

Colloque Spécial Bruxelles 2017

■ **Règlementation Générale des Données sur la Vie Privée**

Madame Valérie VERBRUGGEN, Conseiller Juridique



Règlement général sur la protection des données à caractère personnel (RGPD)



Secrétariat de la CPVP
Valérie Verbruggen

Attractions & Tourisme
(Bruxelles)

6 décembre 2017

CBPL
Commissie voor de bescherming
van de persoonlijke levenssfeer

CPVP
Commission de la
protection de la vie privée

ASP
Russschuss für den
Schutz des Privatlebens

CPP
Commission for the
protection of privacy

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

https://www.privacycommission.be/fr/la-loi-vie-privee-et-ses-arretes-d-execution

La Loi vie privée et ses arrêtés d'exécution

La Loi vie privée

La Loi vie privée a pour objectif de protéger le citoyen contre l'utilisation abusive de ses données personnelles. Elle décrit aussi bien les droits et les obligations de la personne dont les données sont traitées que les droits et obligations de celle qui les traite.

[VOIR LOI VIE PRIVÉE](#)

Arrêtés d'exécution de la Loi vie privée

Le premier arrêté royal d'exécution de la Loi vie privée date de 2001, suite à l'adaptation de la Loi vie privée à la Directive européenne 95/46/EG. En 2003, un deuxième arrêté d'exécution a établi le mode de fonctionnement des comités sectoriels.

[VOIR ARRÊTÉ ROYAL 13/02/2001](#)

[VOIR ARRÊTÉ ROYAL 17/12/2003](#)

top

Au niveau national	Au niveau européen	Au niveau international
<ul style="list-style-type: none">La Loi vie privée et ses arrêtés d'exécutionLa législation des comités sectoriels	<ul style="list-style-type: none">Union européenneConseil de l'Europe	<ul style="list-style-type: none">Normes internationalesLignes directrices de l'OCDEISONations Unies

https://www.privacycommission.be/fr/node/3810

FRA 10:54

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN Documents - European Commi... eur-lex.europa.eu

File Edit Go to Favorites Help

dms Free Hotmail Web Slice Gallery Webtop

4.5.2016 FR Journal officiel de l'Union européenne L 119/1

I
(Actes législatifs)

RÈGLEMENTS

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

FRA 14:29

25 mai 2018: RGPD d'application

The screenshot shows the homepage of the CPVP (Commission de la protection de la vie privée) website. The browser address bar displays <https://www.privacycommission.be/fr>. The page features a navigation menu with links for 'Plan du site', 'Lexique', 'FAQ', 'Presse', 'Liens', and 'Contact'. The main header includes the CPVP logo and a statement: 'La Commission vie privée veille à ce que les données à caractère personnel soient utilisées et sécurisées soigneusement, et que votre vie privée future soit également garantie.' Below this, a large blue banner highlights the 'RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES' with a digital countdown timer showing 602022226 seconds remaining. To the right, two posters for '13 ÉTAPES' are displayed. A green box on the right side of the banner promotes a 'Nouveau dossier thématique et plan par étapes RGPD'. The footer contains five main sections: 'THÈMES DE VIE PRIVÉE', 'LÉGISLATION ET NORMES', 'DÉCISIONS', 'PUBLICATIONS', and 'À PROPOS DE LA CPVP', each with a brief description. A search bar is located on the right side of the footer. The Windows taskbar at the bottom shows the system tray with the date 'FRA 21:37'.

https://www.privacycommission.be/fr

Commission vie privée

File Edit View Favorites Tools Help

dms Free Hotmail Web Slice Gallery Webtop

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

NL • EN • FR

CPVP
Commission de la
protection de la vie privée

La Commission vie privée veille à ce que les données à caractère personnel soient utilisées et sécurisées soigneusement, et que votre vie privée future soit également garantie.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

6 0 2 0 2 2 2 2 6
DAYS HOURS MINUTES SECONDS

➤ [Plus d'informations](#)

PRÉPAREZ-VOUS EN 13 ÉTAPES

BEREID UZ VOOR IN 13 STAPPEN

Nouveau dossier thématique et plan par étapes RGPD

La Commission vie privée lance un nouveau dossier thématique sur le Règlement général sur la protection des données ainsi qu'un plan en 13 étapes.

