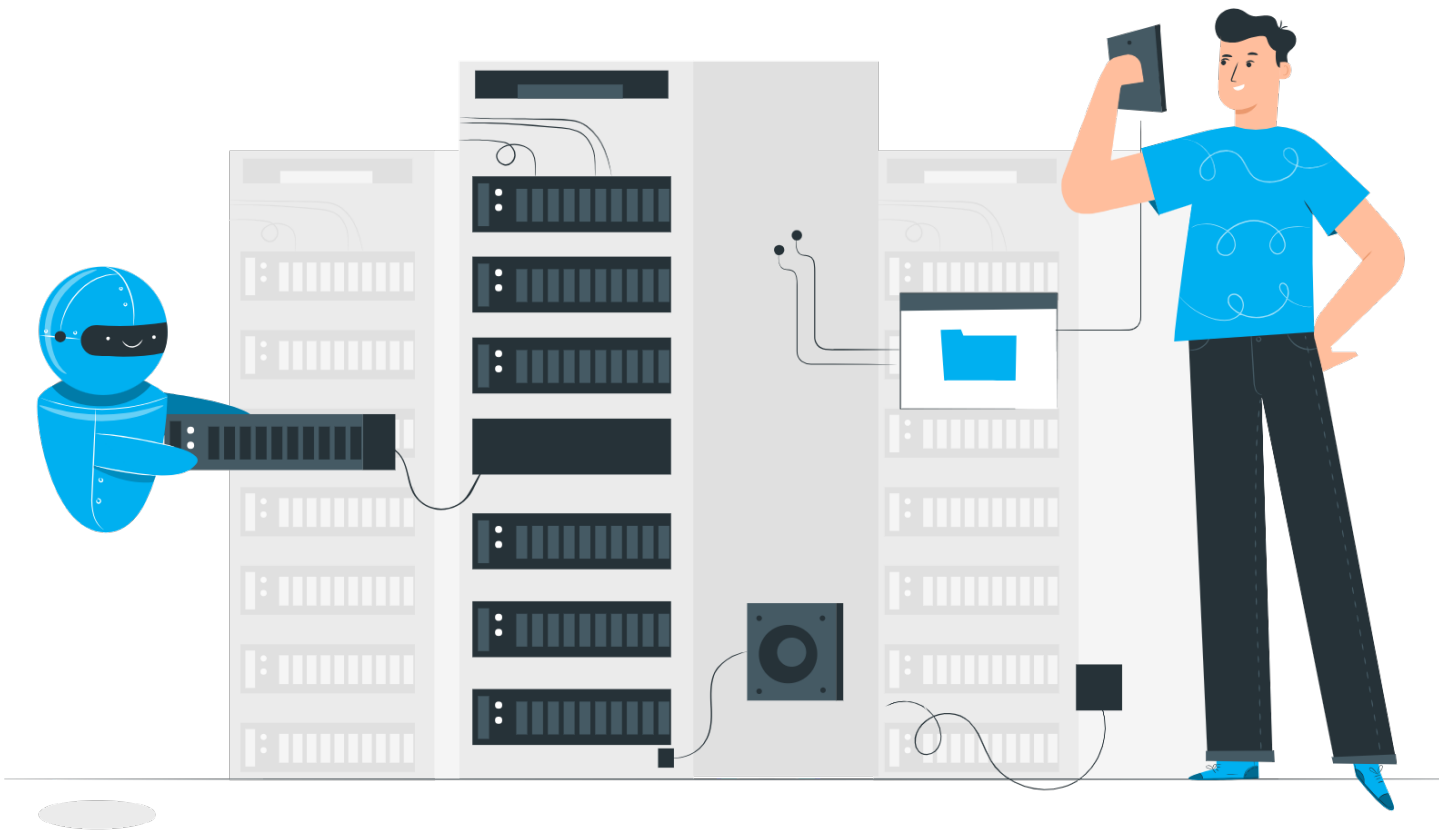
Mots clés : anonymisation - chiffrement (cryptage) - clauses contractuelles types - confidentialité - contrat de sous-traitance - données personnelles des employés - droits et libertés des personnes physiques - information des personnes concernées - mesures de sécurité techniques et organisationnelles - notification, pays tiers - pseudonymisation - registre des violations - responsabilité - risques - transferts - violation de données

Luxembourg House of Cybersecurity

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES
National Commission for Data Protection
Grand-Duchy of Luxembourg

Co-funded by the European Union

Mise à jour : 4 Juin 2024



Bon à savoir

Luxembourg House of Cybersecurity (LHC)

LHC est l'épine dorsale de la cyber- résilience de pointe au Luxembourg et vise à capitaliser et à développer davantage l'innovation, les compétences, la collaboration et le renforcement des capacités.

