

Partie 1:

Droit de la protection des données à caractère personnel

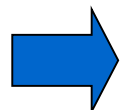
Franck Dumortier
franck.dumortier@unamur.be

Respect de la Vie Privée

Les bases légales

- ✓ Article 8 de la Convention Européenne des Droits de l'Homme:
*« Toute personne a droit au **respect de sa vie privée** et familiale, de son domicile et de sa correspondance
Il ne peut y avoir ingérence dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure nécessaire dans une société démocratique » Voir [ici](#)*

- ✓ Article 22 de la Constitution:
*« Chacun a droit au **respect de sa vie privée** et familiale, sauf dans les cas et conditions fixés par la loi. »*



Mais qu'entend-t-on donc par « **vie privée** »?

Evolution du concept de « vie privée » (1)

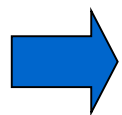
- ✓ « Il faut se réserver une arrière-boutique toute nôtre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude » MONTAIGNE
- ✓ « The right to be let alone » - le droit d'être laissé seul
WARREN & BRANDEIS (1890)
- ✓ « La solitude à plusieurs » : La liberté de conduire ses relations avec autrui sans être exposé à une immixtion illicite F. RIGAUX (1984)



Sphère intime à l'abri des immixtions, des regards

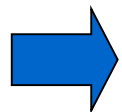
Evolution du concept de « vie privée » (2)

- ✓ « Le droit au respect de la vie privée consiste essentiellement à pouvoir mener sa vie comme on l'entend avec un minimum d'ingérence » Recomm. Ass. Conseil de l'Europe 23.01.1970
- ✓ Arrêt Guerra c. Italie de la Cour E.D.H., 19.02.1998
- ✓ Arrêt Pretty c. RU de la Cour E.D.H., 29.04.2002



Droit à l'épanouissement, liberté d'être soi
Pouvoir poser certains choix existentiels

- ✓ Arrêt de la Cour constitutionnelle allemande, 15.12.1983
« Recht auf Informationelle Selbstbestimmung »:



Droit à l'autodétermination informationnelle

1. Risques d'atteintes à la vie privée liés aux technologies:

- Le manque de sécurité informatique
- L'opacité des traitements et le manque d'information
- Une érosion du principe de finalité

+

2. Risques d'atteintes à la vie privée liés aux bases de données:

- Conservation trop longue des données
- Données inexactes ou non pertinentes
- Données sensibles

=

3. Risques d'atteinte plus graves

- Discrimination
- Restriction de la liberté de circulation
- Restriction de la liberté d'opinion (politique, religieuse, etc.)

Protection des données à caractère personnel : bases légales

- ✓ **Convention n° 108** du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981) (Voir [ici](#))
- ✓ **Directive 95/46/CE** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Voir [ici](#))
- ✓ **Loi du 8 décembre 1992** relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Voir [ici](#))
- ✓ **Règlement général sur la protection des données** (« GDPR ») du 27 avril 2016 (abrogeant la directive 95/46/CE) applicable dès mai 2018 (et ne nécessitant « pas » de transposition en droit belge) (Voir [ici](#))

GDPR: objectifs

1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.
2. Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.
3. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite (/shall be neither restricted nor prohibited) pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Finalité

Proportionnalité

Transparence

Champ d'application de la loi

La loi (et GDPR) s'applique quand il y a :

- ✓ traitement
- ✓ de données personnelles
- ✓ automatisé en tout ou en partie OU
- ✓ manuel (organisation de données dans fichiers – voir slide suivant)

La loi ne s'applique PAS aux :

- ✓ traitements personnels (domestiques)

- ✓ **Exclusions** (art. 2, § 2): pour les traitements de DACP effectués:
 - a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union;
 - b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne;
 - c) par une personne physique dans le cadre d'une **activité strictement/ exclusivement personnelle ou domestique**;
 - d) **par les autorités compétentes à des fins de prévention et de détection des infractions pénales**, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. (mais Directive « police » - voir [ici](#))

Considérant 18 GDPR:

« Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ».