➤ [Consultez nos autres thèmes du mois](#)

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

PUBLICATIONS
Les publications de la Commission vie privée

À PROPOS DE LA CPVP
Pour en savoir plus sur la Commission vie privée

🔍 🔍

Windows taskbar: FRA 21:37

<https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees>

https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees

Règlement Général sur la Protection des Données

JE SUIS UN RESPONSABLE DU TRAITEMENT

Je suis considéré comme un responsable du traitement si c'est moi qui détermine les finalités et les moyens du traitement de données à caractère personnel.

JE SUIS UN SOUS-TRAITANT

Je suis considéré comme un sous-traitant dès que je traite des données à caractère personnel pour le compte d'un responsable du traitement.

Introduction - principe

- *AU SECTEUR PUBLIC*

- *Et*

- *AU SECTEUR PRIVE*

= situation actuelle

Champ d'application matériel (art. 2)

Le RGPD s'applique au

traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé des données à caractère personnel contenues ou appelées à figurer dans un fichier

Application territoriale (Art. 3 RGPD)

RT / ST établis dans l'UE

- Peu importe où a lieu le traitement, que ce soit dans l'Union ou non



RT /ST non établis dans l'UE

- PC sont dans l'UE
- Les traitements concernent
 - Une offre de biens et de services aux PC
 - Le suivi de leur comportement, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE

Le responsable de traitement

- « *Soit la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui seul **ou conjointement** avec d'autres, détermine les finalités et les moyens du traitement* » (RGPD – art. 4.7.): **pouvoir décisionnel**
- **Secteur privé et secteur public visés**
 - Personne physique – particulier: exception domestique dans certains cas (voir supra)
- Les co-responsables (art. 26): accord, point de contact et transparence

Définition

*Donnée à caractère personnel
(donnée personnelle): toute
information se rapportant à une
personne physique, identifiée ou
identifiable (= la personne
concernée)*

Origine raciale ou ethnique

Données génétiques

Données biométriques

Opinions politiques

Données concernant la santé

Convictions religieuses ou philosophiques

Vie sexuelle

Appartenance syndicale

Orientation sexuelle



Licéité, Loyauté
et Transparence

FINALITE

EXACTITUDE

PERTINENCE
(minimisation)



LIMITER LA
CONSERVATION

Base légale

SECURITE

Accountability

Bases de légitimité du traitement (Art. 6 RGPD)



- Consentement
- Contrat
- Obligation légale
- Intérêt vital
- Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique
- Intérêt légitime poursuivi par le RT ou par un tiers

Consentement (art. 7 RGPD)



La PC a consenti
au traitement
pour une ou
plusieurs finalités
spécifiques

- Libre
- Spécifique
- Informé
- Non ambigu / univoque
(Acte positif, manifestation claire)

- Preuve par le RT
- Droit de retrait du consentement à tout moment
(sans affecter les traitements opérés avant ce retrait)

Principe de responsabilité / Accountability



- Le responsable de traitement est **responsable du respect des principes** applicables à tout traitement (voy. ci-dessus)
 - LVP: art. 4
 - RGPD: art. 5.2.
- ET est en mesure de **démontrer que ceux-ci sont respectés** (RGPD: art. 5.2.)



Approche par le risque



*Obligations des responsables de traitement (RT) et sous-traitants (ST)**

Désigner un
représentant*

Privacy by design
et by default

Sécurité
notification des
failles de sécurité*

Analyse d'impact
(DPIA) / consultation
préalable

Registre des
activités de
traitement*

Délégué à la
protection des
données (DPO)*



Sous-traitant
(ultérieur)*

Suppression de la déclaration préalable (art.17 LVP)



https://elokit.privacycommission.be/elg/main.htm?siteLanguage=fr

File Edit View Favorites Tools Help

dms Free Hotmail Web Slice Gallery Webtop

Aide Home nl fr de

CPVP
Commission de la
protection de la vie privée

Compléter une nouvelle déclaration

Compléter une nouvelle déclaration thématique d'une caméra de surveillance

Gestion de déclaration

Introduire une nouvelle déclaration de traitement

Vous êtes le responsable du traitement et vous souhaitez

- Compléter une déclaration ordinaire
- Compléter une déclaration VIA/DPR

Vous êtes le responsable du codage des données à caractère personnel et vous souhaitez