En tant qu'acteur central, le LHC abrite tous les types d'activités liées à la cyber sécurité. Avec ses deux centres, à savoir le CIRCL (Computer Incident Response Center Luxembourg) et le NC3 (National Cybersecurity Competence Center) et avec des partenaires clés, LHC soutient, nourrit et dessert un large éventail de secteurs, tels que les secteur privés, publique, la santé, l'éducation, l'insdustrie.

Computer Incident Response Center Luxembourg

CIRCL est une initiative gouvernementale conçue pour recueillir, examiner, signaler et répondre aux menaces et incidents de sécurité informatique.

CIRCL fournit un point de contact fiable et de confiance pour tous les utilisateurs, entreprises et organisations basés au Luxembourg, pour le traitement des attaques et des incidents. L'objectif de CIRCL est de recueillir, d'examiner, de signaler et de répondre aux cyber menaces de manière systématique et rapide.

1. Les notions en matière de violation de données

Qu'est-ce qu'une violation de données

Une violation de données à caractère personnel est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou 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.

Les violations de données peuvent être catégorisées selon les trois principes bien connus de la sécurité de l'information :

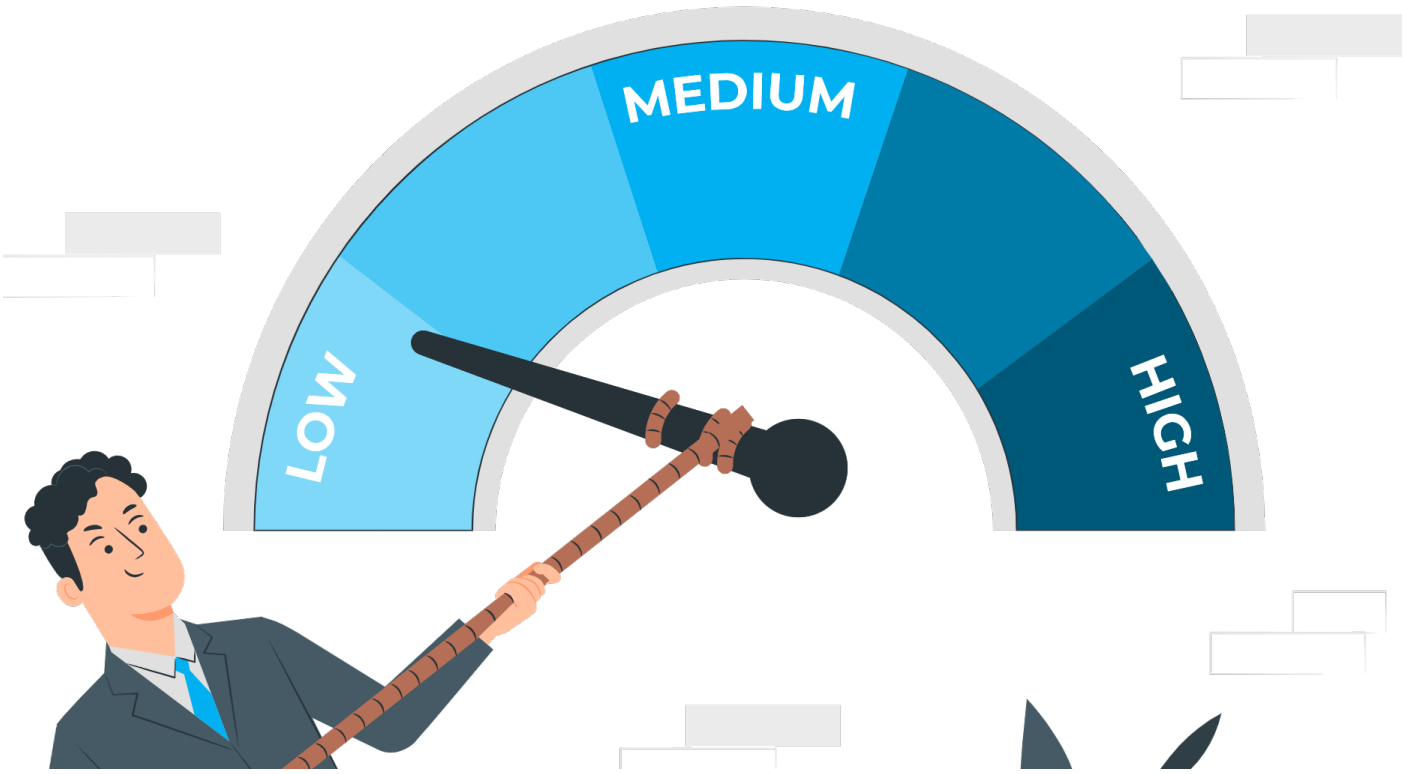
- **Violation de confidentialité :** en cas de divulgation ou d'accès non autorisé ou accidentel à des données à caractère personnel
- **Violation de disponibilité :** en cas de perte ou de destruction accidentelle ou non autorisée de données à caractère personnel
- **Violation d'intégrité :** en cas de modification accidentelle ou non autorisée de données à caractère personnel

