Politique de protection de la vie privée -

Protection des données à caractère personnel

# Législation

Le Règlement général sur la proction des données ( ou GDPR) concerne la gestion et la sécurité des données person

# Définitions

## Qu’entend-on par données à caractère personnel ?

Une donnée à caractère personnel est toute information concernant une personne physique identifiée ou identifiable (dénommée "personne concernée" dans la Loi Vie Privée). Autrement dit, une donnée à caractère personnel est toute donnée qui permet d'identifier une personne.

Il peut s'agir du nom d'une personne, d'une photo, d'un numéro de téléphone, même d'un numéro de téléphone au travail, d'un code, d'un numéro de compte bancaire, d'une adresse e-mail, d'une empreinte digitale, …

Il ne s'agit pas uniquement de données qui se rapportent à la vie privée de personnes, mais également de données concernant la vie professionnelle ou publique d'une personne.

On ne tient compte que des données relatives à une personne physique et pas des données relatives à une personne morale ou à une association (société civile ou commerciale ou une a.s.b.l.).

## Qu’est-ce qu’un traitement de données ?

Par "traitement de données", on entend : toute opération éventuelle appliquée à des données à caractère personnel, telle que la collecte, l'utilisation, la gestion ou la communication d’informations.

La loi s'applique dès que les opérations effectuées sur des données personnelles se réalisent, ne fût-ce qu'en partie, par des moyens automatisés. Les moyens automatisés englobent toutes les technologies de l'information: informatique, réseaux de télécommunication (Internet), …

Quand les opérations sur les données se font sans recours à des procédés automatisés (sur papier notamment), il faut tout de même respecter la loi si les données figurent ou sont destinées à figurer dans un fichier manuel, c'est-à-dire un ensemble dans lequel les données sont accessibles selon des critères spécifiques (par exemple, un classement, par ordre alphabétique, des noms des personnes,).

## Qui est le responsable du traitement ?

C'est sur cette personne que repose la charge de presque toutes les obligations imposées par la loi pour assurer la protection des données traitées.

C'est aussi le responsable du traitement qui est l'interlocuteur principal des personnes concernées et des autorités de contrôle.

Le responsable du traitement est la personne qui détermine les objectifs et les moyens de ce traitement de données. Il peut s'agir d'une personne physique ou morale (par exemple, une entreprise).

Le responsable du traitement ne doit pas effectuer le traitement lui-même, il peut faire appel à un [sous-traitant](http://www.privacycommission.be/fr/lexique/sous-traitant), c’est-à-dire qu’une autre personne effectue le traitement concret mandaté par le responsable du traitement. Ainsi, il arrive souvent qu’un secrétariat social s’occupe de certains traitements pour le compte d’un employeur.

# Formalités préalables

## Déclarations des traitements et registre public

Avant que le responsable du traitement n'effectue un traitement automatisé, il doit déclarer ce traitement à la Commission vie privée.

Toutes les informations figurant dans cette déclaration sont reprises dans le registre public.

Tout le monde peut consulter ce registre dans les locaux de la Commission de la vie privée ou en ligne. Un extrait du Registre peut également être demandé.

## Contenu de la déclaration

La déclaration contient une description des caractéristiques du traitement. Les données suivantes doivent être reprises :

* la dénomination du traitement ;
* les finalités ;
* les catégories de données traitées (et donc pas les données elles-mêmes) ;
* l'éventuelle base légale ou réglementaire permettant le traitement ;
* les destinataires potentiels à qui les données peuvent être fournies ;
* …

## Exemptions à l’obligation de déclaration

Les traitements manuels ne doivent pas être déclarés.

Certains traitements automatisés sont exemptés de l'obligation de déclaration moyennant le respect de certaines conditions mentionnées dans l'Arrêté Royal du 13 février 2001 :

* l'administration du personnel,
* l'administration des salaires,
* la comptabilité,
* la gestion de la clientèle et des fournisseurs à la condition
  + que le fichier ne se rapporte, ni à des données relatives à la santé de la personne concernée, ni à des données sensibles ou judiciaires;
  + qu’aucune donnée à caractère personnel ne soit enregistrée sur base d'informations obtenues de tiers
  + que les données ne soient pas communiquées à des tiers (sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou encore aux fins de la gestion normale d'entreprise).
* Les données à caractère personnel traitées par une ASBL
* …

Cette exemption ne signifie toutefois pas que les autres dispositions légales ne doivent pas être respectées.