- Compléter une déclaration pour un nouveau codage des données à caractère personnel à des fins historiques, statistiques ou scientifiques

Vous êtes le responsable du traitement ultérieur de données à caractère personnel et vous souhaitez

- Compléter une nouvelle déclaration de traitement ultérieur de données codées à des fins historiques, statistiques ou scientifiques
- Compléter une nouvelle déclaration de traitement ultérieur de données non-codées à des fins historiques, statistiques ou scientifiques

La finalité et les moyens sont déterminés par un seul responsable

La finalité et les moyens sont déterminés conjointement par plusieurs personnes, associations de fait, etc., au nom desquelles la déclaration est complétée

Compléter une déclaration

Les données à caractère personnel qui sont collectées dans le cadre de l'application de la déclaration servent uniquement à exécuter les obligations légales de la Commission concernant le Registre public des traitements (traitement interne de votre formulaire, publication de la déclaration au Registre public sur Internet). Vos données à caractère personnel ne seront utilisées pour aucune autre finalité.

FRA 21:38

MAIS: registre interne de traitements (RT – ST) et transparence PC (information, registres spécifiques (CEPD)

Registre des traitements

Chaque responsable de traitement tient un registre des activités de traitement effectuées sous sa responsabilité

Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement

Les registres se présentent sous une forme écrite y compris la forme électronique. Ils sont tenus à la disposition de la CPVP à première demande

Seules exceptions pour les PME (sauf exceptions)



Rubrique GDPR

Modèle de Registre des activités de traitement

Téléchargement

» [Modèle de Registre des activités de traitement](#)



Recommandation n° 06/2017 du 14 juin 2017

Objet: Recommandation relative au Registre des activités de traitements (article 30 du RGPD)
(CO-AR-2017-011)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après LVP), en particulier l'article 30 ;

Vu le rapport de Monsieur Willem Debeuckelaere;

Émet, le 14 juin 2017, la recommandation suivante:

La Commission vie privée met à disposition un modèle de Registre destiné aux responsables de traitements afin d'aider les entreprises et organismes à établir un Registre des activités de traitement.

Comment compléter le Registre ?

Le modèle de registre que nous proposons contient plus d'informations que ce que le RGPD ne requiert. Ce modèle de Registre doit donc être considéré comme un réel outil car il permet à l'utilisateur de garder une vue d'ensemble sur d'autres informations qui ont également une importance à la lumière de l'application du RGPD.

- Les informations qui doivent absolument figurer dans le Registre, telles que le RGPD le prévoit, sont marquées en rouge. En supprimant les autres colonnes et en ne maintenant donc que les champs marqués en rouge, vous obtiendrez un Registre contenant le minimum d'informations requises par le RGPD.
- Le modèle de Registre permet d'établir un historique concernant le traitement des données en y complétant les champs « date de fin du traitement » et « traitement alternatif » sous la rubrique « statut ». Ceci peut s'avérer utile afin d'obtenir un aperçu des aspects importants des traitements qu'une organisation a opérés antérieurement.
- Le modèle de Registre est composé de 5 onglets :



Un outil interne de
l'accountability:
cartographie des
traitements



Une source
d'information pour
l'autorité de contrôle

Application dans le temps




Le Registre devra,
à partir du 25 mai 2018,
contenir les éléments d'information
ci-après
au regard des
traitements opérés à cette date,
qu'ils soient opérés de longue date
ou nouveaux.

?? Dois-je conserver les informations dans le Registre une fois que le traitement a cessé ?

Infos relatives aux traitements opérés

(pas un relevé des données à caractère personnel en tant que telles)





Quelles informations dans le Registre
du responsable de traitement (RT) ?

Qui ?