Champ d'application de la loi/GDPR

✓ Fichier (loi/GDPR applicable):

« *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » - Art. 4, 6, GDPR

✓ Dossier (loi/GDPR non applicable):

« *Les **dossiers** ou ensembles de dossiers de même que leurs couvertures, qui n sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent règlement* » - Cons. 15 GDPR

✓ Considérant 14 GDPR:

« La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. **Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales**, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale ».

Notions de base

Donnée à caractère personnel

- ✓ Information qui concerne une **personne physique** identifiée ou identifiable
 - Identifiable? (**directement ou indirectement...**)
 - Exemples :
 - Nom, prénom, âge, sexe, nationalité, état civil
 - Adresse, numéro de téléphone, ... (**y compris sur le lieu de travail**)
 - Données relatives à la santé
 - Profession, religion, orientation politique, loisirs
 - Photo, video
 - Empreintes et autres données biométriques
 - Numéro d'immatriculation
 - Casier judiciaire
 - Cookie, adresse IP, adresse e-mail (si on peut remonter à la personne)



Notion très large : voir l'avis du Groupe de l'article 29 ([ici](#))

Notions de base

Donnée à caractère personnel

✓ Le GDPR confirme la définition large.

« **Données à caractère personnel** » (DACP): *toute information se rapportant à une personne physique identifiée ou identifiable; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.* (Art. 4, §1^{er} GDPR)

➡ Définition très large des DACP dans le GDPR: Le ciblage (« singling out » - « l'individualisation ») est considéré comme permettant l'identifiabilité. (Cons. 26 GDPR)

➡ Peuvent être considérées comme DACP les adresses IP, cookies, tags RFID... (Cons. 30 GDPR)

- ✓ Loi 1992: Une opération ou un ensemble d'opérations effectuées à l'aide ou non de procédés automatisés et appliquée(s) à des données à caractère personnel

- ✓ Exemples :
 - Collecte, enregistrement, organisation
 - Conservation, adaptation, modification, extraction
 - Consultation, utilisation
 - Communication par transmission, diffusion ou autre mise à disposition
 - Rapprochement, interconnexion
 - Verrouillage, effacement, destruction, anonymisation

- ✓ Art. 4, §2, GDPR : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, **la limitation**/le verrouillage, l'effacement ou la destruction »
- ✓ Art. 4, §3, GDPR - **limitation du traitement**: « le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur »



Je recherche...

OK

NL

CITOYENS

CULTURE & LOISIRS

COMMUNE

JE SUIS...

Démarches administratives

S'établir à Ixelles

Obtenir un document en ligne

Identité / Nationalité

Naissance

Cohabitation légale

Mariage

Divorce

Décès

Construction / Rénovation

Taxes, redevances et impôts

Quitter Ixelles

Organiser un événement

Obtenir un document en ligne

Commande de documents en ligne

Ce service vous permet de commander un document et de payer directement en ligne (s'il s'agit d'un document payant). Le document sera délivré à votre domicile par la Poste.

Ce système présente de nombreux avantages, notamment en termes de sécurité et de paiement en ligne.

Afin de pouvoir utiliser ce service, vous devez :

- posséder un [lecteur de carte](#);
- posséder une [carte d'identité électronique](#) et en connaître le [code PIN](#);
- installer la dernière version du [logiciel eID](#);
- installer la dernière version de [java](#);
- insérer votre carte d'identité électronique dans le lecteur et accepter l'enregistrement des certificats;
- vous connecter sur le [site web de Irisbox](#).

Vous pouvez maintenant commander les documents suivants :

- extrait d'acte de naissance;
- extrait d'acte de mariage;
- extrait d'acte de divorce;
- extrait d'acte de décès;
- carte de stationnement;
- certificat de nationalité;
- certificat de composition de ménage;
- certificat de domicile et de résidence;
- certificat de résidence avec historique de l'adresse;
- certificat de vie;
- déclaration de changement d'adresse.



Ouverture d'un compte Yahoo! - Mozilla Firefox

Echier Edition Affichage Aller à Marque-pages Outils ?

http://edit.europe.yahoo.com/config/eval_register?.intl=fr&new=1&.done=http://fr.promotions.yahoo.com/mail/transfertmail.html&.src=ym&partner=&.p=&promo=&.last=

IMP Droit et Nouvelles Technologies: Membre Ouverture d'un compte Yahoo!

