LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

SENSIBILISATION À LA PROTECTION DES DONNÉES

En collaboration avec :

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

PRÉFACE

Léif Lieserinnen a Lieser,

D'Vertraue vum Bierger an déi ëffentlech Instanzen ass e Pilier vun enger Demokratie. Den Dateschutz ass dofir essentiel. Mir all musse sécher goen, datt dëst Vertraue net verluere geet. D'Biergerinnen a Bierger musse sech drop verloosse kënnen, datt de Staat an d'Gemenge virsiichteg a responsabel mat perséinlechen Informatiounen ëmginn.

Jiddwer Eenzelen dréit a sengem Aarbechtsalldag eng grouss Verantwortung, fir de Schutz vun der Privatsphär vum Bierger ze garantéieren, an domat zum Erhalt vum Vertrauen an eis ëffentlech Institutioune bäizedroen.

Dës Publikatioun vum Kommissariat fir Dateschutz beim Staat ass an Zesummenaarbecht mat der nationaler Dateschutzkommissioun ausgeschafft ginn an ergänzt déi vill Dateschutz-Moossnamen, déi scho vun Ärer Entitéit geholl goufen, esouwéi d'Formatiounen iwwer den Dateschutz, déi vum INAP ugebuede ginn. Ech sinn dervun iwwerzeegt, datt dës Publikatioun zur Dateschutz-Kultur am ëffentlechen Déngscht bäidroe wäert.

Ech felicitéieren den Auteure fir hiert Wierk, dat Iech erlabt, d'Konzepter vum Dateschutz nach besser ze verënnerlechen a se an Ärem berufflechen Alldag unzewennen.

Ech wënschen Iech eng gutt Lektür.

Xavier BETTEL
Monsieur le Premier ministre,
Ministre des Communications et des Médias

Cette publication éditée par le Commissariat du Gouvernement à la protection des données auprès de l'Etat (CGPD), en collaboration avec la Commission nationale pour la protection des données (CNPD), s'inscrit dans l'objectif de sensibiliser les agents étatiques et communaux aux bases du Règlement Général sur la Protection des Données.

TABLE DES MATIÈRES

INTRODUCTION// 5

CHAPITRE 1//
Les principales notions du Règlement général sur la protection des données 9

CHAPITRE 2//
Les grands principes de la protection des données 13

Section 1 : La limitation des finalités du traitement 14
Section 2 : La licéité du traitement 16
Section 3 : La minimisation des données et des accès 22
Section 4 : L'exactitude des données 24
Section 5 : La limitation de la conservation des données 25
Section 6 : La sécurité des données 26
Section 7 : La transparence à l'égard de la personne concernée 27

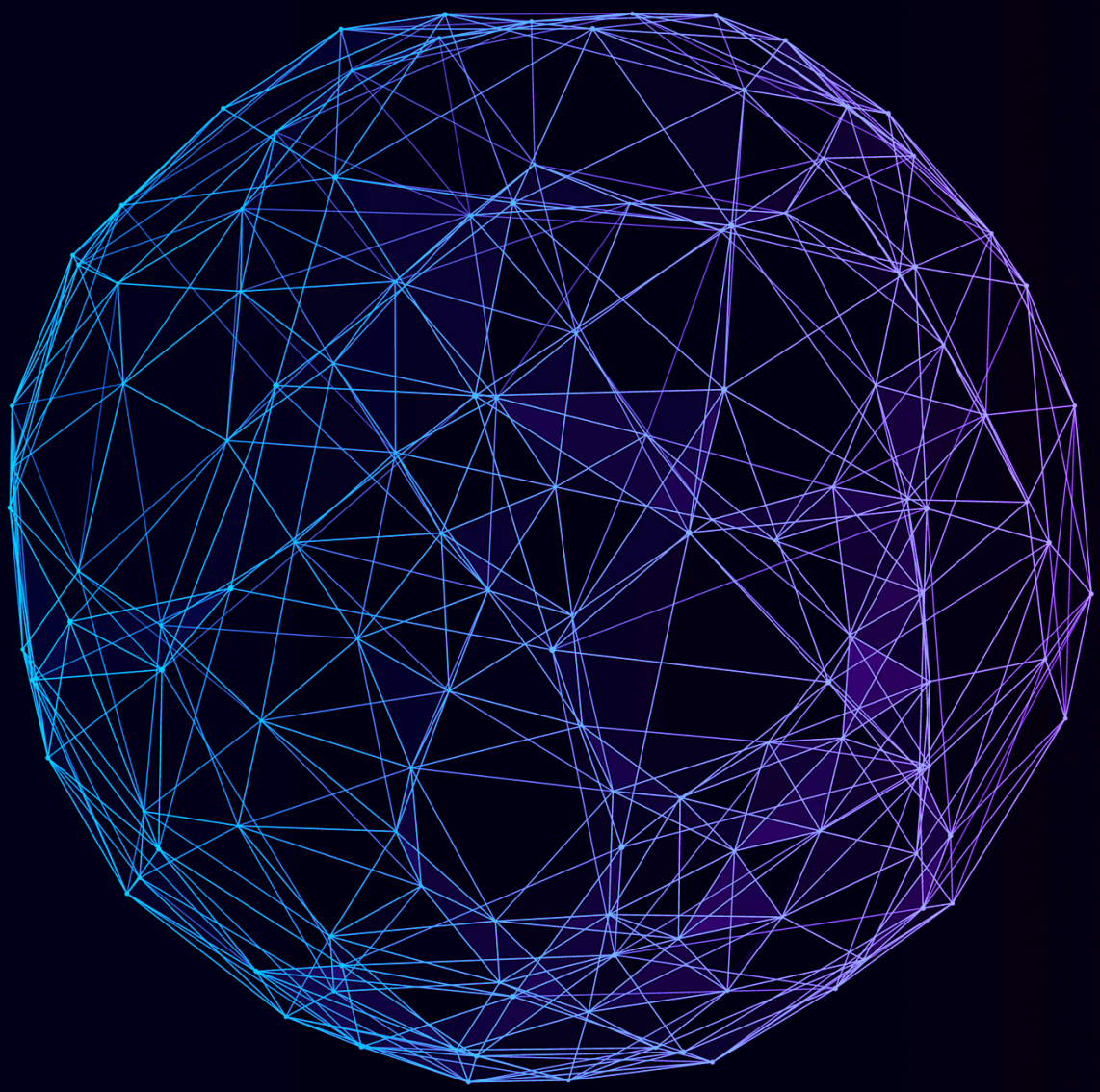
CHAPITRE 3//
L'exercice des droits de la personne concernée 29

CHAPITRE 4//
Les rôles et responsabilités des principaux acteurs 33

Section 1 : Le responsable du traitement et l'« accountability » 34
Section 2 : Les responsables conjoints du traitement 36
Section 3 : Le sous-traitant 36
Section 4 : Le Commissariat du gouvernement à la protection des données auprès de l'Etat (CGPD) 37
Section 5 : La Commission nationale pour la protection des données (CNPD) 38

CHAPITRE 5//
Le délégué à la protection des données et les outils essentiels de la conformité au RGPD 39

Section 1 : Le délégué à la protection des données 40
Section 2 : Le registre des activités de traitement 42
Section 3 : L'analyse d'impact relative à la protection des données 43
Section 4 : La gestion des violations de données 45



INTRODUCTION

INTRODUCTION

L'importance de veiller au respect de la protection des données.

Toute personne qui confie ses données à caractère personnel à une administration (entité étatique ou communale) attend d'elle un comportement exemplaire. Ses données lui sont précieuses, et toute atteinte injustifiée au droit à la vie privée et à la protection des données, risque de nuire à la confiance du citoyen envers nos institutions démocratiques.

Il est primordial que les agents de la fonction publique soient sensibilisés à la protection des données et aux risques qui peuvent découler de comportements inappropriés lors du traitement de données. En effet, **un agent bien sensibilisé à la protection des données contribue à la relation de confiance** qui doit impérativement subsister entre les citoyens et l'administration.

HISTORIQUE DE LA LÉGISLATION EN MATIÈRE DE PROTECTION DES DONNÉES

Le droit à la protection des données et le droit au respect de la vie privée sont étroitement liés. Ces droits assurent la protection de valeurs similaires. Cependant, bien qu'étroitement liés, ces droits sont distincts.

Le droit à la vie privée est apparu pour la première fois comme l'un des droits fondamentaux protégés **sur le plan international** au travers de la Déclaration universelle des droits de l'homme de 1948.

Sur le plan européen, la Convention européenne des droits de l'homme, entrée en vigueur le 3 septembre 1953, a consacré le droit à la vie privée.

Sur le plan national des Etats de l'Europe, la protection des données est apparue dans les années 1970 avec l'adoption – par certains législateurs nationaux – de législations visant à contrôler le traitement de données, en particulier par les autorités publiques.