Dépendant des circonstances, une violation peut concerner la confidentialité, l'intégrité et la disponibilité au même moment, ainsi que toute combinaison de ces 3 principes.

Considérant 85 du RGPD: « Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important.»

Que doit-on faire en cas de violation de données ?

Le responsable du traitement doit identifier si la violation de données présente un risque pour les individus concernés. Le responsable de traitement peut se servir de ses réponses aux informations demandées dans le formulaire de notification comme base pour déterminer si la violation présente un risque pour les personnes concernées.



Quand et comment notifier la CNPD ?

Si la violation de données présente un risque pour les personnes, une notification de celle-ci à la Commission nationale est requise dans un délai de 72 heures après en avoir pris connaissance.

Le formulaire peut être utilisé pour effectuer la notification.

La notification doit, à tout le moins:

1. Décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
2. Communiquer 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;
3. Décrire les conséquences probables de la violation de données à caractère personnel;
4. Décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

La notification de la violation peut être transmise à l'adresse email databreach@cnpd.lu. Vous pouvez utiliser la clé publique gpg téléchargeable sur le site de la CNPD, pour sécuriser la transmission des informations en les chiffrant.

Bon a savoir:

Le risque se définit entre autres par le degré de sensibilité des données traitées ainsi que de la sévérité et la probabilité d'impact sur les droits et libertés des personnes concernées (impacts corporels, matériels, moraux...). Par exemple, la gestion des membres d'une ASBL nécessite un degré de sécurité moins élevé que la gestion d'un dossier médical par un médecin.

Bon a savoir:

La référence aux droits et libertés des personnes physiques vise principalement la protection des données et la protection de la vie privée mais s'étend également, le cas échéant, à d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion.

Quand et comment informer les personnes concernées par la violation de données ?

Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais. La communication à la personne concernée doit décrire, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

1. 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;
2. Une description des conséquences probables de la violation de données à caractère personnel;
3. Une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le moyen de communication utilisé pour contacter les personnes concernées doit être effectif, c'est-à-dire qu'il faut s'assurer que les personnes concernées reçoivent avec une forte probabilité les informations communiquées. Si cela s'avère nécessaire, une communication publique peut être requise.

La tenue d'un registre des violations

Que le risque soit élevé ou inexistant, le responsable du traitement doit documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.