Yahoo! MAIL [Yahoo! - Aide](#)

Vous avez déjà un compte Yahoo! ou une adresse mail ? [Ouvrir session](#).

Les champs précédés d'une astérisque * sont obligatoires.

Créer mon compte Yahoo!

* Prénom :

* Nom :

* Sexe : [choisir] ▼

* Compte Yahoo! : @yahoo.fr
Lettres, chiffres et souligné, seulement.

* Mot de passe :
Au moins 6 caractères (attention, les majuscules comptent!)

* Saisir à nouveau le mot de passe :

En cas d'oubli de mot de passe...

* Question secrète : [Choisir une question] ▼

* Votre réponse :
Au moins 4 caractères (choisissez une réponse facile à retenir pour vous et difficile à deviner pour les autres).

* Date de naissance : jj [Mois] ▼ aaaa ?

* Code postal :

* Pays : France ▼


Adresse mail alternative : ?

Email d'information sur l'actualité des produits et services Yahoo!

☒ Je veux recevoir les emails d'information sur l'actualité des services Yahoo! (je peux me désabonner à tout moment).

Confirmer votre inscription

* Code sur l'image ci-dessous : [Plus d'infos sur ce champ](#) ⓘ
Cette étape sert à éviter les inscriptions automatisées.



Conditions d'Utilisation du Service

Veuillez prendre connaissance des Conditions d'Utilisation du Service ci-dessous et en accepter les termes en cliquant sur le bouton "J'accepte". [Version imprimable](#) ⓘ

1. ACCEPTATION DES CONDITIONS D'UTILISATION

Bienvenue sur Yahoo! Yahoo! France vous fournit ses services sous réserve que vous vous engagiez à respecter les présentes conditions d'utilisation

Terminé

Notions de base Pseudonymisation

✓ Pseudonymisation:

- Art. 4, § 4, GDPR: « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise **sans avoir recours à des informations supplémentaires**, pour autant que ces informations supplémentaires **soient conservées séparément** et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »
- Considérant 26 RGPD: « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation **et/**, qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».

✓ Pseudonymisation:

- Cons. 28 GDPR: « *La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données* ».

Notions de base Données anonymes

✓ Considérant 26 dir. 95/46:

*« données rendues anonymes d'une manière telle que la personne concernée **n'est plus identifiable** »*

✓ Considérant 26 GDPR:

*« les informations **ne concernant pas** une personne physique identifiée ou identifiable + données à caractère personnel rendues anonymes de telle manière que la personne concernée **ne soit pas ou plus identifiable** ».*

Notions de base

Responsable du traitement/sous-traitant

- ✓ **Responsable du traitement** : Celui (personne physique ou morale) qui décide (seul ou avec d'autres):
 - quelles données vont être traitées
 - dans quel but elles vont être traitées
 - par quel(s) moyen(s)

- ✓ « **Par "sous-traitant"**, on entend la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel **pour le compte du** responsable du traitement **et est autre que la personne qui, placée sous l'autorité directe** du responsable du traitement, est habilitée à traiter les données. »

✓ Art. 3bis.

« La présente loi est applicable au traitement de données à caractère personnel

*1° lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un **établissement fixe du responsable du traitement sur le territoire belge** ou en un lieu où la loi belge s'applique en vertu du droit international public;*

*2° lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne et recourt, à des fins de traitement de données à caractère personnel, **à des moyens automatisés ou non, situés sur le territoire belge**, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge »*^{24/}

✓ Art. 3, § 1er GDPR:

*« Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un **établissement** d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, **que le traitement ait lieu ou non dans l'Union** ».*

+ voir slide suivant

✓ Art. 3, § 2 GDPR

« Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

- a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
- b) Au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Conditions de traitement de DACP

✓ **Les données doivent être :**

- a) **traitées de manière licite, loyale et transparente** au regard de la personne concernée (licéité, loyauté, transparence);
- b) **collectées pour des finalités déterminées**, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; (limitation des finalités);
- c) **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
- d) **exactes et, si nécessaire, tenues à jour**; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes,, soient effacées ou rectifiées sans tarder (exactitude);
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une **durée n'excédant pas celle nécessaire** au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation);
- f) traitées de façon à garantir une **sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

