FR

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Vos obligations en matière de protection des données

Guide pour les entreprises, organismes publics et associations

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette

cnpd.public.lu

accentaigu

À partir du 25 mai 2018, le règlement général sur la protection des données responsabilisera davantage les acteurs privés et publics ainsi que leurs sous-traitants. Ils devront en effet assurer à tout moment un respect des règles en matière de protection des données et être en mesure de le démontrer en documentant leur conformité.

Au Luxembourg, la Commission nationale pour la protection des données (CNPD) est chargée de vérifier la légalité des fichiers et de toutes collectes, utilisations et transmissions de données concernant des individus identifiables. Elle doit assurer dans ce contexte le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée.

[!] VOICI QUELQUES EXEMPLES DE DONNÉES À CARACTÈRE PERSONNEL :

- nom,
- adresse,
- matricule,
- données de santé,
- adresse e-mail,
- numéro de téléphone,
- opinion politique,
- etc.

[?] VOUS ENREGISTREZ, UTILISEZ OU TRAITEZ DES DONNÉES À CARACTÈRE PERSONNEL ?

Oui ? Alors le règlement s'applique et vous devez respecter les règles !

[?] VOUS TRAITEZ DES DONNÉES POUR LE COMPTE D'AUTRES ORGANISMES ?

Vous êtes aussi concerné.

[?] ÊTES-VOUS UN RESPONSABLE DU TRAITEMENT OU UN SOUS-TRAITANT ?

Responsable du traitement :
détermine les finalités et les moyens du traitement de données à caractère personnel

Sous-traitant :
traite des données à caractère personnel pour le compte du responsable du traitement

Vos obligations

Commencez à faire l'inventaire de tous les traitements de données personnelles que vous mettez en œuvre (p. ex. données des employés, des clients, etc.). Interrogez-vous notamment : quelle est la base légale et la finalité des traitements existants ? D'où proviennent les données et qui en sont les destinataires ? Où sont stockées les données et qui y a accès ?

[!] Veillez au respect des grands principes

Quand vous traitez des données à caractère personnel, vous devez respecter les principes suivants :

COLLECTEZ LES DONNÉES PERSONNELLES DE FAÇON LICITE, LOYALE ET TRANSPARENTE

La collecte, l'enregistrement, l'utilisation et la transmission de données personnelles doivent se faire en conformité au règlement, de bonne foi, et non pas à l'insu de la personne concernée.

NE COLLECTEZ PAS DES DONNÉES PERSONNELLES SANS FINALITÉ BIEN DÉTERMINÉE

Les données personnelles doivent être collectées pour des finalités (objectifs) déterminées, explicites et légitimes et ne peuvent pas être traitées d'une manière incompatible avec ces finalités (p. ex. une utilisation ultérieure pour une autre finalité).

APPLIQUEZ LE PRINCIPE DE MINIMISATION DES DONNÉES

Il faut traiter uniquement les données qui sont nécessaires à la réalisation des finalités.

VEILLEZ À CE QUE LES DONNÉES SOIENT EXACTES ET TENUES À JOUR

Vous devez prendre toutes les mesures raisonnables afin de garantir que les données personnelles inexactes sont rectifiées ou supprimées sans tarder.

DÉTERMINEZ UNE DURÉE DE CONSERVATION PROPORTIONNÉE

Les données ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées. Au-delà, les données doivent être supprimées ou anonymisées.

ASSUREZ L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

Il faut garantir une sécurité suffisante des données à l'aide de mesures techniques et organisationnelles appropriées, notamment contre un traitement non-autorisé ou illégal et contre la perte, destruction ou altération accidentelle des données.

DÉMONTREZ VOTRE CONFORMITÉ (« ACCOUNTABILITY »)

Vous devez prendre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.

[!] Identifiez la base juridique sur laquelle se fonde votre traitement

Pour être licite, un traitement de données doit se fonder sur l'une des six conditions suivantes :

1. le consentement de la personne concernée (distinct pour chaque finalité) ;
2. un contrat ;
3. une obligation légale (claire et précise) ;
4. l'intérêt vital de la personne concernée ou d'une autre personne ;
5. une mission d'intérêt public, ou encore ;
6. l'intérêt légitime du responsable de traitement (p. ex. à des fins de marketing, anti-fraude, traitement des données clients ou salariés, sécurité des traitements, etc.).

Le consentement doit être « libre, spécifique, éclairé et univoque », c'est-à-dire que la personne concernée doit avoir un véritable choix.

Si vous recueillez des données liées à des enfants via votre site web commercial (p. ex. jeux en ligne, réseaux sociaux), il est nécessaire d'obtenir l'accord des parents. L'information à l'égard des utilisateurs doit être facile à comprendre et formulée en termes simples et clairs.