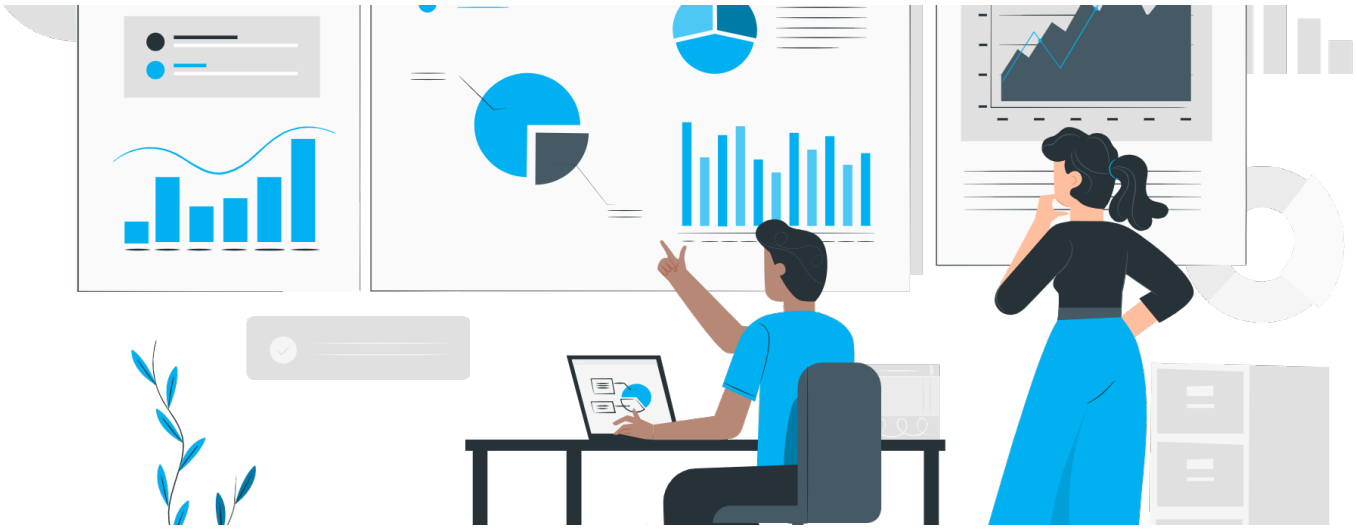
La Commission nationale peut demander l'accès à cette documentation pour vérifier le respect des obligations par le responsable de traitement ou le sous-traitant liées à la gestion des violations de données.

Que va faire la CNPD suite à la réception de la notification ?

Dès réception de la notification, la Commission nationale va :

- Envoyer un accusé de réception électronique (à la même adresse qui l'a envoyée) ;
- Vérifier la notification et, le cas échéant,
- contacter le responsable de traitement pour vérifier l'authenticité de la notification ;
- En fonction des circonstances revenir vers le responsable de traitement en cas de questions – dont notamment la nécessité de contacter les personnes concernées ou pas.

Le traitement de la notification par la Commission nationale sera fortement axé sur la gestion de l'incident par le responsable de traitement et, le cas échéant, sur la communication aux personnes concernées.



Les responsabilités des sous-traitants

Les sous-traitants ont la responsabilité de mettre en place des mesures organisationnelles et techniques pour être en mesure d'informer dans le meilleur délai le / les responsable(s) de traitement d'un incident sur des données à caractère personnel afin que ce dernier soit en mesure de respecter le délai de notification de 72 heures après la détection de l'incident.

Que faire après la gestion de la violation de données ?

Il est important pour une entité d'adapter les mesures de sécurité organisationnelles et techniques à ses traitements pour éviter que le même type de violation puisse se reproduire.

Confidentialité de la violation

Il n'est pas du ressort de la Commission nationale de rendre publique une violation de données. Toutefois, un responsable de traitement peut être amené, par sa décision propre ou sur demande de la Commission nationale, à communiquer publiquement sur une violation de données si celle-ci peut avoir un impact sur la vie privée, les droits et libertés des personnes concernées et que ces dernières ne peuvent pas être contactées efficacement par un autre moyen.

2. LES MESURES TECHNIQUES ET ORGANISATIONNELLES

Garantir un niveau de sécurité adapté au risque

L'une des exigences du RGPD est que les données à caractère personnel soient traitées de façon à garantir un niveau de sécurité approprié desdites données, et notamment à les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Le RGPD exige par conséquent des responsables du traitement et des sous-traitants qu'ils mettent en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les données à caractère personnel traitées. Ils devraient tenir compte de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques. Le RGPD exige également que toutes les mesures de protection techniques et organisationnelles appropriées soient mises en oeuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite, ce qui déterminera si l'obligation de notification s'applique.

À la suite d'un incident, il est important pour une entité d'adapter les mesures de sécurité organisationnelles et techniques à ses traitements pour éviter que le même type de violation puisse se reproduire.