# Collecte des données

## Obligations en cas de collecte de données à caractère personnel?

La collecte doit être *loyale.* Cela signifie que l'on doit agir de manière transparente: celui qui collecte des informations doit indiquer pourquoi il veut obtenir des données personnelles. Il ne peut faire croire qu'il poursuit un but alors qu'il a l'intention de faire autre chose avec les informations recueillies.

On ne peut pas non plus agir à l'insu des personnes. Par exemple, si une commande est faite via internet et que vous devez communiquer des données à caractère personnel à cette fin, le site web en question doit comporter une rubrique décrivant comment vos données seront traitées. Dans la plupart des cas, cette rubrique s'appelle "privacy policy".

Aux personnes auprès desquelles les données sont recueillies, il faut *fournir les informations suivantes :*

* dans quel but les informations sont collectées ;
* le nom et l'adresse du responsable du traitement ;
* les destinataires des données ;
* l'existence d'un droit d'accès et d'un droit de rectification des données ;
* si les données seront traitées à des fins de marketing direct (démarches publicitaires), il faut signaler aux personnes concernées qu'elles disposent du droit de s'opposer gratuitement à un tel traitement.

## Quelles données peut-on collecter ?

On ne peut collecter que les données qui sont *pertinentes et nécessaires par rapport à*  l'objectif annoncé.

On n'a pas le droit de collecter certaines *données qui sont par nature sensibles.* Il s’agit des données relatives à la race, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives. Il est en principe interdit de récolter ces données. Certaines exceptions sont toutefois admises.

## Peut-on se fournir en données auprès de tiers ?

Des données peuvent être obtenues auprès de tiers mais la personne concernée doit en être informée et recevoir l’information reprise ci-dessus.

# A quelles conditions peut-on traiter des données à caractère personnel ?

Pour pouvoir traiter des données personnelles, deux conditions doivent être remplies :

## Poursuivre un objectif particulier et légitime

### Un ou plusieurs objectifs particuliers

Les données personnelles ne peuvent être recueillies qu'en vue d'un ou de plusieurs *objectifs particuliers*. C'est ce but décidé au départ qui va orienter toute la suite des opérations.

C'est en fonction de l'objectif poursuivi que l'on saura

* quelles données on peut collecter,
* ce que l'on peut faire avec ces données,
* si on peut les communiquer et à qui,
* ...

On ne peut faire que ce qui répond à ou aux objectifs poursuivis et ce qui est *compatible* avec ces objectifs. On considère comme compatible notamment ce qui est prévu par la loi et ce que la personne concernée peut raisonnablement prévoir.

Ne se conforment par exemple pas aux principes légaux :

* le club de fitness qui vend son registre d'adhérents à une société qui propose des cures d'amaigrissement;
* l'oculiste qui communique le nom de ses patients à une société spécialisée dans la vente de lentilles de contact (par contre, il peut communiquer un dossier à un confrère duquel il veut avoir l'avis);

### Un objectif légitime

Cela signifie qu'un équilibre doit exister entre l'intérêt du responsable du traitement et les intérêts des personnes sur qui portent les données traitées.

On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées.

Par exemple

* On ne peut pas considérer comme légitime le fait de constituer un fichier des personnes proches de la soixantaine pour leur envoyer le jour de leur 60e anniversaire une documentation sur une assurance pour subvenir aux frais d'un enterrement ou d'une crémation, "car il devient temps d'y songer". L'atteinte portée aux personnes est sans aucun doute supérieure à l'intérêt commercial du responsable du traitement.