[!] Identifiez les traitements nécessitant une vigilance particulière

VOUS TRAITEZ CERTAINS TYPES DE DONNÉES

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

VOTRE TRAITEMENT A POUR OBJET OU POUR EFFET

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

Si vos traitements répondent à l'une des caractéristiques énumérées ci-dessus, des mesures ou des règles particulières peuvent s'appliquer (exemples : analyse d'impact relative à la protection des données, information renforcée, recueil du consentement, clauses contractuelles, etc.).

[!] Protégez les données dès la conception

Intégrez des mesures de protection appropriées dès les premières étapes de développement de vos produits et services (« Data protection by design »). Vous devez adopter des mesures consistant à limiter par défaut le traitement à ce qui est strictement nécessaire (« Data protection by default »), p. ex. la mise en place d'un mécanisme automatique de suppression des données qui ne sont plus nécessaires.

Vérifiez que vos sous-traitants connaissent leurs obligations

Votre organisme ne peut choisir que des sous-traitants présentant des garanties suffisantes pour assurer la protection des données à caractère personnel qu'ils traitent. Assurez-vous de l'existence de clauses contractuelles précisant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.

Vérifiez les mesures de sécurité mises en place

Des mesures de sécurité appropriées tenant compte du risque pour la personne concernée et de la catégorie des données traitées doivent être mises en place par vous et par vos sous-traitants.

Notifiez les violations de données à la CNPD

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, vous devez en informer la CNPD et, dans certains cas, les personnes concernées.

Vérifiez si vous transférez des données hors de l'Union européenne

Si le pays vers lequel vous transférez les données n'est pas reconnu comme adéquat par la Commssion européenne, vous devrez encadrer vos transferts avec des outils assurant un niveau de protection suffisant et approprié des personnes concernées.

Respectez les droits des personnes concernées

1/ Le droit à l'information

Vous devez informer les personnes concernées que leurs données personnelles sont traitées, par qui et pourquoi. Cette information doit se présenter dans un langage simple et clair au moment même de la collecte des données, ou si les données n'ont pas été collectées auprès de la personne elle-même, de manière générale dans un délai raisonnable ne dépassant pas un mois.

2/ Le droit de contester une décision prise sur base de processus automatisés

Si vous prenez des décisions sur base de processus automatisés, y compris le profilage (p.ex. approbation d'une demande de crédit de consommation ou d'un contrat d'assurance), vous devez accorder aux personnes la possibilité de faire valoir leur point de vue et de contester, le cas échéant, la décision. Vous devez, en plus, informer les personnes concernées sur la logique qui sous-tend cette décision.

3/ Le droit d'accès

Si une personne vous demande si vous détenez des informations sur elle, vous devez confirmer que des données personnelles la concernant sont ou ne sont pas traitées, et, le cas échéant, lui communiquer une copie de l'intégralité des données que vous possédez à son sujet.

4/ Le droit de rectification

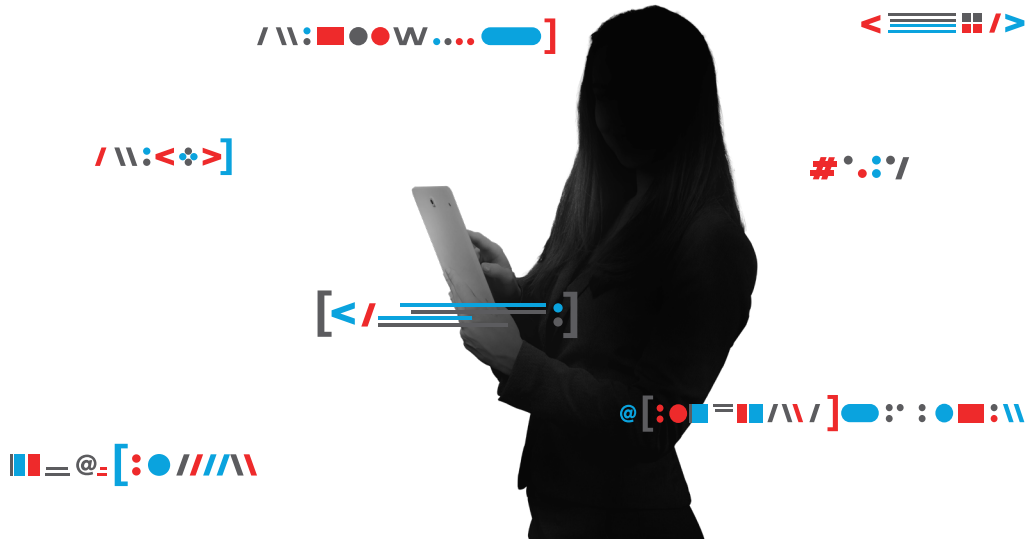
Vous avez l'obligation de veiller à ce que les données que vous collectez soient exactes et, si nécessaire, tenues à jour. À la demande d'une personne concernée, vous devez rectifier les informations inexactes.