Légitimité du traitement de DACP

Les traitements dans un but déterminé et légitime **sont autorisés uniquement dans l'un des cas suivants :**

1. La personne dont on traite les données **a donné indubitablement son consentement** de manière libre, spécifique et informée
2. Le traitement est **nécessaire pour exécuter un contrat** (ou des mesures précontractuelles prises à la dde de la personne) Ex. : pour la livraison, la facturation, l'octroi d'un crédit...
3. Le traitement **est exigé par la loi** Ex.: un employeur doit transmettre à l'ONSS les données relatives à ses employés
4. **Interêt vital** de la personne concernée Ex. : personne accidentée dont on transfère les données médicales d'un hôpital à l'autre.
5. **Mission d'intérêt public** Ex. : Les traitements du Ministère des Finances
6. Si l'intérêt légitime du responsable du traitement est supérieur à l'intérêt de la personne dont on traite les données (Balance d'intérêts a priori)

Conditions applicables au consentement

1. Le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

✓ Art. 9 GDPR:

*« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique **sont interdits** ».*

Mais exceptions.... (voir slides suivant)

Données « sensibles »

Exceptions

- ✓ la personne concernée a donné son **consentement explicite**
- ✓ le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits en matière de droit du travail, de la sécurité sociale et de la protection sociale,
- ✓ le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
- ✓ le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale
- ✓ le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée
- ✓ le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice
- ✓ le traitement est nécessaire pour des motifs d'intérêt public important,
- ✓ le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale;
- ✓ le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux
- ✓ le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Obligations et droits dans la loi actuelle

Obligations dans la loi « vie privée » actuelle

✓ Les obligations du responsable du traitement :

1. Déclaration à la Commission vie privée (**ATTENTION ! Supprimé dans le GDPR**);
2. Information;
3. Sécurité.

✓ Droits de la personne concernée:

1. **Droit d'accès :**
 - recevoir (sur demande) copie des données la concernant
 - demander au responsable s'il détient des données la concernant, lesquelles et pourquoi et à qui elles sont transférées
2. **Droit de rectification des données inexacts la concernant**
3. **Droit de suppression de données inexacts, incomplètes ou non pertinentes**
4. **Droit d'opposition :**
 - si raisons légitimes, droit de s'opposer au traitement (à moins qu'il ne soit nécessaire à l'exécution du contrat ou exigé par la loi),
 - droit d'opposition sans raison si *marketing direct*

Obligations du sous-traitant:

1. Agir sur instruction du responsable
2. Respecter le contrat de sous-traitance
3. Sécurité



Le sous-traitant a beaucoup moins d'obligations que le responsable du traitement mais TOUS DEUX ONT UNE OBLIGATION DE SECURITE

1. Déclaration

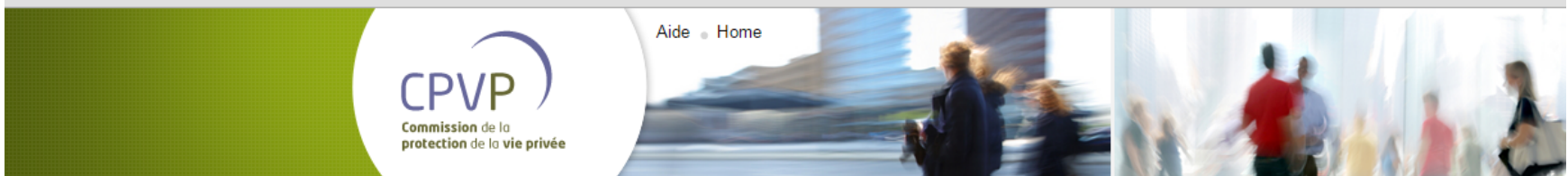
- ✓ Obligation de déclarer le traitement de données personnelles à la Commission de la protection de la vie privée (supprimé dans le GDPR)

Comment ? Formulaire à remplir :

<https://eloket.privacycommission.be/elg/main.htm?siteLanguage=fr>

← → ↺ 🏠 <https://elokit.privacycommission.be/elg/newGeneralDeclaration.htm?clearSession=true#>