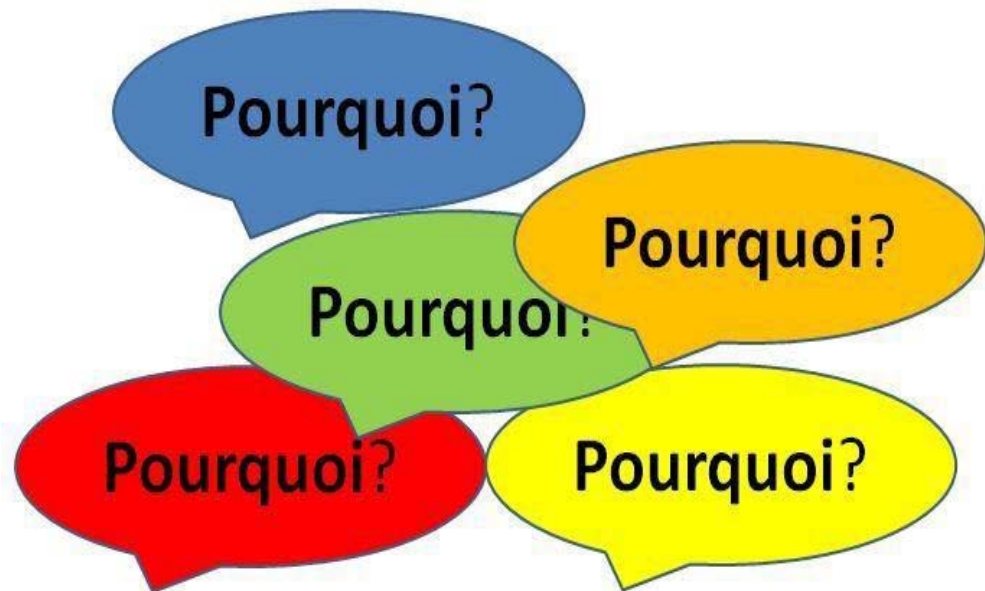
Le responsable de traitement (art. 4.7.)

Le co-responsable de traitement (art.26)

Le représentant si RT hors UE (art. 27)

(Registre accessible)

Le délégué à la
protection des données (art. 37-39 DPO)



Pourquoi ?

Les finalités des traitements

- Claire et précise
- Formulation générale (quelle granularité ?)
- Complétée par un descriptif plus précis

Quoi?

Mention
des catégories de
Personnes
concernées et
des catégories de
Données
au regard de chaque
finalité

- Finalité A
- Finalité B ...
- Finalité C ...



Exemples de catégories de données

- Issus de la notice explicative à la déclaration

91	Liste indicative des catégories de données fonctionnelles
92	Catégorie de données fonctionnelle
93	Données d'identification
	Données d'identification personnelles
94	
	Données d'identification émises par les services publics, autres que le numéro de registre national
95	
96	Données d'identification électroniques
97	Données d'identification électroniques
	Données d'identification biométriques
98	
99	Particularités financières
	Données d'identification financières
100	
	Moyens financiers
101	
102	Dettes, dépenses
103	Solvabilité
	Emprunts, hypothèques et crédits
104	
105	Aide financière
	Détails relatifs aux assurances
...	

- Catégories particulières de données (art. 9 et 10 RGPD)



Non obligatoire



Où les données sont-elles localisées ? Transférées

Identification du pays tiers, garanties le cas
échéant (art. 49 § 1 alinéa 2) ?

Règles relatives aux flux transfrontières de données (hors UE / EEE)





Jusqu'à quand
les données sont – elles conservées ?
(mention des délais
pour l'effacement des données)



Comment
les données
sont-elles
sécurisées ?

**Mesures de référence en matière de sécurité applicables à tout traitement
de données à caractère personnel¹**

Version 1.0

Le présent document reprend une liste d'onze domaines d'actions liées à la sécurité de l'information pour lesquels tout organisme - personne morale², entreprise ou administration - qui conserve, traite ou communique des données à caractère personnel doit prendre des mesures.

Vu l'extrême diversité des situations concrètes rencontrées, il n'est pas possible de définir précisément les actions à entreprendre pour chaque cas.

[https://www.privacycommission.be/sites/privacycommission/files/documents/mesures de reference en matiere de securite applicables a tout traitement de donnees a caractere p ersonnel 0.pdf](https://www.privacycommission.be/sites/privacycommission/files/documents/mesures%20de%20reference%20en%20matiere%20de%20securite%20applicables%20a%20tout%20traitement%20de%20donnees%20a%20caractere%20p%20ersonnel%200.pdf)

Quelles informations dans le Registre du sous-traitant (ST)



Qui ? Nom et coordonnées du ST, de chaque RT pour lequel il opère; le cas échéant du représentant et du DPO

Quoi ? Les catégories de traitements effectués pour le compte de chaque RT

Où ? Les transferts vers des destinataires tiers à l'UE, quels pays et le cas échéant avec quelles garanties ?