5/ Le droit à l'oubli

Lorsqu'une personne ne souhaite plus que les données qui la concernent soient traitées, vous avez l'obligation de supprimer ces données à moins qu'un motif légitime ne justifie leur conservation. Un citoyen peut ainsi, par exemple, exiger le retrait immédiat de données à caractère personnel collectées ou publiées sur un réseau social alors qu'il n'était encore qu'un enfant et n'était pas pleinement conscient des risques inhérents au traitement.

6/ Le droit à la portabilité

Une personne concernée doit pouvoir récupérer les données qu'elle a communiquées à un organisme (dans un format structuré, couramment utilisé et lisible par machine) et les transmettre à un autre (réseau social, fournisseur d'accès à Internet, site de streaming, etc.).



7/ Le droit d'opposition

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel nécessaire à la poursuite de vos intérêts légitimes ou à l'exécution d'une mission d'intérêt public. Dans ce cas, vous devez arrêter le traitement, sauf si vous pouvez démontrer l'existence de motifs légitimes et impérieux pour continuer le traitement.

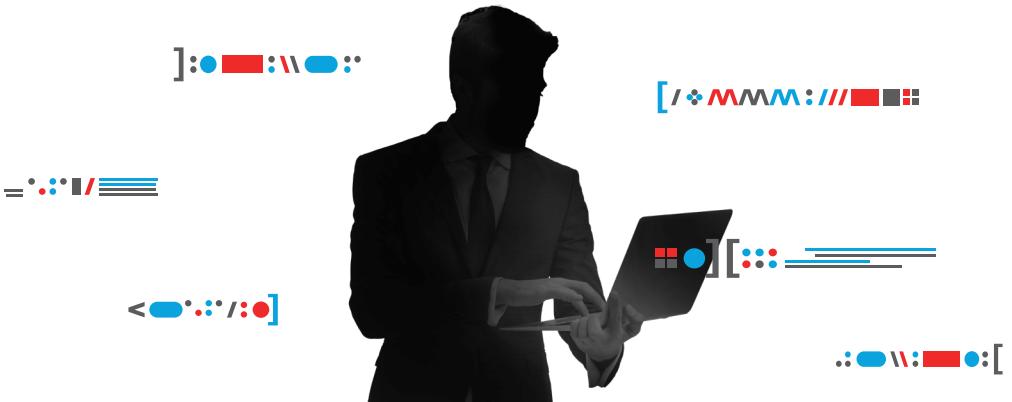
Vous devez aussi respecter le droit de la personne concernée de s'opposer, sans qu'elle doive fournir de justification, à l'utilisation de ses données à des fins de prospection commerciale ou de démarchage à orientation idéologique (partis politiques, syndicats, groupements religieux, etc.).

8/ Le droit à la limitation

La personne concernée peut revendiquer la limitation du traitement de ses données :

- lorsqu'elle conteste l'exactitude d'une donnée, le temps que vous puissiez vérifier celle-ci ;
- si le traitement est illicite et qu'elle s'oppose néanmoins à leur effacement, préférant une telle limitation ;
- quoique n'étant plus nécessaire, la personne concernée en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice.

En cas de limitation, les données ne peuvent plus faire l'objet d'un quelconque traitement. La limitation peut être effectuée selon diverses modalités (déplacement temporaire vers un autre fichier, verrouillage des données, retrait temporaire d'un site Internet, etc.).



Avez-vous besoin d'un délégué à la protection des données ?

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

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

Dans tous les autres cas, la désignation est facultative.

Dans quel cas dois-je désigner un délégué ?

OUI Vous traitez des données à caractère personnel pour diffuser des **publicités ciblées sur les moteurs de recherche** en fonction du comportement en ligne des personnes concernées.

OUI Vous êtes **une banque qui doit régulièrement et systématiquement suivre l'évolution des comptes et des transactions de ses clients** notamment dans le cas de ses obligations liées à la prévention de la fraude, du blanchiment d'argent ou du financement du terrorisme.

NON Vous envoyez une publicité à vos clients une fois par an pour promouvoir votre entreprise locale de denrées alimentaires.

NON Vous êtes un médecin généraliste et vous collectez des données sur la santé de vos patients.

OUI Vous traitez des données à caractère personnel portant sur **la génétique et la santé** pour le compte d'un établissement hospitalier.