Au Luxembourg, le législateur a adopté un cadre spécifique applicable aux banques de données implantées sur le territoire luxembourgeois par le biais de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques.

Ouverte à la signature le 28 janvier 1981, la Convention 108 du Conseil de l'Europe était le premier instrument international juridique contraignant dans le domaine de la protection des données.

Le premier instrument complet et harmonisé en matière de protection des données a été adopté au sein de l'Union européenne en 1995 avec la directive 95/46/CE. Cette directive a été transposée en droit luxembourgeois par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Suite à l'entrée en vigueur du Traité de Lisbonne en 2009, le droit à la protection des données a également été érigé au rang de droit fondamental européen par la Charte des droits fondamentaux de l'Union européenne.

Au fil du temps, l'évolution rapide des technologies et la mondialisation ont créé de nouveaux défis pour la protection des données et ont requis un cadre de protection des données plus cohérent pour l'Union européenne, assorti d'une application rigoureuse des règles visant la protection des données.

Fort de ce constat, le législateur européen a adopté **le règlement (UE) 2016/679** du 27 avril 2016 (règlement général sur la protection des données ; ci-après « RGPD »). Ce dernier a abrogé et remplacé la directive 95/46/CE.

Le RGPD est complété en droit interne luxembourgeois par les dispositions de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ainsi que par les législations sectorielles relatives au traitement de données (en particulier la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale).

TRANSITION DU MANUSCRIT AU DIGITAL

De plus en plus d'administrations traitent leurs dossiers de manière digitale. Ceci a pour avantage, notamment, de permettre aux usagers de ne plus devoir se déplacer et de pouvoir réaliser de nombreuses démarches en ligne à n'importe quel moment de la journée.

Cette **digitalisation** doit se réaliser de manière à assurer le respect de la protection des données afin de maintenir la relation de confiance entre l'administration et les citoyens.

CHAPITRE 1//
LES PRINCIPALES NOTIONS DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

CHAPITRE 1 :
LES PRINCIPALES NOTIONS DU RGPD

Qu'est-ce qu'une « donnée à caractère personnel » ?

Le RGPD définit une « donnée à caractère personnel » comme « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne physique est réputée être **« identifiable »** lorsqu'elle peut être **identifiée, directement ou indirectement**, notamment par référence à un identifiant, tel qu'un nom, le numéro de matricule ou un autre numéro d'identification, des données de localisation, un identifiant en ligne, ou encore moyennant un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Qu'elle soit confidentielle ou publique, de nature privée ou professionnelle, toute information qui se rapporte à une personne physique identifiée ou identifiable est considérée comme une donnée à caractère personnel au sens du RGPD (« données »).

Les données peuvent ainsi être **directement** « identifiantes » ou être **indirectement** « identifiantes ».

Le RGPD ne prévoit pas de limitation quant au support sur lequel peuvent figurer les données. Ainsi, les données peuvent être contenues sur un(e) :

NOTE SUR UN POST-IT | **DOCUMENT PAPIER** | **FICHIER INFORMATIQUE** | **PHOTO** | **VIDÉO** | **ENREGISTREMENT AUDIO**

LES DONNÉES DIRECTEMENT « IDENTIFIANTES »

Les données sont directement « identifiantes » lorsqu'elles révèlent clairement l'identité de la personne concernée. Il peut notamment s'agir d'un nom, d'un prénom, d'une adresse email nominative, ou d'une photo personnelle.

Ce type de données figure, par exemple, sur :

- *les fiches de paie ;*
- *les relevés de compte bancaire ;*
- *les certificats de maladie.*

LES DONNÉES INDIRECTEMENT « IDENTIFIANTES »

Les informations qui se rapportent indirectement à une personne physique, telles qu'**un numéro de téléphone**, **un identifiant**, **le numéro client** ou **le numéro d'une carte de crédit**, ne permettent pas, si elles sont prises de manière isolée, de savoir à qui elles correspondent.

Pourtant, elles constituent des données, car elles se rapportent à une personne identifiable à l'aide d'informations supplémentaires, que celles-ci soient détenues par l'administration elle-même ou par un tiers.

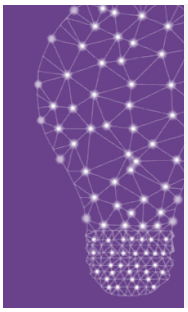
En revanche, les coordonnées d'une administration (adresse postale, numéro de téléphone du standard, courriel de contact générique, etc.) ne sont en principe pas des données à caractère personnel au sens du RGPD.

LES COMBINAISONS D'INFORMATIONS

Certaines informations, prises isolément, ne contiennent pas – directement ou indirectement – d'indications sur l'identité d'un individu. Toutefois, elles peuvent constituer des données si leur **combinaison avec d'autres informations** permet d'identifier la personne concernée de manière univoque.

Ainsi, une enquête ne sera pas rendue anonyme seulement parce que la personne interrogée n'a pas dévoilé son nom et prénom ou une autre information sur son identité.

En effet, selon le niveau de détail des informations collectées, **la combinaison de ces informations peut se révéler « identifiante »** pour les personnes concernées. Ceci est, en particulier le cas si les informations collectées concernent peu de personnes.



Un sondage par questionnaire auprès de certains agents d'une administration pourrait, même en l'absence d'indication des noms et prénoms, contenir des informations qui, combinées les unes aux autres, permettent de révéler l'identité de la personne concernée.

***Par exemple :** 45 ans, homme, juriste, date d'entrée en service en janvier 2019.*

Par ailleurs, l'essor du numérique apporte des possibilités croissantes d'identification ou de ré-identification des personnes concernées sur la base d'informations dépersonnalisées.

De nombreux travaux de recherche portant sur cette question démontrent en effet que la ré-identification devient de plus en plus facile, du fait de la multiplicité des données disponibles, de leur degré de précision et des techniques informatiques de recoupement de données, y compris à l'aide de solutions d'intelligence artificielle.

A quoi correspond la notion de « traitement » de données ?

Le RGPD définit le « traitement » de données comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel ».

Sont ainsi notamment concernées les opérations suivantes :

LA COLLECTE

L'ENREGISTREMENT

LA LECTURE (VISUALISATION)

LA STRUCTURATION

LA TRANSMISSION

LA CONSERVATION (HÉBERGEMENT)

LA MODIFICATION

L'EFFACEMENT

Constituent également des traitements de données :

- l'extraction de données ;
- la communication de données ;
- la mise à disposition de données ;
- le rapprochement de données ;
- l'archivage de données ;
- la destruction de données ;
- etc.

Exemples de traitements :

- *la tenue du registre national des personnes physiques ;*
- *la publication de l'annuaire d'une administration ;*
- *la tenue du cadastre ;*
- *la tenue du registre d'état civil ;*
- *la gestion des inscriptions en crèche ;*
- *la gestion des listes électorales ;*
- *la gestion des ordures ménagères ;*
- *la gestion des adhérents de la médiathèque.*

CHAPITRE 2//
LES GRANDS PRINCIPES DE LA PROTECTION DES DONNÉES

SECTION 1 :
LA LIMITATION DES FINALITÉS DU TRAITEMENT

A quoi correspond la notion de « finalité » ?

La finalité est l'objectif en vue duquel le traitement des données est opéré.

La limitation de la finalité constitue le principe-clé de la protection des données qui rayonne sur l'ensemble des autres principes prévus par le RGPD.

C'est à partir de la finalité que découlent notamment la pertinence des données collectées et la liste des personnes habilitées à y accéder ainsi que la durée de conservation des données. Le principe de la limitation de la finalité est, en outre, étroitement lié à la transparence, à la prévisibilité et au contrôle que la personne concernée exerce sur ses données.

Par ailleurs, si la finalité du traitement est suffisamment précise et claire, les personnes concernées savent à quoi s'attendre lors du traitement de leurs données et sont en mesure d'exercer leurs droits en matière de protection des données.

LA FINALITÉ DOIT ÊTRE « DÉTERMINÉE, EXPLICITE ET LÉGITIME »

Tout traitement de données doit répondre à une finalité « **déterminée, explicite et légitime** ».

La finalité du traitement de données doit être déterminée avant la mise en œuvre du traitement.

Pour le secteur public, les finalités sont en principe définies dans une base juridique ou doivent être rattachées aux missions légales de l'administration.

Le caractère déterminé et explicite de la finalité est vérifié lorsque la finalité est énoncée de manière compréhensible et suffisamment claire et précise.

Par contre, le traitement de données pour des finalités indéfinies, voire imprécises est illicite. Ainsi, la collecte et le traitement de données dans l'esprit que ces dernières pourraient tôt ou tard être utiles sont proscrits. En effet, une vision floue à ce niveau risque de se traduire par des consultations injustifiées des données des personnes concernées et par des utilisations de ces données allant au-delà de ce que justifient les missions de l'administration et les intentions du législateur.