Illustrations de mesures de sécurité

- **Le chiffrement ou cryptage**

Le cryptage des données traduit les données sous une autre forme, ou code, de sorte que seules les personnes ayant accès à une clé secrète (appelée clé de décryptage) ou à un mot de passe peuvent la lire. Les données chiffrées sont communément appelées texte chiffré, tandis que les données non chiffrées sont appelées texte en clair ou donnée en clair. Actuellement, le chiffrement est l'une des méthodes de sécurité des données les plus populaires et les plus efficaces utilisées par les entreprises.

L'état des connaissances actuelles est à prendre en compte, une technologie désuète ne sera pas considérée comme valide.

- **La pseudonymisation**

La pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénoms, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Contrairement à l'anonymisation, la pseudonymisation est une opération réversible : il est possible de retrouver l'identité d'une personne si l'on dispose d'informations supplémentaires.

- **L'anonymisation**

L'anonymisation est un traitement de données personnelles qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute ré-identification de la personne, par quelque moyen que ce soit. Cette opération est irréversible, de sorte qu'il n'est plus possible de retrouver l'identité d'une personne.

L'anonymisation ouvre des potentiels de réutilisation des données et permet ainsi aux acteurs d'exploiter et de partager leur « gisement » de données sans porter atteinte à la vie privée des personnes. Elle permet également de conserver des données sans limitation.

Il est à noter qu'en pratique l'anonymisation est une technique destructrice d'information. Il est donc conseillé d'avoir recours à l'anonymisation lorsqu'on :

- Dispose de quantités suffisantes de données
- A une idée précise de l'utilisation qui sera faite des données anonymisées
- Est en mesure de mettre en oeuvre une méthode d'anonymisation qui conservera les propriétés souhaitées du jeu de données.

Pour construire un processus d'anonymisation pertinent, il est conseillé de :

- Examiner les catégories de données à anonymiser (données structurées ou non, séries temporelles, informations de géolocalisation, etc.)
- Supprimer les éléments d'identification directe ainsi que les valeurs rares qui pourraient permettre une réidentification aisée des personnes (par exemple, la connaissance précise de l'âge des individus présents dans un jeu de données peut permettre dans certains cas de réidentifier très facilement les personnes centenaires)
- Distinguer les informations importantes des informations secondaires ou inutiles (c'est-àdire supprimables, qu'il est préférable de ne pas collecter du tout en vertu du principe de minimisation des données)
- Définir la finesse idéale et acceptable pour chaque information conservée
- Définir les priorités (exemple : est-il plus important de conserver une grande finesse sur telle information ou de conserver telle autre information ?).

MAÎTRISER LES TRANSFERTS DE DONNEES VERS LES PAYS TIERS !

Qu'est-ce qu'un pays tiers ?

Un pays tiers est un pays qui n'est pas lié par le règlement général sur la protection des données (RGPD), contrairement aux 27 États membres de l'UE et aux trois pays de l'Espace économique européen (EEE), la Norvège, le Liechtenstein et l'Islande.

Transfert au sein de l'Espace Economique Européen

Les données à caractère personnel peuvent circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande), tant que les principes généraux du RGPD sont respectés.

En effet, les États membres appliquent le même niveau de protection lors du traitement de données à caractère personnel. Un transfert au sein de l'Espace économique européen est par conséquent régi de la même manière qu'un transfert au Luxembourg et doit par conséquent respecter les principes généraux du RGPD (respect notamment du principe de licéité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

Transfert vers un pays tiers reconnu comme assurant un niveau de protection adéquat

Les pays tiers peuvent être reconnus comme assurant un niveau adéquat de protection des données à caractère personnel afin de permettre le transfert de données à caractère personnel au départ des États membres de l'UE et de l'EEE vers ces pays.

À ce jour, la Commission européenne a reconnu qu'Andorre, l'Argentine, le Canada (uniquement les organisations commerciales), la Corée du Sud, les Îles Féroé, Guernesey, Israël, l'Île de Man, le Japon, Jersey, la Nouvelle-Zélande, le Royaume-Uni, la Suisse, l'Uruguay et les États-Unis (uniquement pour les organisations commerciales participant au EU-US Data Privacy Framework) fournissaient un niveau de protection adéquat (en date du 1er janvier 2024).