Quelle sécurité ? Description générale des mesures techniques et organisationnelles

Data Protection Impact Assessment
Analyse d'impact
(DPIA)



Data Protection Impact Assessment (DPIA)

Obligation

- Lorsqu'un type de traitement est susceptible d'engendrer un **RISQUE ELEVE** pour les droits et libertés des personnes, le responsable de traitement effectuera, avant le traitement, une analyse d'impact.

Contenu

- Description des traitements et finalités
- Nécessité et proportionnalité des opérations de traitement
- Evaluation des risques pour les droits et libertés des personnes concernées
- Les mesures envisagées pour faire face aux risques

Cas obligatoires

- Evaluation systématique et approfondie d'aspects personnel fondée sur un traitement automatisé - profilage
- Traitements à grande échelle de catégories particulières de données ou judiciaires
- Surveillance systématique à grande échelle d'une zone accessible au public



Délégué à la protection des données (DPO)



Obligatoire

• **Autorité ou organisme public**

• Activités de base du RT ou ST consistent en des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées

• Activités de base du RT et ST consistent en des traitements à grande échelle de données sensibles s.l.

Droit national

• *Cas obligatoires supplémentaires*

Qui désigner ?



Designation

- **Interne** (membre du personnel – 37.6)
- **Externe** (contrat de service 37.6.)
 - Un pour plusieurs RT et ST (groupe d'entreprises – PME – 37.2.)
 - Un pour plusieurs autorités publiques ou organismes publics (37.3.)
- **Compétence et qualités requises (37.5):**
 - Connaissances spécialisées du **droit et des pratiques en protection des données** et capacité à exercer ses missions
- Personne **physique** et/ou personne **morale** ?

« Fonction » du délégué (art. 38)

INDEPENDENT



Position

- **Etre indépendant**
- Ne pas recevoir d'instruction en ce qui concerne l'exercice de ses missions (38.3.)
- Ne pas être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions (38.3.)
- Faire rapport directement au niveau le plus élevé de la direction (38.3.)
- Etre soumis au secret professionnel ou à une obligation de confidentialité (38.5.)
- Ne pas avoir de conflit d'intérêt (38.6.)

« Fonction » du délégué (art. 38)




- **Etre en mesure d'exercer effectivement ses missions**
- Etre associé de manière appropriée et en temps utile à toutes les questions relatives à la protection des données (38.1.)
- Bénéficiaire des ressources nécessaires (38.2.)
- Accéder aux données et opérations de traitement (38.2.)
- Entretenir sa formation spécialisée (38.2.)
- Durée minimale ?

« Fonction » du délégué (art. 38)



- **Etre accessible**
- « Facilement **joignable** au départ de chaque établissement » : ~~localisation~~ (37.2.)
- Connu de la **DPA**: obligation de notification des coordonnées du DPO (37.7.)
- Connu des **personnes concernées (PC)**
 - Publication des **coordonnées** du DPO (37.7.)
 - Droit à l'information de la PC (13.1.b) et 14.1.b))
- Connu **en interne**

Délégué à la protection des données (DPO)

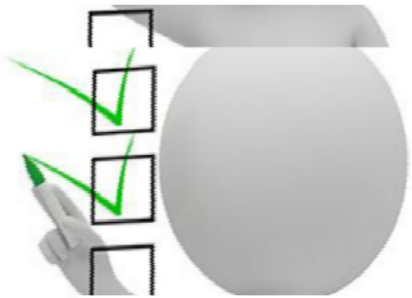


Informer et conseiller le RT et le ST ainsi que les employés sur les obligations qui leur incombent en application du RGPD et autres dispositions en matière de protection des données

Contrôle le respect du RGPD

Dispense des conseils, sur demande, en ce qui concerne le DPIA

Fait office de point de contact sur les questions relatives aux traitements, y compris la consultation préalable



Missions

Sécurité (article 32)

Par qui?