En plus, la finalité doit être légitime par rapport aux activités de l'administration et ne pas être trop intrusive dans la sphère privée des personnes concernées.

LE TRAITEMENT DE DONNÉES POUR UNE FINALITÉ AUTRE QUE CELLE INITIALEMENT DÉTERMINÉE

Au-delà de sa (ou de ses) finalité(s) primaire(s), le traitement de données peut donner lieu à des usages secondaires (traitement ultérieur).

La finalité compatible

Un traitement ultérieur des données pour une finalité différente de celle initialement fixée peut être envisagé, sous réserve de sa compatibilité avec la finalité initiale du traitement.

La vérification de la compatibilité présuppose que la finalité initiale ait clairement été identifiée, faute de quoi l'évaluation de la compatibilité des finalités ultérieures ne pourrait être réalisée. De ce fait, il serait impossible de s'assurer que le lien entre les finalités ultérieures et la finalité initiale est suffisamment pertinent et prévisible pour permettre d'apprécier si le traitement subséquent est loyal envers la personne concernée ou non.

Pour évaluer si la finalité secondaire est compatible avec la finalité initiale, l'administration en charge du traitement doit considérer les facteurs suivants :

- l'existence d'un lien entre la finalité initiale et la finalité secondaire ;
- le contexte dans lequel les données ont été collectées (relation entre personnes concernées et responsable du traitement) ;
- la nature des données ;
- les conséquences possibles pour les personnes concernées ;
- l'existence de garanties appropriées (ex.: chiffrement).

Par ailleurs, le RGPD prévoit 3 cas de figure dans lesquels les finalités sont présumées compatibles avec la finalité initiale, à savoir :

- *le traitement de données à des fins archivistiques dans l'intérêt public ;*
- *le traitement de données à des fins de recherche scientifique ou historique ;*
- *le traitement de données à des fins statistiques.*

L'interdiction de traiter les données pour une finalité incompatible

Le traitement de données pour une finalité dite « incompatible » avec la finalité initiale est interdit, à moins que ledit traitement soit expressément prévu par le droit luxembourgeois ou européen ou que la personne concernée ait donné son consentement.

En effet, le non-respect de la limitation des finalités est considéré comme un détournement illicite de la finalité, tout comme la consultation à des fins privées par l'agent des données contenues dans un fichier (ex.: le registre national des personnes physiques, ainsi que le registre communal) tenu par l'administration.

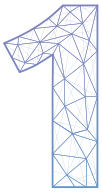
SECTION 2 :
LA LICÉITÉ DU TRAITEMENT

Les bases de licéité du traitement de données.

Pour qu'une administration puisse collecter et traiter des données, elle doit impérativement identifier la base de licéité du traitement.

Tout traitement de données doit reposer sur une des 6 bases de licéité prévues par l'article 6, paragraphe 1er du RGPD.

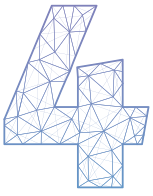
Le traitement de données n'est donc licite que si une des conditions suivantes est remplie :



La personne concernée **a consenti** au traitement de ses données pour une ou plusieurs finalités spécifiques.

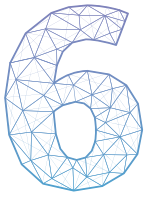
Le traitement est nécessaire à l'**exécution d'un contrat** auquel la personne concernée est partie ou à l'**exécution de mesures précontractuelles** prises à la demande de celle-ci.

Le traitement est nécessaire au respect d'une **obligation légale** à laquelle le responsable du traitement est soumis.



Le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique.

Le traitement est nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de **l'exercice de l'autorité publique** dont est investi le responsable du traitement.



Le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données, notamment lorsque la personne concernée est un enfant.

En ce qui concerne le secteur public, les traitements sont généralement effectués en vue de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ou encore pour le respect d'une obligation légale lorsque le traitement est explicitement prévu par un texte de loi.

En revanche, les autres bases de licéité de l'article 6, paragraphe 1er du RGPD ne sont que rarement applicables aux traitements effectués par les administrations.

PRÉCISIONS QUANT À CHAQUE BASE DE LICÉITÉ DE L'ARTICLE 6 DU RGPD

LE CONSENTEMENT DE LA PERSONNE CONCERNÉE

Le RGPD prévoit que les données peuvent être traitées, si la personne concernée **a consenti** audit traitement pour une ou plusieurs finalités spécifiques.

Le consentement de la personne concernée est défini par le RGPD comme « 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 ».

Pour être valide, le consentement de la personne concernée doit dès lors présenter différentes caractéristiques.

Le consentement doit être « libre »

La personne concernée doit disposer d'un véritable choix et être en mesure de refuser ou de retirer son consentement sans subir de préjudice.

Par ailleurs, le RGPD prévoit une **présomption de déséquilibre manifeste** dans les relations entre les pouvoirs publics et les personnes concernées.

De ce fait, le traitement de données par les administrations sur base du consentement de la personne concernée ne constitue qu'un cas marginal.

Le consentement doit être « spécifique »

Un consentement doit correspondre à une finalité spécifique et déterminée à l'avance.

Lorsqu'un traitement comporte plusieurs finalités, la personne doit pouvoir consentir à chacune d'entre elles.

Le consentement doit être « éclairé »

Pour que le consentement soit éclairé, la personne concernée doit être informée de l'identité du responsable du traitement et des finalités du traitement auxquelles sont destinées ses données. Par ailleurs, il convient de préciser, dans le formulaire de consentement, que la personne a le droit de retirer son consentement à tout moment.

Les informations fournies doivent permettre à la personne concernée de comprendre ce qu'il va advenir de ses données. Pour ce faire, les informations ne devront pas être « noyées » dans des notices générales.

Le consentement doit être « univoque »

Le consentement doit être donné sans ambiguïté par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement de données la concernant.

Cet acte positif clair peut prendre la forme d'une déclaration écrite, y compris par voie électronique. Cela pourrait se faire également en cochant une case lors de la consultation d'un site internet ou en optant pour certains paramètres techniques pour des services en ligne.

Il est aussi possible de formuler le consentement de manière orale, sous réserve que l'administration puisse démontrer que la personne concernée ait consenti au traitement de données.

Par contre, le consentement n'est pas considéré comme univoque si :

- les cases sont pré-cochées ou pré-activées ;
- le consentement résulte de l'acceptation globale d'un contrat ou de conditions d'utilisation d'un service ;
- le consentement résulte d'une inaction ou d'un silence de la personne concernée ou de la simple utilisation d'un service par cette dernière (le consentement tacite n'étant pas reconnu comme valide).

Le cas particulier du consentement des mineurs

Le RGPD prévoit des conditions particulières concernant le consentement des enfants dans l'hypothèse de l'offre directe de services de la société de l'information (réseaux sociaux, plateformes de vidéos à la demande, newsletters, etc.) à l'adresse de ces derniers.

En effet, lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

LA NÉCESSITÉ CONTRACTUELLE

Les données de la personne concernée peuvent être traitées par le responsable du traitement, si le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Le traitement de données par les administrations étatiques sur base d'une nécessité contractuelle ne constitue qu'un cas marginal.

Par exemple dans le cadre de la souscription d'une place de parking par un agent, une convention préalable doit être établie. L'administration pourrait donc traiter, dans le cadre de mesures précontractuelles, un certain nombre de données telles que les coordonnées de la personne concernée.

De même, dans le cadre de la fréquentation d'une cantine, cette dernière pourrait traiter des données relatives aux coordonnées de la personne concernée pour pouvoir lui donner une carte d'accès et pour pouvoir exécuter ce contrat.

LE RESPECT D'UNE OBLIGATION LÉGALE

Pour que le traitement de données puisse être considéré comme étant nécessaire pour le respect d'une obligation légale, il doit être indispensable pour le respect des obligations prévues par la loi. En d'autres termes, il faut que la loi prescrive expressément le traitement de données ainsi que les finalités du traitement.

LA SAUVEGARDE DES INTÉRÊTS VITAUX

Les données de la personne concernée peuvent être traitées si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne. Ce fondement doit être interprété strictement : il peut être utilisé uniquement lorsqu'il est impossible de recourir à un autre fondement de licéité.

Il est ainsi retenu en cas de menace pour la vie de la personne, lorsqu'elle est par exemple en incapacité physique d'exprimer son consentement quant à l'utilisation de ses données.

L'EXÉCUTION D'UNE MISSION D'INTÉRÊT PUBLIC

Les administrations peuvent traiter des données lorsque le traitement est « nécessaire » à l'exécution d'une mission d'intérêt public ou si le traitement relève de l'autorité publique dont est investie l'administration.

Cependant, ce fondement ne constitue pas une « carte blanche » pour le traitement de données par les acteurs du secteur public. En effet, il ne pourra être invoqué que lorsque la finalité poursuivie correspond à une mission dévolue à l'administration en vertu de la législation applicable et que le traitement de données est « nécessaire » pour atteindre la finalité en question.