Gérez les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devez mener, pour chacun de ces traitements, une **analyse d'impact relative à la protection des données** (A.I.P.D. ; en anglais, Data Protection Impact Assessment ou D.P.I.A.).

Une analyse d'impact est nécessaire si plusieurs des critères suivants s'appliquent :

- Le traitement effectue une évaluation ou notation, y compris le profilage et la prédiction.
- Le traitement conduit à une prise de décision automatique entrainant des implications légales ou similaires pour les personnes concernées.
- Le traitement consiste en une surveillance systématique des personnes concernées (traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris les données collectées à partir d'une surveillance systématique des lieux accessibles au public).
- Des données sensibles (suivant la définition de la réglementation) font l'objet du traitement.
- Le traitement est un traitement à grande échelle :
  - le nombre de personnes concernées est élevé ou proportionnellement élevé par rapport à une population ou ;
  - le volume de données traitées est important ou ;
  - la durée ou la permanence de l'activité de traitement est importante ou ;
  - l'étendue géographique du traitement est importante.
- Des ensembles de données à caractère personnel ont été combinés d'une manière qui pourrait dépasser les attentes raisonnables des personnes concernées.
- Les données traitées concernent des personnes vulnérables (ex : situation de déséquilibre des pouvoirs entre les personnes concernées et le responsable de traitement).
- Le traitement se rapporte à l'usage ou l'application de solutions technologiques ou organisationnelles innovantes.
- Le traitement de données ne permet pas aux personnes concernées d'exercer leur droit ou les empêche d'accéder à un service ou un contrat (ex : une banque qui analyse le profil de ses clients pour décider de leur offrir un crédit ou pas).

Dans quel cas dois-je mener une A.I.P.D. ?

OUI

Un hôpital traite les données de santé et les données génétiques de ses patients (système informatique de l'hôpital).

Facteurs de risque :

- données sensibles ;
- données concernent des personnes vulnérables ;
- traitement de données à grande échelle.

OUI

L'utilisation de **caméras pour surveiller le comportement** de conduite sur les autoroutes. Le responsable du traitement envisage d'utiliser un système d'analyse vidéo intelligent pour reconnaître automatiquement les plaques d'immatriculation des voitures.

Facteurs de risque :

- surveillance systématique ;
- solutions technologiques ou organisationnelles innovantes.

OUI

Une société **surveille l'usage de l'outil informatique** : Internet, e-mails, ordinateurs, logiciels, etc.

Facteurs de risque :

- surveillance systématique ;
- données concernent des personnes vulnérables.

NON

Un magazine en ligne qui utilise une liste de diffusion pour **envoyer un résumé quotidien** des actualités à ses abonnés.

Facteurs de risque :

- aucun risque élevé.

NON

Un site de commerce en ligne affiche des annonces pour des accessoires de voitures en utilisant du **profilage limité sur les derniers achats**.

Facteurs de risque :

- évaluation ou notation, mais pas systématique ou extensif.

Documentez vos traitements

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

Votre dossier devra notamment comporter les éléments suivants :

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants) ;
- les analyses d'impact relatives à la protection des données pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes ;
- l'encadrement des transferts de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications) ;
- le registre qui documente toutes les violations de données. Celui-ci renseigne les conséquences de la violation de données et les mesures prises pour y remédier.

L'INFORMATION DES PERSONNES

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

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

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

Attention : cette liste n'est pas exhaustive et les besoins de documentation peuvent varier d'un organisme à l'autre.

Soyez vigilants aux sanctions prévues

En cas de traitement contraire au règlement, la CNPD a, entre autres, le pouvoir d'ordonner l'effacement ou la destruction des données ou encore l'interdiction temporaire ou définitive d'un traitement (mesures correctrices).

La CNPD a encore le pouvoir d'imposer des amendes administratives allant jusqu'à €20 000 000 ou 4% du chiffre d'affaire annuel mondial.

Attention, s'il y a une violation du règlement, les personnes concernées disposent :

- d'un droit à un recours juridictionnel effectif en cas d'atteinte à leurs droits, tant contre le responsable du traitement que contre le sous-traitant ;
- d'un droit de réparation du préjudice matériel ou immatériel pouvant être obtenue du responsable du traitement ou du sous-traitant.

Contacter la Commission nationale pour la protection des données

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

1, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60-1 | Fax. : (+352) 26 10 60-29

Heures d'ouverture :
09h00-12h30 & 13h30-17h30

Pour vos questions ou commentaires, veuillez utiliser le formulaire en ligne disponible sur **cnpd.public.lu** section «Contact» ou envoyer un message à **info@cnpd.lu**