Applications TV Partout - Progra... Your stream on Sou... T411 - Torrent 411 -... Bande Dessinée - T... Torrent a telecharge... Download .kikassto... Unmechanical Gam... Beginne



Aide • Home

Compléter une nouvelle
déclaration >

Compléter une nouvelle
déclaration thématique d'une
caméra de surveillance >

Gestion de déclaration >

1. Responsable du traitement



Numéro attribué par la Commission au responsable

HM

Nom (ou dénomination de la personne morale, de l'association de fait ou de l'administration publique)*

Traduction éventuelle du nom ou autre dénomination

Abréviation courante du responsable

Traduction éventuelle de l'abréviation courante

Pays*

Numéro d'entreprise/Numéro de TVA

(BTW BE 0123.456.789)

Rue*

Numéro*

Boîte

Commune*

Sélectionner une commune

Code postal*

Statut juridique du responsable de traitement*

Sauvegarder un brouillon

Imprimer

Annuler

Le registre public des déclarations est accessible via

<https://eloket.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=fr>

Rechercher un traitement dans le registre public

Traitement:

Responsable: commune d'ixelles

Rechercher

Effacer

Rue:

Numéro:

Code postal:

Résultat de la recherche

23 items résultat 23 items montrer, image: 1 à 10.
[Premier/Précédent] 1, 2, 3 [Suivant/Dernier]

Traitement	Responsable	Code postal	Ville/Commune
Création d'un fichier informatisé dans le cadre de la gestion des utilisateurs de la bibliothèque néerlandophone à Ixelles. Le Numéro de registre National des personnes physiques sera utilisé comme identifiant unique directement dans le logiciel de la bibliothèque.	Commune d'Ixelles	1050	Ixelles
OBJET : CONCEPTION ET DIFFUSION D'UNE NEWSLETTER ELECTRONIQUE COMMUNALE Une newsletter, ou lettre d'information électronique, est un document d'information envoyé de manière périodique par courrier électronique (e-mail) à une liste de diffusion regroupant l'ensemble des personnes qui y sont inscrites. La lettre d'information peut également être consultée depuis un site internet. Informer les Ixellois des dernières nouvelles de l'administration communale d'une manière rapide, attrayante, moderne, simple et gratuite. Avant de s'inscrire le citoyen doit cocher la mention légale suivante : « La Commune d'Ixelles peut utiliser ces données pour informer sur ses activités, services et publications. En aucun cas, ces données ne seront utilisées à des fins politiques, commerciales ou autres. » A tout moment, le citoyen aura la possibilité de se désinscrire facilement et rapidement. Chaque citoyen peut s'inscrire via le site web de la commune. Il doit tout simplement compléter une case avec son adresse mail. Il recevra automatiquement un mail de vérification contenant un lien. En cliquant sur ce lien, il confirme sa son inscription à la newsletter communale. Au service Population, les nouveaux arrivants auront la possibilité (pas d'obligation !) de remplir un petit formulaire sur un carton (format A6). Leur adresse mail sera ensuite encodée par un agent du service Population via le site communal et le carton sera détruit. De nouveau, le citoyen recevra un mail de vérification pour confirmer son inscription à la newsletter communale. chaque numéro de la newsletter donnera la possibilité aux abonnés de se désinscrire rapidement et facilement. Cela implique que le fichier des abonnés se met à jour automatiquement ! La newsletter pourra également être consultée depuis le site web communal. La newsletter sera diffusée en français et en néerlandais, selon la langue	Commune d'Ixelles - Collège des Bourgmestre et Echevins	1050	Ixelles

Exemptions (dans AR)

- ✓ Administration des salaires
- ✓ Administration du personnel
- ✓ Comptabilité
- ✓ Administration d'actionnaires et d'associés
- ✓ Gestion de la clientèle et des fournisseurs
- ✓ Administration des membres
- ✓ Simple contact avec l'intéressé
- ✓ Contrôle d'accès
- ✓ Gestion des relations avec les étudiants et les profs
- ✓ Registres de la population
- ✓ Registres publics
- ✓ Régime spécifique

Voir le texte de l'AR ([ici](#)). Art 51 et suivants

2. Information

Informations de base :

1. L'identité et l'adresse du responsable du traitement
2. Le but du traitement (*finalité*)
3. Le fait que le personne a toujours le droit de s'opposer au traitement de ses données à des fins de marketing

Informations supplémentaires :

1. Destinataires ou catégories de destinataires
2. Caractère obligatoire ou non des informations à fournir, conséquences défaut
3. Droit d'accès, de rectification

2. Information

Quand fournir ces informations ?