LES INTÉRÊTS LÉGITIMES DU RESPONSABLE DU TRAITEMENT OU D'UN TIERS

Si les acteurs du secteur privé ont la possibilité de fonder leur traitement de données aux fins des intérêts légitimes qu'ils ou qu'un tiers poursuivent, le RGPD a clarifié que **cette faculté n'est pas ouverte aux autorités publiques agissant dans l'exécution de leurs missions.**

Cela étant dit, certains traitements de données sans rapport direct avec les spécificités des missions d'intérêt public confiées à l'administration peuvent être fondés sur les intérêts légitimes poursuivis par celle-ci, sous réserve qu'elle n'agit pas dans l'exercice de ses missions.

Par exemple :

La vidéosurveillance des alentours des infrastructures de l'administration, la tenue d'une liste des visiteurs des locaux de l'administration ou l'organisation d'événements « team-building ».

Pour que ces traitements soient licites, il faut cependant qu'ils soient **nécessaires** aux fins des intérêts légitimes poursuivis par l'administration et que **les intérêts ou libertés et droits fondamentaux de la personne concernée ne prévalent pas sur les intérêts de l'administration**. La balance des interêts doit être documentée par l'administration qui traite les données sur base de ce fondement de licéité.

LE TRAITEMENT DE DONNÉES DITES « SENSIBLES »

Le RGPD prévoit des conditions spécifiques pour le traitement de données portant sur des catégories particulières de données au sens de l'article 9, paragraphe 1er du RGPD (**« données sensibles »**).

Constituent des données sensibles au regard du RGPD :

- LES ORIGINES RACIALES OU ETHNIQUES
- LES OPINIONS POLITIQUES
- LES CONVICTIONS RELIGIEUSES OU PHILOSOPHIQUES
- L'APPARTENANCE SYNDICALE
- LA SANTÉ (PHYSIQUE OU MENTALE)
- LA VIE SEXUELLE OU L'ORIENTATION SEXUELLE
- LES DONNÉES GÉNÉTIQUES
- LES DONNÉES BIOMÉTRIQUES

Le RGPD édicte une interdiction de principe de traiter les « données sensibles ». Leur traitement n'est autorisé que dans les cas spécifiques prévus par l'article 9, paragraphe 2 du RGPD, à savoir :

Consentement explicite de la personne concernée.

Le traitement est nécessaire aux fins de **l'exécution des obligations et de l'exercice des droits** propres au responsable du traitement ou à la personne concernée **en matière de droit du travail, de la sécurité sociale et de la protection sociale** (condition : le traitement est autorisé par la loi ou par une convention collective).

Sauvegarde des interêts vitaux.

Traitement des données rendues publiques par la personne concernée.

Action en justice.

Traitement par un organisme à but non lucratif poursuivant une finalité **politique, philosophique, religieuse ou syndicale** visant exclusivement aux membres dudit organisme.

Motifs d'interêt public important sur base du droit européen ou national qui prévoit des garanties appropriées.

Médecine préventive/du travail, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des sytèmes de services de soins de santé ou de protection sociale sur la base du droit européen ou national/sur base d'un contrat avec un professionnel de santé.

Motifs d'interêt public dans le domaine de la santé publique.

Fins archivistiques, recherche scientifique, historique ou statistiques.

SECTION 3 :
LA MINIMISATION DES DONNÉES ET DES ACCÈS

Les données traitées par l'administration doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Les données faisant l'objet d'un traitement doivent être « nécessaires » pour atteindre les objectifs de ce traitement et le responsable du traitement doit limiter au strict minimum l'utilisation des données.

Pour vérifier le respect du principe de minimisation des données, il convient en particulier de se poser les questions suivantes :

- quelle est la finalité du traitement (l'objectif poursuivi par l'administration) ?
- est-ce que toutes les données sont indispensables pour atteindre cet objectif ?

BONNES PRATIQUES

1

FAIRE LE TRI
en se questionnant sur la nature des données collectées, leur quantité et leur précision.

Exemple : *Une administration publie un formulaire de contact sur son site internet pour permettre à tout intéressé de signaler sa volonté d'être contacté par cette administration.*

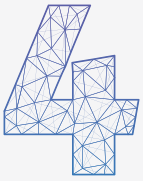
Dans ce cas de figure, le formulaire doit recueillir uniquement les informations nécessaires à la prise de contact.

2

S'INTERROGER
sur l'existence d'une solution alternative moins intrusive face à un projet de traitement de données.

Exemple : *Une administration souhaite renforcer la protection de ses locaux. A cette fin, elle envisage de mettre en place un dispositif biométrique. Il y a lieu de se demander si un dispositif moins intrusif, tel que le recours à un système d'accès avec des badges, ne pourrait suffire.*

PSEUDONYMISER
les données toutes les fois ou leur conservation sous une forme directement identifiante n'est pas nécessaire.

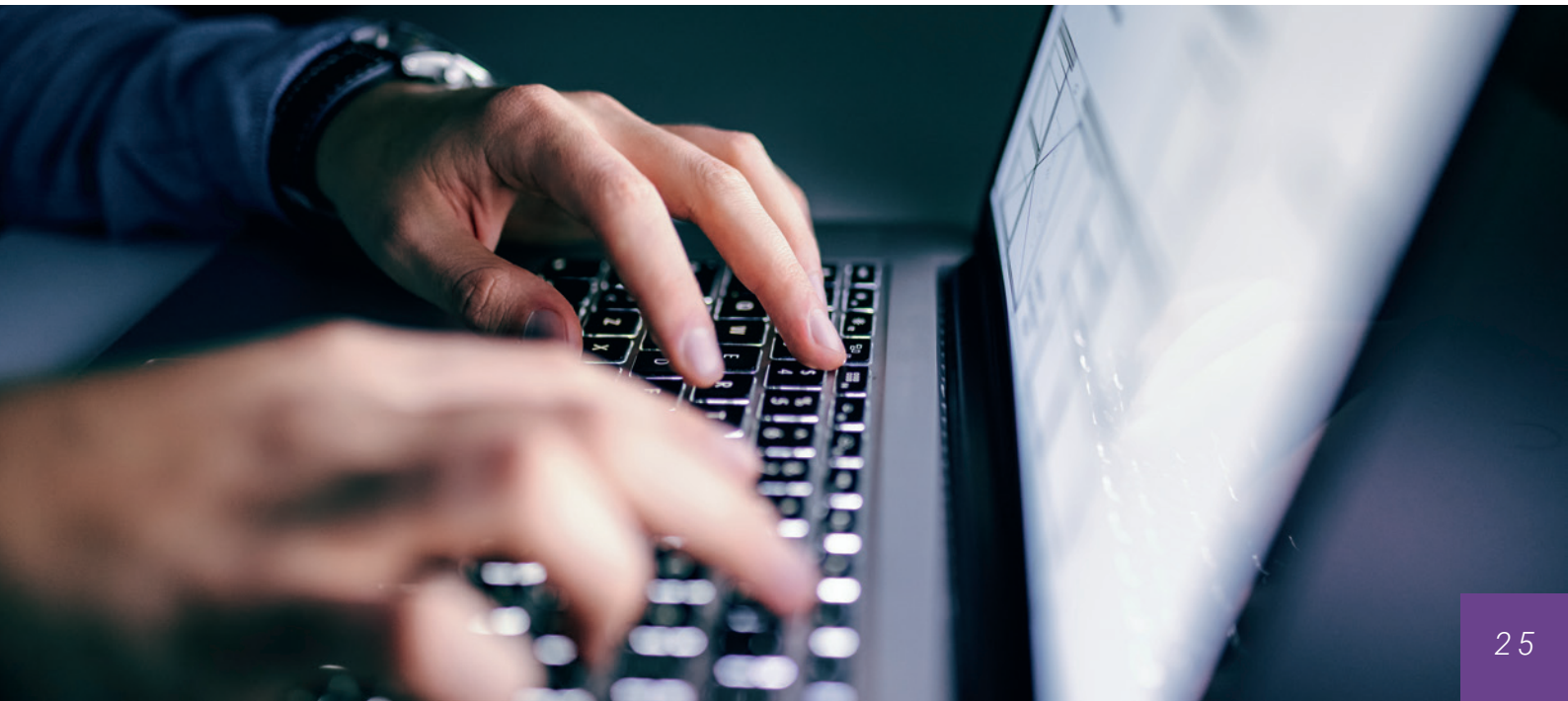


BANNIR
toute collecte de données à titre préventif.

Seules les personnes ayant un besoin impératif pour l'accomplissement de leurs missions doivent pouvoir accéder aux données (principe du besoin d'en connaître).