Cette décision a pour effet que des données à caractère personnel peuvent être transférées des États membres de l'UE et de l'EEE vers le pays tiers concerné (dans les limites du champ d'application matériel décrit par chaque décision) sans exigences supplémentaires.

TRANSFERT VERS UN PAYS TIERS NON RECONNU COMME ASSURANT UN NIVEAU DE PROTECTION ADÉQUAT

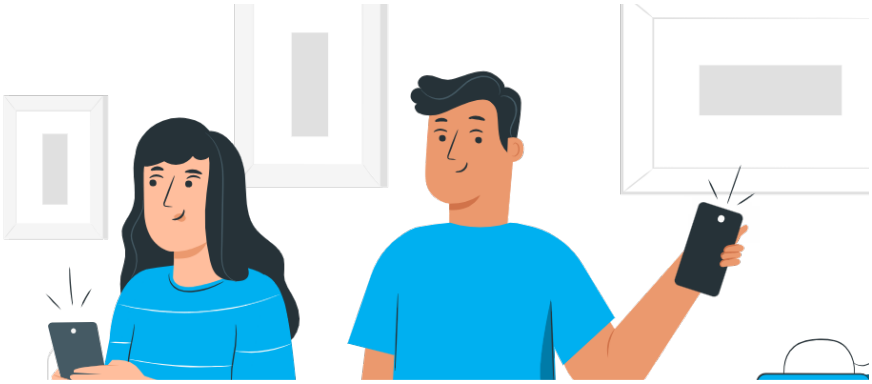
Diverses possibilités de garanties s'offrent aux responsables de traitement ou sous-traitants qui souhaitent transférer des données personnelles vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat.

Ces responsables du traitement et sous-traitants peuvent notamment s'appuyer sur les clauses contractuelles types (CCT) adoptées par la Commission européenne, qui constituent en quelque sorte des modèles de contrat de transfert de données personnelles. Ces CCT ont été mises à jour le 4 juin 2021 et remplacent les CCT précédemment applicables. Elles sont distinctes des CCT pour les relations de soustraitance. Il s'agit des garanties appropriées les plus adaptées aux petites et moyennes entreprises.

Les règles d'entreprise contraignantes (en anglais « binding corporate rules », ou BCR) permettent d'assurer un niveau de protection suffisant aux données transférées au sein d'un groupe d'entreprise tant à l'intérieur qu'à l'extérieur de l'Espace économique européen. Cette garantie appropriée se prête surtout aux groupes internationaux d'entreprises mettant en oeuvre un grand nombre de transferts internationaux de données.

Depuis l'entrée en application du RGPD le 25 mai 2018, de nouvelles possibilités s'offrent aux responsables de traitement ou sous-traitants qui souhaitent transférer des données personnelles vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat. Il s'agit :

- De codes de conduite approuvés conformément à l'article 40 du RGPD, assortis de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; et
- De mécanismes de certification approuvés conformément à l'article 42 du RGPD, assortis de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.



Accordez de l'interet au contrat de sous-traitance (art 28 rgpd) !

Pourquoi encadrer la sous-traitance des données ?

Le responsable du traitement conserve la responsabilité globale de la protection des données personnelles, mais le sous-traitant a un rôle important à jouer pour permettre au responsable du traitement de respecter ses obligations et cela inclut la notification de violation.

Quelles sont les obligations des sous-traitants (nonexhaustif) ?

- Traiter les données à caractère personnel que sur instruction documentée du responsable du traitement

- Traiter les données à caractère personnel

uniquement pour la ou les finalités spécifiques du traitement

- Mettre en oeuvre les mesures techniques et organisationnelles pour assurer la sécurité des données à caractère personnel

- N'accorder aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat

- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité

- Appliquer des limitations spécifiques et/ou des garanties supplémentaires en cas de traitement de données sensibles

- Traiter de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données

- Permettre la réalisation d'audits des activités de traitement à la demande du responsable du traitement

- Recourir aux services d'un sous-traitant ultérieur pour mener des activités de traitement spécifiques, que sur autorisation écrite préalable, spécifique ou générale du responsable du traitement. Indépendamment de la nature spécifique ou générale de cette autorisation préalable, le sous-traitant initial doit tenir à jour une liste des autres sous-traitants.