- Au moment de la collecte des données (sauf si déjà informée)
- ou dès l'enregistrement (ou la première communication) en cas de collecte indirecte

Comment fournir ces informations ?

De manière loyale...

Exemptions

Infos 'supplémentaires' :

- ✓ pas si pas nécessaires pour traitement loyal

Toutes les infos:

- ✓ Information impossible ou disproportionnée
 - Statistique, historique, scientifique, dépistage
- ✓ Enregistrement ou communication réalisée par application d'une loi (décret, ordonnance)

3. Obligation de sécurité

✓ Art. 16, §4 de la loi du 8 décembre 1992 :

« Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu:

- 1) d'une part, de l'état de la technique en la matière
- 2) et des frais qu'entraîne l'application de ces mesures et,
- 3) d'autre part, de la nature des données à protéger
- 4) et des risques potentiels (...) »

3. Obligation de sécurité

✓ L'obligation de sécurité selon la CPVP:

- Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel ([lien](#))
- Lignes directrices pour la sécurité de l'information ([lien](#))
- Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données ([lien](#))

➡ La CPVP recommande déjà:

- La présence d'un **conseiller en sécurité** (en fonction de la nature des données)
- L'**organisation et aspects humains** de la sécurité de l'information
- La **sécurité physique** et de la **sécurisation des réseaux**
- La **sécurisation logique des accès** et la **journalisation, traçage et analyse des accès**
- La **surveillance, revue et maintenance** (audits)
- La **gestion des incidents de sécurité** et de la **continuité**
- De **disposer d'une documentation**

✓ Mesures de références CPVP:

7. Journalisation, traçage et analyse des accès

L'organisme doit mettre en œuvre des mécanismes de journalisation et de traçage.

Ces derniers doivent permettre de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci. L'enregistrement de ces informations de contrôle peut concerner, suivant les cas, l'accès physique, l'accès logique ou les deux.

La granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte. Des mécanismes supplémentaires de détection d'intrusion pourraient être requis. Le conseiller en sécurité de l'information doit être en mesure de justifier la politique adoptée.

Les données de traçage étant elles-mêmes des données à caractère personnel, tout traitement de celles-ci doit s'accompagner des mesures de sécurité adéquates.

Recommandation de notification dans la loi « vie privée » actuelle

✓ Recommandation CPVP 01/2013 :

2.5. GESTION DES INCIDENTS

24. L'organisme doit disposer de procédures d'alertes connues et documentées à appliquer en cas d'incidents portant atteinte à la sécurité des informations à caractère personnel. Ces procédures doivent mentionner l'identification et les coordonnées des responsables à contacter au niveau technique et au niveau management.
25. Une attribution claire des responsabilités de sécurité, que ce soit en régime et/ou en cas d'incident, doit être établie au sein de toute organisation.
26. Plus particulièrement, en cas d'incident public, les autorités compétentes (Commission vie privée) doivent être informées des causes et des dommages endéans les 48 heures.
27. Une campagne d'information au public doit aussi être réalisée 24 à 48 heures au plus tard après notification aux autorités.

Recommandation de notification dans la loi « vie privée » actuelle



The screenshot shows the website of the Commission de la protection de la vie privée (CPVP). The header includes a navigation menu with links: Plan du site, Lexique, FAQ, Presse, Liens, and Contact. Below the header, there are four main sections: THÈMES DE VIE PRIVÉE (Nos activités quotidiennes), LÉGISLATION ET NORMES (Textes de référence relatifs à la protection des données), DÉCISIONS (Nos avis, autorisations et recommandations), and PUBLICATION (Les publications de Commission vie privée). The main content area is titled 'La notification de fuites de données' and contains a quote: 'Lorsque des données à caractère personnel ont involontairement été piratées, volées ou rendues publiques d'une façon ou d'une autre, en premier lieu il est nécessaire d'en informer les personnes concernées.' Below the quote, there is a paragraph explaining the legal obligation to notify in the telecom sector and the Commission de la protection de la vie privée. At the bottom, there are two links with green arrow icons: 'NOTIFICATION D'UNE FUITE DE DONNÉES DANS LE SECTEUR TELECOM' and 'NOTIFICATION D'UNE FUITE DE DONNÉES DANS UN AUTRE SECTEUR'.