En effet, l'agent doit garantir la confidentialité des données et il doit seulement les traiter dans les limites des missions d'intérêts public poursuivies par l'administration et pour les seuls objectifs fixés par celle-ci.

Le traitement des données en dehors d'une nécessité et d'une justification professionnelle est prohibé et toute transmission ou divulgation de données à autrui est proscrite si le destinataire (même s'il se trouve également sous l'autorité directe du même responsable du traitement) ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter. Les documents papier doivent être conservés de manière sécurisée (politique du bureau rangé) et l'agent ne doit pas communiquer ses clés d'accès à des personnes non autorisées.



SECTION 4 :
L'EXACTITUDE DES DONNÉES

L'administration qui traite les données est tenue d'assurer l'exactitude des données. Les données doivent être exactes et, si nécessaire, tenues à jour.

SECTION 5 :

LA LIMITATION DE LA CONSERVATION DES DONNÉES

L'administration ne doit pas conserver les données sous une forme permettant l'identification (directe ou indirecte) des personnes concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Pour ce faire, l'administration en charge du traitement devrait **fixer des délais de conservation des données**, et procéder à un examen périodique de ces délais.

A moins que la loi ne prescrive une durée de conservation précise, l'administration en charge du traitement doit déterminer pour quelle période les données seront conservées en :

- fixant une durée précise de conservation (ex.: 8 jours après la prise d'image) ou ;
- précisant des critères objectifs qui permettent d'identifier la durée de conservation des données (ex.: 6 mois après la fin de la relation contractuelle).

Pour chacun des traitements mis en œuvre, l'administration en charge du traitement doit se poser, en particulier, les questions suivantes :

- *Jusqu'à quand est-ce que l'administration doit disposer des données pour atteindre l'objectif fixé ?*
- *Existe-t-il une obligation légale de conserver les données ? Si oui, quelle est l'étendue exacte de cette obligation ?*
- *Une fois que l'objectif poursuivi est atteint, est-ce que l'administration doit encore disposer des données dans le cadre d'un éventuel contentieux ?*
- *Existe-t-il des recommandations officielles ? (autorité nationale, …).*

Une fois que les finalités d'un traitement sont atteintes, les données faisant l'objet du traitement doivent être effacées ou anonymisées, à moins qu'elles ne doivent être traitées ultérieurement exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherches scientifiques ou historiques ou à des fins statistiques et ceci conformément aux dispositions légales applicables. Notons que l'archivage des données au-delà du terme de leur utilité administrative est encadré par la loi du 17 août 2018 relative à l'archivage.

SECTION 6 :
LA SÉCURITÉ DES DONNÉES

Les données doivent être traitées de manière à garantir leur sécurité à l'aide de mesures appropriées.

Les mesures appropriées visent à se prémunir contre :

- le traitement illicite de données ;
- la divulgation non autorisée ou illicite de données ;
- la perte (temporaire ou définitive) de données ;
- la destruction illicite de données ;
- les défaillances (techniques ou organisationnelles) des systèmes d'information.

L'administration en charge du traitement de données doit implémenter les mesures de sécurité en tenant compte :

- de l'état des connaissances techniques et organisationnelles ;
- de la nature, de la portée, du contexte et des finalités du traitement ; et
- des risques pour les droits et libertés des personnes physiques.

En fonction du niveau des risques pour les droits et libertés des personnes physiques, le facteur du coût d'implémentation de ces mesures pourra être considéré. Plus le niveau de risque est élevé, moins l'argument du coût élevé pourra être retenu.

Par exemple :

Une base de données d'un professionnel de santé qui contient des données médicales ou un fichier des autorités judiciaires contenant des données sur les condamnations pénales des individus nécessite davantage de mesures de sécurité qu'un fichier avec les coordonnées des agents ayant accès à la cantine.

Les mesures de sécurité peuvent être de nature technique et organisationnelle.

Elles peuvent, selon les besoins, comprendre :

- *la pseudonymisation et le chiffrement des données ;*
- *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
- *des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;*
- *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.*

LES 3 PRINCIPES DE LA SÉCURITÉ DES DONNÉES

Pour être pleinement prise en compte, l'obligation de sécurité doit être appréhendée de manière globale, sous l'angle des 3 principes suivants :

- le principe de confidentialité : les données ne doivent être accessibles qu'aux personnes autorisées ;
- le principe d'intégrité : les données ne doivent pas être altérées ou modifiées de manière illicite ;
- le principe de disponibilité : les données doivent être en permanence accessibles pour les personnes autorisées.

En préservant l'intégrité, la confidentialité et la disponibilité des données traitées, ces mesures de sécurité protègent à la fois les personnes concernées, ainsi que les interêts et la réputation de l'administration.

SECTION 7 :
LA TRANSPARENCE À L'ÉGARD DE LA PERSONNE CONCERNÉE

Obligation d'informer les personnes concernées sur le traitement de leurs données.

Les administrations sont tenues, sauf exceptions légales, d'informer les personnes concernées sur les traitements de leurs données.

L'obligation d'information n'est pas subordonnée à une demande ou une action positive de la personne concernée. L'administration en charge du traitement de données doit, au contraire, adopter une **approche proactive** et ceci indépendamment de la question de savoir si la personne concernée a manifesté un intérêt pour ces informations ou non.

L'obligation d'informer les individus découle directement des **principes de loyauté et de transparence** qui exigent que les données ne soient pas collectées, utilisées, consultées ou traitées à l'insu de la personne concernée.

Dès lors, l'administration qui met en œuvre un traitement de données doit fournir aux personnes concernées les informations sur le traitement de leurs données de **manière concise, transparente et compréhensible**. De même, elle doit leur expliquer comment exercer leurs droits individuels.

Les informations – qui doivent être communiquées en des termes **clairs et simples** *– doivent contenir, en particulier :*

- *l'identité du responsable du traitement ;*
- *les finalités et la base de licéité du traitement ;*
- *les coordonnées du délégué à la protection des données ;*
- *les destinataires des données ;*
- *la durée de conservation des données ;*
- *Les droits individuels de la personne concernée.*

L'obligation d'informer est une condition *sine qua non* du respect du principe de transparence et de loyauté. Dans cet ordre d'idées, il est interdit à une administration de transmettre des données à une autre administration en vue d'un traitement ultérieur sans que les individus concernés ne soient informés de la transmission de leurs données.

Le devoir d'information des personnes concernées est d'autant plus important qu'il est une condition nécessaire à l'exercice par ces personnes de leurs droits d'accès et de rectification des données traitées et de leur droit d'opposition au traitement desdites données.

Il s'ensuit que l'exigence de traitement loyal des données oblige une administration à informer les personnes concernées de la transmission de leurs données à une autre administration (destinataire) en vue d'être traitées par cette dernière.

Par ailleurs, les administrations « destinataires » doivent à leur tour informer les personnes concernées quant aux traitements de données qu'elles effectuent.

Exceptions à l'obligation d'information et limitations au droit d'être informé.

Le droit à l'information **n'est pas absolu.**

L'obligation d'informer les personnes concernées ne s'applique pas lorsque le responsable du traitement peut démontrer que la personne concernée dispose déjà de toutes les informations pertinentes.

Dans l'hypothèse où les données ne sont pas collectées directement auprès de la personne concernée (notamment dans les cas où une administration reçoit les données d'une autre administration), l'obligation d'informer ne s'applique, en outre, pas dans les trois cas de figure suivants :

- la fourniture des informations se révèle matériellement impossible ou exigerait des efforts disproportionnés. Pour que cette exception puisse être invoquée, l'administration en charge du traitement doit toutefois (i) prouver le caractère disproportionné ou impossible et (ii) prendre des mesures appropriées pour protéger les droits et libertés des personnes concernées, y compris en rendant les informations publiquement disponibles (notamment moyennant une brochure/un dépliant, ou sur son site internet) ;
- l'obtention ou la communication des données sont expressément prévues par la loi ;
- les données doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par la loi.

CHAPITRE 3//
L'EXERCICE DES DROITS DE LA PERSONNE CONCERNÉE

Les droits de la personne concernée.

Les administrations en charge du traitement de données doivent faciliter l'exercice des droits individuels conférés à la personne concernée par le RGPD.

Ces droits – contrairement au droit à l'information – s'exercent uniquement **sur demande expresse** de la personne concernée.