## Se trouver dans une des hypothèses suivantes :

Des données personnelles ne peuvent être traitées que :

* si la personne concernée a sans ambiguïté donné son CONSENTEMENT. Le consentement n'est valable que s'il est libre (c'est-à-dire s'il a été émis sans pression), spécifique (le consentement doit porter sur un traitement précis) et informé (la personne a reçu toute l'information utile sur le traitement envisagé).
* si le traitement des données est nécessaire à l'exécution d'un CONTRAT ou à l'exécution de mesures précontractuelles sollicitées par la personne concernée. C'est le cas de l'enregistrement de données pour permettre l’établissement d’ un contrat d'assurance,
* si le traitement est exigé par une LOI, un décret ou une ordonnance ;
* si le traitement est nécessaire pour sauvegarder un INTÉRÊT VITAL de la personne concernée. C'est le cas de l'accidenté inconscient, à propos duquel on rassemble des données médicales (résultats de tests sanguins, notamment) afin de le soigner;
* si le traitement des données est nécessaire pour exécuter une MISSION D'INTÉRÊT PUBLIC. A ce titre, la Poste est autorisée à créer un fichier des changements d'adresses pour lui permettre de faire suivre le courrier en cas de déménagement;
* enfin, si le traitement des données est nécessaire pour réaliser un INTÉRÊT LÉGITIME du responsable ou d'un tiers, à condition que l'intérêt ou les droits de la personne concernée ne prévalent pas.

# Données sensibles

## Quelles sont les données sensibles?

Il s’agit de données délicates comme la race, la santé, les opinions politiques, les convictions philosophiques (croyant ou athée, etc.), les préférences sexuelles ou le passé judiciaire.

En principe, il est interdit de collecter, d’enregistrer ou de demander à pouvoir communiquer ces données sensibles.

A l'exception des données relatives à des suspicions, des poursuites et des condamnations, les données sensibles peuvent être traitées moyennant le respect de certaines conditions très précises.

## Traitements autorisés

Des [données sensibles](http://www.privacycommission.be/fr/lexique/donnees-sensibles) ne peuvent être traitées que moyennant le *consentement écrit* de la personne concernée. Cette exception n'est toutefois pas valable lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement (par exemple l’employeur).

Dans une telle situation, le consentement écrit est tout de même admis s'il permet d'octroyer un avantage à la personne concernée.

Ces données peuvent également être traitées

* si c'est indispensable pour prodiguer les soins nécessaires à la personne concernée (le traitement doit alors se faire sous la surveillance d'un professionnel des soins de santé);
* si la législation du travail ou l'application de la sécurité sociale l'impose ;
* la personne concernée elle-même a rendu les données publiques (l'appartenance politique d'une personne ayant mené une campagne électorale, par exemple);
* si c'est nécessaire dans le contexte d'une recherche scientifique
* les partis politiques, congrégations, syndicats ou autres organismes peuvent bien sûr enregistrer et utiliser des données de leurs membres. Ils ne peuvent toutefois pas communiquer ces données à des tiers sans le consentement des personnes concernées.

## Précautions supplémentaires

Dans toutes ces hypothèses, des garanties supplémentaires sont à respecter, notamment :

* le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par rapport au traitement des données ;
* lors de l'information de la personne concernée, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement des données. Cela permet de contrôler sur quoi il se base pour traiter des données en principe interdites ;
* enfin, lorsqu'on se fonde sur le consentement écrit d'une personne pour traiter ses données sensibles, il faut signaler à cette personne les motifs pour lesquels ces données sont traitées et lui communiquer la liste des catégories de personnes ayant accès aux données.

# Que doit-on faire avec les données recueillies ?

## Veiller à la qualité des données

Les données que l'on traite doivent être exactes et, si c'est nécessaire, mises à jour. Le responsable du traitement doit prendre toutes les mesures raisonnables pour corriger ou effacer les données qui sont inexactes ou incomplètes.

## Veiller à la confidentialité des données

Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité n'aient accès et ne puissent utiliser que les données dont elles ont besoin pour exercer leurs fonctions. Il n'est pas question de permettre aux membres du personnel d'avoir accès à des données qui ne leur sont pas nécessaires.

Le responsable doit en outre mettre son personnel au courant des prescrits de la loi sur la protection des données. Il doit expliquer les principes de protection qui doivent désormais être respectés.

## Veiller à la sécurité des données

Il est important de protéger les données contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées.

Il est essentiel de prendre des mesures de sécurité pour protéger les données.