CPVP
Commission de la
protection de la vie privée

Plan du site • Lexique • FAQ • Presse • Liens • Contact •

THÈMES DE VIE PRIVÉE
Nos activités quotidiennes

LÉGISLATION ET NORMES
Textes de référence relatifs à la protection des données

DÉCISIONS
Nos avis, autorisations et recommandations

PUBLICATION
Les publications de Commission vie privée

Accueil > La notification de fuites de données

La notification de fuites de données

Lorsque des données à caractère personnel ont involontairement été piratées, volées ou rendues publiques d'une façon ou d'une autre, en premier lieu il est nécessaire d'en informer les personnes concernées.

S'il s'agit d'une fuite de données dans le secteur telecom ("violation"), il existe en outre une obligation légale de la notifier auprès de l'IBPT et de la Commission vie privée. Dans d'autres secteurs, il est opportun de notifier la fuite de données auprès de la Commission vie privée.

[NOTIFICATION D'UNE FUITE DE DONNÉES DANS LE SECTEUR TELECOM](#)

[NOTIFICATION D'UNE FUITE DE DONNÉES DANS UN AUTRE SECTEUR](#)

Obligations et droits dans le GDPR

Les obligations prévues par le GDPR

✓ Les données à caractère personnel doivent être :

1. Traitées loyalement, licitement et de manière **transparente**
2. Dans un but déterminé, explicite, légitime (et traitement ultérieur compatible);
3. Adéquates, pertinentes **et limitées à ce qui est nécessaire par rapport aux finalités**
4. Exactes et mises à jour;
5. Conservées pour une durée non excessive par rapport au but défini;

+ consentement/nécessaire à l'exécution d'un contrat/obligation légale/etc...

✓ Les obligations du responsable du traitement :

1. **Registre des activités de traitement** (qui remplace la ~~déclaration~~ à la CPVP);
2. Information;
3. **Obligation de sécurité renforcée**
4. **Obligation d'analyse d'impact**
5. **Désigner un délégué à la protection des données**
6. Accountability;
7. Privacy by design/ by default.

✓ Droits de la personne concernée: accès, rectification, opposition + **droit à l'oubli, droit à la limitation, droit à la portabilité**

GDPR: Le registre d'activités de traitements (1)

- ✓ Ce registre sous une forme écrite (y compris électronique) comporte:
- 1. le nom et les coordonnées du responsable du traitement et du délégué à la protection des données;
- 2. les finalités du traitement;
- 3. une description des catégories de personnes concernées et des catégories de données à caractère personnel;
- 4. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;
- 5. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées;
- 6. dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
- 7. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles

GDPR: Le registre d'activités de traitements (2)

- ✓ L'obligation de tenir un registre d'activités de traitements ne s'applique pas aux entreprises comptant moins de 250 employés,
 - sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel
 - ou s'il porte notamment sur les catégories particulières de données sensibles.

Obligation de sécurité dans le GDPR (1)

- ✓ **Obligation de mettre** en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un **niveau de sécurité adapté au risque** compte tenu de:
 - 1) **l'état des connaissances**;
 - 2) des **coûts** de mise en œuvre;
 - 3) la **nature**, la **portée**, le **contexte** et les **finalités** du traitement;
 - 4) ainsi que les **risques**, dont le **degré de probabilité et de gravité varie**, pour les droits et libertés des personnes physiques.

- ✓ **Y compris entre autres, selon les besoins, en ayant recours à :**
 - a) la **pseudonymisation et le chiffrement** des données à caractère personnel;
 - b) des **moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience** constantes des systèmes et des services de traitement;
 - c) des **moyens permettant de rétablir la disponibilité** des données à caractère personnel **et l'accès** à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
 - d) une **procédure visant à tester, à analyser et à évaluer** régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement .

Obligation de sécurité dans le GDPR (2)

- ✓ L'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect des exigences de sécurité
- ✓ Mais attention !
 - Les codes de conduites élaborés par les associations et autres organismes représentant des catégories de responsables du traitements ou de sous-traitants doivent être soumis à la CPVP et approuvés par celle-ci.
 - Les certifications doivent être délivrées par des organismes de certification agréés:
 - par la CPVP ou
 - par BELAC (l'organisme d'accréditation belge), conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par la CPVP.

- ✓ Lorsqu'un type de traitement est **susceptible d'engendrer un risque élevé**, le responsable du traitement effectue, avant le traitement, **une analyse d'impact**.
- ✓ Analyse d'impact **obligatoire si**:
 - **évaluation systématique et approfondie d'aspects personnels**, y compris le profilage;
 - **le traitement à grande échelle de données sensibles**;
 - **la surveillance systématique à grande échelle d'une zone accessible au public**.
- ✓ L'analyse d'impact **contient au moins**:
 1. **une description systématique des opérations de traitement envisagées et des finalités** du traitement,
 2. **une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités**;
 3. **une évaluation des risques**,
 4. **les mesures envisagées pour faire face aux risques**.

- ✓ **Les entreprises doivent désigner un délégué à la protection des données (« DPO ») lorsque:**
- les **activités de base** consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, **exigent un suivi régulier et systématique à grande échelle des personnes concernées**
- OU
- les **activités de base** consistent en un **traitement à grande échelle de catégories de données sensibles**

- ✓ Missions du délégué à la protection des données:
 - informer et conseiller sur les obligations en matière de protection des données;
 - contrôler le respect des dispositions matière de protection des données, y compris ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;
 - dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci
 - coopérer avec la CPVP;
 - faire office de point de contact pour la CPVP.

GDPR: le délégué à la protection des données (3)

- ✓ Le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui sont confiées.
- ✓ Le DPO doit avoir les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement.
- ✓ Le DPO ne reçoit aucune instruction en ce qui concerne l'exercice des missions.
- ✓ Le DPO peut exécuter d'autres missions et tâches si celles-ci n'entraînent pas de conflit d'intérêts.
- ✓ Le DPO est soumis au secret professionnel ou à une obligation de confidentialité.

GDPR :

Notification auprès de la CPVP

Procédure

- notification effectuée par le responsable du traitement de données
- dans les meilleurs délais, si possible 72h à partir de la connaissance sinon après 72h, nécessité de motiver le retard
- sous-traitant doit notifier sans-délais au responsable du traitement.

SAUF dans une situation :

- pas de risque pour les droits et libertés des personnes physiques

QUOI ?

- nature de la violation des données
- catégories-nombres de personnes/enregistrement concernés
- nom et des coordonnées du délégués à la protection des données
- description des conséquences probables
- description des mesures prises/à prendre afin de minimiser les aspects négatifs

GDPR :

Notification auprès de la personne concernée

Procédure:

- notification effectuée par le **responsable du traitement de données**
- dans les **meilleurs délais**
- si susceptible d'engendrer un **risque élevé** pour les droits et libertés d'une personne physique

SAUF dans trois **situations** (constatées par la CPVP):

- mesures de protection techniques et organisationnelles appropriées ont été appliquées → **données incompréhensibles** (ex : chiffrement)
- mesures ultérieures qui garantissent que le **risque élevé n'est plus susceptible de se matérialiser**
- exigerait des **efforts disproportionnés** → communication publique

✓ GDPR:

- **Responsabilité civile** : Toute personne ayant subi un **dommage matériel ou moral** du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi
- **Responsabilité pénale** : augmentation du montant des amendes « administratives » : **10,000,000 EUR ou 2% du chiffre d'affaires** annuel global réalisé par l'entreprise (le + élevé est retenu)

Franck Dumortier
Chercheur
Centre de Recherche Information, Droit et Société (CRIDS)
franck.dumortier@unamur.be
www.crids.eu