La personne concernée peut, dans les limites de la loi, demander à l'administration qui traite ses données :

1. **l'accès à ses données** ainsi que la fourniture d'informations sur le traitement de données opéré par l'administration, notamment les finalités pour lesquelles les données sont traitées. Par ailleurs, la personne concernée peut demander de recevoir une copie des données traitées (le droit de recevoir une copie ne doit toutefois pas porter atteinte aux droits et libertés d'autrui) ;

2. **la rectification des données** inexactes la concernant ;

3. **l'effacement de ses données**, lorsqu'elle ne souhaite plus que ses données soient traitées (« droit à l'oubli »). Dès lors, l'administration devra supprimer ces données, à moins qu'un motif légitime ne justifie leur conservation (ex. : une obligation légale) ;

4. **la limitation du traitement** de ses données lorsque l'un des éléments suivants s'applique :

   - l'exactitude des données est contestée par la personne concernée. Dans ce cas de figure, l'administration ne peut plus traiter les données jusqu'à vérification de leur exactitude ;
   - le traitement est illicite et la personne concernée s'oppose à l'effacement des données et exige à la place la limitation de leur utilisation ;
   - l'administration n'a plus besoin des données aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la contestation, l'exercice ou la défense des droits en justice ;
   - la personne concernée s'est opposée au traitement des données. L'administration ne peut plus traiter les données, jusqu'à vérification du bien fondé de la demande de la personne concernée.

   Lorsque le traitement a été limité, les données de la personne concernée ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de cette dernière, ou pour :

   - la constatation, l'exercice ou la défense de droits en justice ;
   - la protection des droits d'une autre personne physique ou morale ; ou
   - des motifs importants d'intérêt public de l'Union ou d'un État membre.

5

de récupérer les données qu'elle a communiquées à une administration et de les voir transmettre à un autre organisme dans un format structuré, couramment utilisé et lisible par machine (« droit à la portabilité des données »). Notons que ce droit ne s'applique que dans l'hypothèse où le traitement repose sur le consentement de la personne concernée ou sur la nécessité contractuelle. Ainsi, il n'est guère d'application pour les traitements de données réalisés par les acteurs du secteur public ;

6

de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement de ses données nécessaire à la poursuite des intérêts légitimes du responsable du traitement ou à l'exécution d'une mission d'intérêt public. Dans ce cas de figure, l'administration en charge du traitement doit arrêter le traitement, sauf si elle peut démontrer l'existence de motifs légitimes et impérieux pour continuer le traitement.

A noter que la personne concernée a également le droit de s'opposer au traitement de données la concernant, sans qu'elle doive fournir de justification, si les données sont utilisées à des fins de prospection (ex.: newsletter de l'administration).

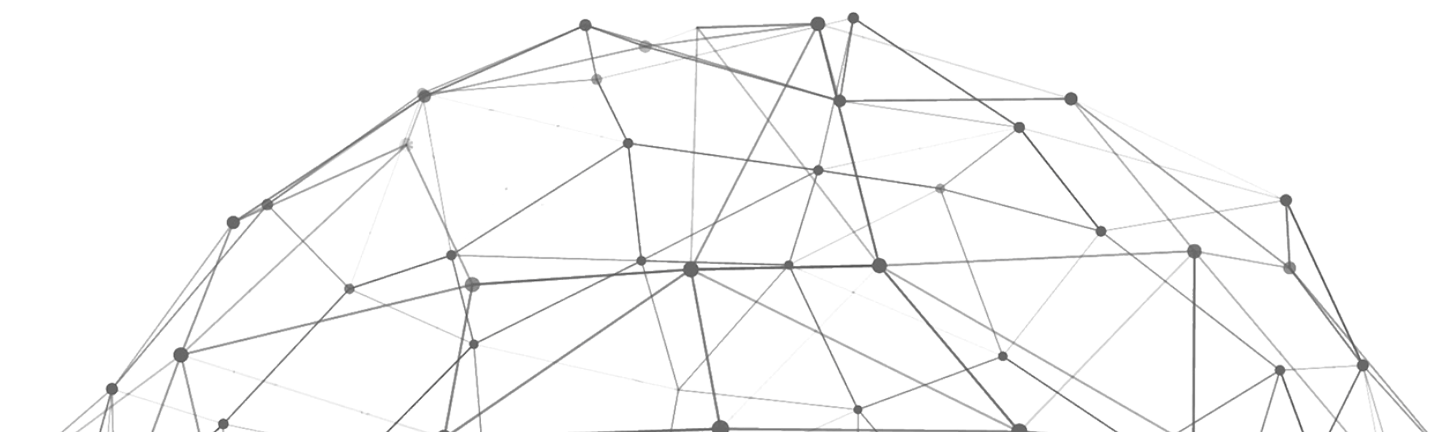
Par ailleurs, la personne concernée a **le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage**, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Le principe d'interdiction du profilage ne s'applique pas lorsque la décision :

- est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ;
- est autorisée par le droit de l'Union ou le droit national qui prévoit des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ;
- est fondée sur le consentement explicite de la personne concernée.

Toutefois, lorsque l'administration en charge du traitement prend des décisions qui impactent directement la personne concernée sur base de processus automatisés (y compris le profilage), elle doit permettre à cette dernière de faire valoir son point de vue et, le cas échéant, de contester la décision. En outre, l'administration doit informer les personnes concernées des critères ayant mené à la décision en question.

Notons, à toutes fins utiles, que la personne concernée a le droit d'introduire à tout moment une réclamation auprès de la Commission nationale pour la protection des données (CNPD).



REMARQUE CONCERNANT LA GESTION DE L'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

Les administrations disposent d'un **délai d'un mois** à compter de la date de réception d'une demande pour y apporter une réponse. Au besoin, ce délai peut être prolongé de 2 mois, compte tenu dela complexité et du nombre de demandes.

La décision de l'administration de ne pas donner suite à une demande de la personne concernée dans les délais impartis doit être **motivée**.

Pour éviter des retards ou dépassements de délais, les agents publics doivent remonter dans les meilleurs délais lesdites demandes au niveau approprié retenu par le responsable du traitement, y compris le délégué à la protection des données.

CHAPITRE 4//
LES RÔLES ET RESPONSABILITÉS DES PRINCIPAUX ACTEURS

SECTION 1 :
LE RESPONSABLE DU TRAITEMENT ET L'« ACCOUNTABILITY »

LE RESPONSABLE DU TRAITEMENT

Le responsable du traitement est la personne ou l'entité (une personne physique ou morale, une autorité publique, un service ou un autre organisme) qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens du traitement de données**.

Les termes de « responsable du traitement » et de « sous-traitant » ont pour objet de définir les responsabilités en fonction des rôles réels des parties au traitement de données.

La charge d'assurer le respect des principes de la protection des données incombe au responsable du traitement.

En principe, il n'y a pas de limitation quant au type de personne ou d'entité qui peut assumer le rôle de responsable du traitement. Toutefois, en pratique, c'est généralement l'entité en tant que telle, et non un individu au sein de l'entité (tel que le chef d'administration ou un agent), qui agit en qualité de responsable du traitement.

La loi peut désigner le responsable du traitement. Dans le cas contraire il convient d'analyser les éléments factuels et les circonstances dans lesquelles l'opération de traitement est réalisée.

Pour ce faire, il convient de tenir compte des deux facteurs suivants :

- *qui détermine les finalités du traitement, c'est-à-dire le « pourquoi » du traitement (qui décide quelles données sont collectées et qui définit les objectifs pour lesquels ces données sont traitées ?) ;*
- *les moyens essentiels du traitement, c'est-à-dire le « comment » du traitement (qui décide par quels instruments les données sont collectées et comment ces dernières sont traitées ?).*

LE PRINCIPE D'« ACCOUNTABILITY »

Le RGPD introduit le principe d'« accountability » du responsable du traitement.

Ce dernier ne doit pas seulement assurer le respect du RGPD, il doit également être en mesure de démontrer que celui-ci est respecté.

Pour ce faire, il doit mettre en place des mesures techniques et organisationnelles appropriées pour la sauvegarde des droits et libertés des personnes concernées et être en mesure de prouver que ces mesures ont été prises et qu'elles sont effectives.

Il doit, par ailleurs, appliquer des mesures de protection des données dès la conception et par défaut.

L'administration en charge du traitement doit mettre en oeuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement en lui-même, des mesures techniques et organisationnelles appropriées (ex. : la pseudonymisation des données) qui sont destinées à mettre en oeuvre les principes de la protection des données (ex. : la minimisation des données) de façon effective. Elle doit également assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD et de protéger les droits de la personne concernée.

En outre, l'administration doit garantir que, par défaut, seules les données qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Parmi les instruments permettant au responsable du traitement de démontrer le respect du RGPD, il y a lieu de citer, notamment :

- la désignation d'un délégué à la protection des données ;
- la tenue d'un registre des activités de traitement ;
- la réalisation d'analyses d'impact relatives à la protection des données ;
- la fourniture d'informations sur les traitements opérés aux personnes concernées ;
- la sensibilisation des agents quant à leurs obligations en matière de protection des données ;
- la répartition claire des rôles et responsabilités des agents dans le respect du besoin d'en connaître (« need to know »).

La documentation de la conformité comprend également (mais sans limitation) l'encadrement des relations de responsabilité conjointe et de sous-traitance, la mise en œuvre d'outils de gestion des violations de données ainsi que l'adoption de lignes de conduite et de procédures internes.