Ces mesures de sécurité sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques.

Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (par une compagnie d'assurance pour octroyer une assurance-vie, par exemple), devront être encadrées de mesures de sécurité sévères.

## Effacer les données

Les données personnelles ne doivent pas être conservées sous une forme qui permet d'identifier les personnes plus longtemps qu'il n'est nécessaire par rapport à l'objectif poursuivi. Il convient alors de les effacer ou de les rendre anonymes.

# Droits des personnes concernées

## Le droit à l’information

On ne peut pas traiter des données personnelles à l'insu des personnes concernées. A partir du moment où l'on recueille des données sur des personnes, on doit mettre ces personnes au courant de ce que l'on compte faire de ces données. La loi indique quelles informations doivent être communiquées.

## Le droit de poser des questions

Chaque personne a le droit d'interroger tout responsable de traitement pour savoir s'il détient ou non des données sur lui. Si le responsable interrogé détient des données relatives à cette personne, il doit préciser dans quel but il détient les données, de quelles catégories de données il s'agit et quels sont les destinataires de ces données.

## Le droit d’accès direct

### A quoi les personnes concernées ont-elles accès ?

Chacun a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information disponible sur l'origine des données. Le droit de connaître la provenance des données utilisées est particulièrement important car c'est souvent la question de la source des informations qui préoccupe les personnes concernées.

Il arrive qu'une décision affectant de manière significative une personne soit prise sur la seule base d'un traitement automatisé (cela peut être le cas pour l'octroi d'un prêt ou la souscription d'une assurance, par exemple). Dans ce cas, la personne en cause doit pouvoir avoir aussi accès à la logique qui sous-tend le traitement automatisé en question.

### Comment le droit d’accès doit-il être exercé ?

Pour exercer son droit d'accès, il faut adresser une demande au responsable du traitement en faisant la preuve de son identité (en joignant la photocopie de sa carte d'identité, par exemple). La demande peut être envoyée par la poste ou par tout moyen de télécommunication (par fax, par courrier électronique avec apposition d'une signature électronique).

Le responsable doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande.

## Le droit d’accès indirect

En deux circonstances, la personne concernée a un accès indirect à ses données.

L'accès aux données relatives à sa santé peut s'effectuer soit directement par la personne sur qui portent les données, soit par l'intermédiaire d'un professionnel des soins de santé choisi par cette personne, si le responsable du traitement ou la personne elle-même demande l'intervention d'un intermédiaire.

Pour les données traitées à des fins de sûreté de l'État, de sécurité publique, de défense nationale, de prévention ou de répression des infractions, c'est également un accès indirect qui est mis en place.

## Le droit de rectification

Chacun peut, sans frais, faire rectifier les données inexactes qui se rapportent à lui et faire effacer ou interdire l'utilisation les données incomplètes, non pertinentes ou interdites.

Le responsable du traitement doit répondre dans le mois à la personne qui a demandé les corrections. Il doit indiquer les rectifications ou effacements qu'il a effectués. S'il ne le fait pas, la personne concernée peut s'adresser à la Commission vie privée en dénonçant son comportement.

Elle peut également porter plainte en justice.

Si des données inexactes, incomplètes, non pertinentes ou interdites ont été transmises à des tiers, le responsable doit, dans le mois, signaler les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées, à moins que cela ne s'avère impossible ou extrêmement difficile.

## Le droit d’opposition

Chacun a le droit de s'opposer à ce que les données le concernant fassent l'objet d'un traitement, mais il doit invoquer des raisons sérieuses et légitimes.

Limites du droit d'opposition : le droit d'opposition n'est pas admis pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat ; les personnes concernées ne peuvent pas non plus s'opposer au traitement de leurs données imposé par une obligation légale ou réglementaire.

Lorsque les données sont collectées à des fins de marketing direct (notamment, pour des démarches publicitaires), la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement de ses données. Ainsi, lorsque l'on est invité à remplir un talon-réponse, si celui qui récolte les données a l'intention de les transmettre à des sociétés de marketing direct, il doit le mentionner sur le talon et la personne concernée a le droit de s'opposer sans justification à ces transmissions.