Il s'agit ainsi pour le responsable du traitement de constituer un « ensemble de preuves » permettant de **démontrer sa conformité au RGPD**.

SECTION 2 :
LES RESPONSABLES CONJOINTS DU TRAITEMENT

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont considérés comme étant « responsables conjoints du traitement ».

Pour garantir la conformité au RGPD ainsi que la transparence à l'égard des personnes concernées, les responsables conjoints du traitement sont tenus de définir leurs obligations respectives de manière transparente.

Cet encadrement conventionnel (contrat) doit, en l'absence d'un acte juridique précis tel qu'une loi ou un règlement, préciser notamment :

- quelle entité est responsable pour la communication des informations sur le traitement de données à la personne concernée ; et
- quelle entité est en charge pour l'exercice des droits de la personne concernée.

Par ailleurs, l'encadrement conventionnel pourra définir un point de contact unique pour la personne concernée.

Les grandes lignes de l'accord doivent être mises à disposition de la personne concernée.

SECTION 3 :
LE SOUS-TRAITANT

Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données **pour le compte** du responsable du traitement ».

Sont a priori visés par cette définition tous les prestataires de services informatiques, les sociétés de sécurité informatique, les intégrateurs de logiciels, les entreprises de service du numérique, ou par exemple des entreprises de restauration de documents papier ayant accès et traitant des données non pas pour leur propre finalité, mais « pour le compte » du responsable du traitement. Tout traitement de données par le sous-traitant pour une finalité autre que celles fixées par le responsable du traitement est strictement interdit.

Lorsque le traitement est effectué par un sous-traitant pour le compte du responsable du traitement, un encadrement particulier de cette relation s'impose aux termes du RGPD. En effet, la collaboration entre les parties doit être régie par un accord conventionnel ou un autre acte juridique contraignant tel qu'une loi ou un règlement.

Cet accord doit contenir les éléments clés listés à l'article 28 du RGPD. Il doit notamment définir l'objet de la collaboration, énoncer les finalités, la nature et la durée du traitement de données. Il doit également stipuler que le sous-traitant n'agit que sur instruction documentée du responsable du traitement.

Par ailleurs, le sous-traitant doit assurer la sécurité des données qui lui ont été confiées et informer l'administration, responsable du traitement, de toute violation de données.

SECTION 4 :

LE COMMISSARIAT DU GOUVERNEMENT À LA PROTECTION DES DONNÉES AUPRÈS DE L'ETAT (CGPD)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

Le Commissariat du gouvernement à la protection des données auprès de l'Etat (« CGPD ») est une administration qui, de manière générale, a pour mission de contribuer au développement de la protection des données au sein des administrations étatiques.

Le CGPD peut être désigné comme délégué à la protection des données par les ministres ou leurs chefs d'administration, ainsi que par les communes.

Conformément à l'article 59 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, le CGPD contribue à une mise en œuvre cohérente des politiques dans le domaine de la protection des données au sein de l'Etat. A cette fin, il conseille, sur demande, les membres du Gouvernement et accompagne les chefs d'administration dans la mise en place de mesures appropriées pour protéger les droits et libertés des personnes concernées. En outre, il assiste les délégués à la protection des données que les administrations étatiques ont désignés en interne.

Dans le cadre de ses missions, concernant la promotion des bonnes pratiques en matière de protection des données au sein de l'administration étatique, le CGPD sensibilise les agents publics afin de leur permettre d'acquérir les bons réflexes en la matière. Pour ce faire, des séances d'initiation à la protection des données et des cours de formation spécialisés dédiés aux différents aspects du règlement général sur la protection des données sont régulièrement offerts aux agents de l'Etat et des communes.

En ce qui concerne le volet touchant à la guidance, le CGPD développe par ailleurs des documents et des outils adaptés visant à assister les entités en matière de conformité au RGPD.

SECTION 5 :

LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES (CNPD)

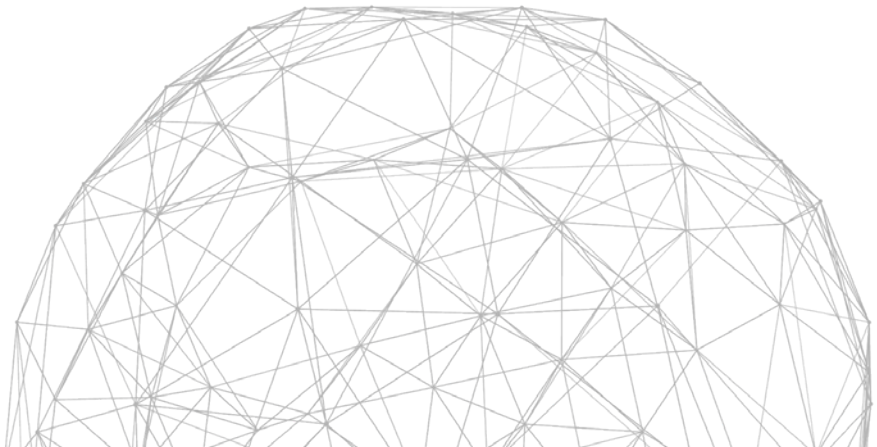
La Commission nationale pour la protection des données (« CNPD ») est l'autorité de contrôle de la protection des données au Luxembourg. Créée en 2002, il s'agit d'un établissement public disposant d'une autonomie financière et administrative et doté de la personnalité juridique.

Depuis la loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données, la CNPD se charge de deux grandes missions, à savoir : d'une part le volet « conseil » et d'autre part le volet « contrôle » :

- Le volet « conseil » regroupe les activités de guidance et de sensibilisation à travers l'organisation de formations et de conférences s'adressant au grand public, ainsi qu'aux experts en matière de protection des données. La CNPD est également sollicitée pour, répondre aux demandes des personnes concernées sur l'exercice de leurs droits, publier des guidances thématiques, rédiger des avis juridiques et aviser des projets de loi ou de mesures réglementaires du gouvernement ;
- Le volet « contrôle » comprend le traitement des réclamations introduites par une personne concernée ou par une organisation, le traitement des notifications de violations de données personnelles déclarées à la CNPD, ainsi que les enquêtes que la CNPD décide de mener auprès des responsables du traitement et de leurs sous-traitants.

Avec l'entrée en application du RGPD, la CNPD a également un pouvoir de sanction et peut donc prononcer des mesures correctrices, des suspensions de traitements de données personnelles et des amendes administratives.

Dans le cadre de réclamations transfrontalières, la CNPD coopère avec les autres autorités de contrôle européennes. Elle représente le Luxembourg au sein du Comité européen de la protection des données, (« European Data Protection Board » (EDPB)). Cet organe européen contribue à garantir que la législation en matière de protection des données est appliquée de façon systématique et cohérente au sein de l'Union Européenne. Il assure également une coopération efficace entre les autorités de contrôle.



CHAPITRE 5//
LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET LES OUTILS ESSENTIELS DE LA CONFORMITÉ AU RGPD

SECTION 1 :
LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Chaque autorité publique ou organisme public (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle) doit désigner un délégué à la protection des données (« DPD »).

La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données dispose que les ministres du ressort ou, sous leur autorité, les chefs d'administration compétents doivent désigner un ou plusieurs DPD. Il en va de même pour les communes.

Le DPD doit avoir les qualités professionnelles requises et exercer ses fonctions en toute indépendance. Le DPD ne peut pas exercer d'autres missions et tâches qui entraîneraient un conflit d'intérêts. De ce fait, il ne peut pas exercer au sein de l'entité une fonction qui l'amènerait à déterminer les moyens (le comment ?) et les finalités (le pourquoi ?) du traitement de données.

Exemples de fonctions qui sont incompatibles avec la fonction de DPD :

Toutes les fonctions dirigeantes telles que directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable de département (ressources humaines, service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement.

DÉSIGNATION DU DPD

La désignation d'un DPD est obligatoire pour toutes les autorités publiques.

Le DPD peut être un membre du personnel du responsable du traitement (DPD interne) ou exercer ses missions sur la base d'un contrat de service (DPD externe).

Dans cet ordre d'idées, la loi du 1er août 2018 précitée dispose que les ministres du ressort ou, sous leur autorité, les chefs d'administration compétents, peuvent désigner le CGPD comme leur délégué à la protection des données. Cette même faculté est offerte aux communes.

La désignation d'un DPD doit être notifiée par le responsable du traitement à la CNPD.

Les missions du DPD sont :

- d'informer et conseiller le responsable du traitement sur les obligations qui lui incombent en vertu de la législation en matière de protection des données ;
- de contrôler le respect des règles de protection des données et des règles internes du responsable du traitement ou du sous-traitant en la matière ;
- de dispenser des conseils, sur demande du responsable du traitement, en ce qui concerne l'analyse des impacts relatifs aux traitements à risques élevés pour les droits et libertés des personnes concernées ;
- de coopérer avec la CNPD et faire office de point de contact pour cette dernière. Le DPD a dès lors vocation à jouer un rôle de « facilitateur » des relations entre la CNPD et le responsable du traitement.

La responsabilité de répondre à l'ensemble des demandes que la CNPD pourrait émettre à l'occasion d'un contrôle sur place, de l'instruction d'une réclamation, d'une consultation sur une analyse d'impact ou de la notification d'une violation de données, repose exclusivement sur le responsable du traitement.

D'après les autorités de protection de données, il est essentiel que le DPD, ou son équipe, soit associé **au stade le plus précoce** à toutes les questions inhérentes à la protection des données.

S'y ajoute que le DPD doit disposer du soutien du responsable du traitement (en particulier en termes de ressources et d'accès aux informations liées aux traitements de données) pour pouvoir exercer ses missions conformément au RGPD.

L'information et la consultation du DPD dès le début permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception. Il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'administration. En outre, il importe que le DPD soit considéré comme un interlocuteur au sein de l'administration et qu'il soit membre des groupes de travail consacrés aux activités de traitement de données.

SECTION 2 :
LE REGISTRE DES ACTIVITÉS DE TRAITEMENT

Chaque administration, en sa qualité de responsable du traitement, voire de sous-traitant, doit tenir un registre des activités de traitement de données.

FORME DU REGISTRE

Le registre des activités de traitement (« registre ») peut être constitué sous forme écrite ou électronique. Son format est libre.

CONTENU DU REGISTRE

Le registre doit comprendre des informations sur tous les traitements de données effectués par l'administration. Il comporte les informations suivantes :

> le nom et les coordonnées du responsable du traitement et du DPD ;

> pour chaque traitement :

- les finalités du traitement ;
- les catégories de personnes concernées ;
- les catégories de données ;
- les catégories de destinataires (y compris dans des pays tiers) ;
- le cas échéant, les transferts de données vers des pays tiers (c'est-à-dire hors de l'espace économique européen) ;
- le cas échéant, les coordonnées du responsable conjoint du traitement ;
- les délais de conservation des données (sinon les critères pour déterminer cette durée) ;
- une description générale des mesures de sécurité techniques et organisationnelles en place pour protéger les données.

LE REGISTRE DU SOUS-TRAITANT

Le sous-traitant doit tenir un registre spécifique pour les activités de traitements réalisées pour le compte de ses clients (ex. : hébergement de base de données, maintenance).

Le registre du responsable du traitement et celui du sous-traitant ne sont donc pas les mêmes.

Si l'organisme agit à la fois en tant que sous-traitant et responsable du traitement, il doit clairement distinguer les deux catégories d'activités.

MISE À DISPOSITION DU REGISTRE À LA CNPD

En cas de demande émanant de la CNPD, le registre devra lui être mis à disposition.

SECTION 3 :
L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Le RGPD prévoit l'obligation pour chaque responsable du traitement d'effectuer des analyses d'impact relatives à la protection des données (« analyse d'impact » ou « AIPD ») pour les traitements susceptibles d'engendrer un **risque élevé** pour les droits et libertés des personnes concernées.

Un tel « risque élevé » existe dans l'hypothèse où le traitement (hypothèses alternatives) :

1. entraine l'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 ;

2. de données sensibles est effectué à grande échelle ;

3. entraine la surveillance systématique à grande échelle d'une zone accessible au public ;

4. correspond au moins à 2 des 9 critères suivants :

   - le traitement consiste dans une évaluation ou notation des personnes concernées, y compris les activités de profilage et de prédiction ;
   - le traitement vise des données sensibles ou hautement personnelles ;
   - le traitement vise des données de personnes vulnérables (ex. : mineurs, personnes en situation de handicap, réfugiés) ;
   - le traitement implique une prise de décision automatisée avec un effet juridique ou similairement significatif ;
   - les données sont traitées à grande échelle ;
   - le responsable du traitement a recours à une technologie innovante pour traiter les données (ex. : intelligence artificielle) ;
   - le traitement entraine une surveillance systématique des personnes concernées ;
   - le traitement entraine un croisement ou une combinaison d'ensembles de données ;
   - le traitement empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service.

5. figure sur la liste de la CNPD des traitements pour lesquels une analyse d'impact est obligatoire (ex.: si le traitement est réalisé à des fins de recherche scientifique).

L'AIPD contient au moins :

- *une description systématique des opérations de traitement ;*
- *les finalités du traitement (y compris, le cas échéant, l'intérêt légitime poursuivi) ;*
- *une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;*
- *une évaluation des risques pour les personnes concernées ;*
- *les mesures envisagées pour faire face aux risques.*

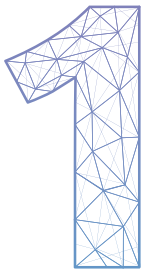
Dans le cadre de l'analyse d'impact, le responsable du traitement doit évaluer la nécessité et la proportionnalité du traitement de données en question et minimiser les risques pour les droits et libertés des personnes concernées.

Lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable, la consultation de la CNPD quant au traitement en question est obligatoire.

SECTION 4 :
LA GESTION DES VIOLATIONS DE DONNÉES

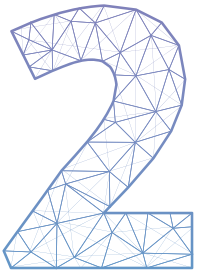
Qu'est-ce qu'une violation de données ?

Une violation de données 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 ».



VIOLATION DE CONFIDENTIALITÉ

En cas de divulgation ou d'accès non autorisé ou accidentel à des données (ex. : envoi d'un courriel contenant des données au mauvais destinataire).



VIOLATION DE DISPONIBILITÉ

En cas de perte ou de destruction accidentelle ou non autorisée de données (ex. : la base de données est temporairement ou définitivement inaccessible, ce qui entraine que les dossiers individuels des administrés ne peuvent pas être traités).

VIOLATION D'INTÉGRITÉ

En cas de modification accidentelle ou non autorisée de données (ex. : dans une base de données, les données sont altérées de manière à ce qu'elles ne correspondent plus à la personne concernée).

Selon les circonstances, une violation peut concerner un ou plusieurs de ces trois cas de figure, et ce sous toutes les combinaisons possibles.

OBLIGATION DE GÉRER LES VIOLATIONS DE DONNÉES DE MANIÈRE APPROPRIÉE

Les administrations doivent être en mesure d'identifier les violations de données dans les meilleurs délais afin de pouvoir réagir de manière appropriée.

Pour ce faire, chaque administration doit :

- mettre en place un **registre interne des violations** de données. Le RGPD ne prescrit pas la méthode et la structure à utiliser pour documenter une violation de données en interne et les mesures mises en œuvre pour réduire le risque en découlant.

Le CGPD conseille toutefois de recenser l'ensemble des éléments relatifs à la violation de données à documenter en s'appuyant sur le formulaire de notification établi par la CNPD (canevas).

- mettre en place une **procédure de gestion des violations de données** informant les agents de leur obligation de rapporter dans les meilleurs délais tout soupçon ou incident de sécurité dont ils prennent connaissance à une personne en charge de leur gestion (cette personne – qui est souvent le DPD – doit être désignée par le responsable du traitement).

La suite que le responsable du traitement doit donner à une violation de données dépend directement du risque engendré par cette dernière :

- si la violation de données **n'est pas susceptible d'engendrer un risque** pour les personnes concernées, elle doit uniquement être documentée dans le registre interne des violations de données ;
- si la violation de données **est susceptible d'engendrer un risque** pour les personnes concernées, elle doit également (c'est-à-dire en sus de la documentation en interne) être notifiée à la CNPD endéans les **72 heures** qui suivent sa prise de connaissance par le responsable du traitement ;
- si la violation de données **est susceptible d'engendrer un risque élevé**, le responsable doit (en sus des actions précitées) également informer la personne concernée de la violation de ses données, et ceci **dans les meilleurs délais**.

	Documenter en interne	Notifier à l'autorité de contrôle	Communiquer à la personne concernée
Aucun risque	✓	✗	✗
Risque	✓	✓	✗
Risque élevé	✓	✓	✓

En tout état de cause, le responsable de traitement doit mettre en oeuvre des mesures techniques et organisationnelles pour limiter les risques émanant de la violation des données et pour limiter les impacts sur la personne concernée.

La présente publication ne prétend pas à l'exhaustivité et n'a pas vocation à couvrir tous les aspects, conditions et exigences de la protection des données.
Les informations contenues dans la présente publication ne préjudicient en aucun cas à une interprétation et application des textes légaux par les administrations étatiques et communales ou les juridictions compétentes.
Le CGPD ne peut être tenu responsable pour d'éventuelles erreurs ou omissions dans la présente publication ou de toutes conséquences découlant de l'utilisation des informations contenues dans celle-ci.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État