- Responsable de traitement ET sous-traitant

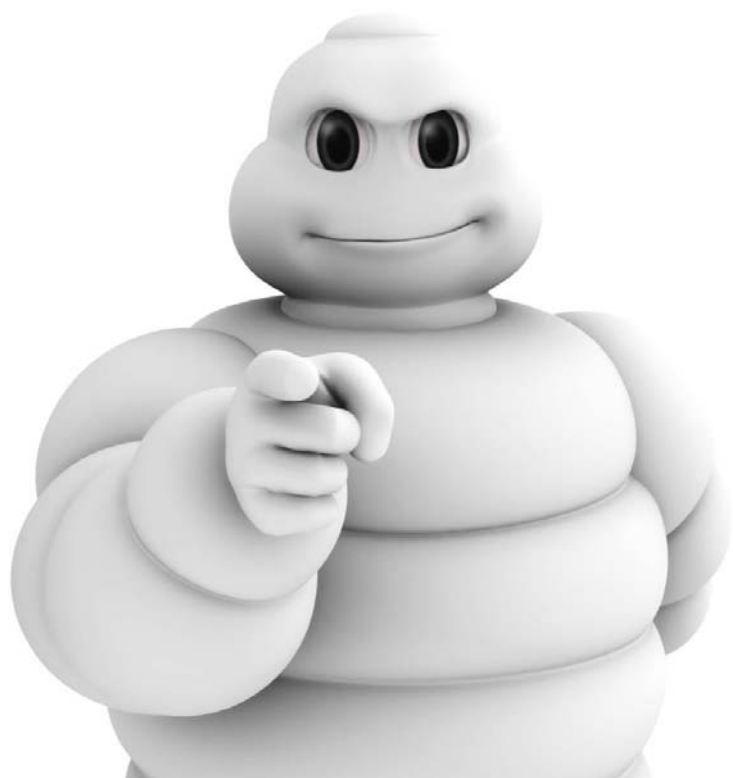
Quoi?

- Paramètres: coût, état de l'art, contexte, finalité, volume, nature des données et du traitement, risques
- Mesures techniques et organisationnelles pour un niveau de sécurité adapté

Comment?

- Conséquences de la perte, de l'altération, de l'accès non autorisé ...

Notification des violations de données



Notification

À la DPA
(CPVP)
(Art. 33)

Aux
personnes
concernées
(Art. 34)

Communication

Notification des violations de données à la DPA

72 heures au plus tard après en avoir pris connaissance à moins que la violation ne soit PAS susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Le sous-traitant notifie au responsable de traitement toute violation de données dans les meilleurs délais

La notification a un contenu minimum

Toute violation doit être documentée

Communication de la violation à la personne concernée



EXCEPTIONS

Lorsqu'une violation est susceptible d'engendrer un **risque élevé** pour les droits et libertés d'une personne physique, le responsable de traitement communique la violation à la **personne concernée**



La communication décrira de manière claire la nature de la violation et a un contenu minimum



Si le responsable de traitement n'a pas communiqué à la personne concernée, la CPVP peut lui ordonner de le faire

Relation entre le RT et le ST

CONTRAT



FAIRE LE BON CHOIX

Le choix du sous-traitant (art. 28)



Faire le bon choix: Appel aux seuls sous-traitants qui présentent des garanties suffisantes quant à la mise en oeuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du Règlement



Contrat exigé: : le traitement par le ST est régi par un contrat ou un autre acte juridique qui lie le ST au RT (voir infra pour le contenu)

New: la sous-traitance ultérieure (art. 28.2.)

- Contrôle du responsable de traitement:
 - Autorisation écrite préalable, spécifique ou générale, du responsable de traitement pour tout recours par le ST à un autre sous-traitant
 - Si accord général, le ST informe le RT de tout changement et ajout de ST, donnant ainsi la possibilité au RT de s'y opposer
- Contrat:
 - En cas de sous-traitance ultérieure, les mêmes obligations que celles du contrat entre RT et ST initial sont imposées à cet autre ST (ultérieur)
- Responsabilité:
 - Lorsque cet autre ST ne remplit pas ses obligations, le ST initial demeure pleinement responsable devant le RT de l'exécution par cet autre ST de ses obligations



Contenu du contrat de sous-traitance

Contenu de base

- Objet du contrat
- Durée
- Nature et finalité du traitement
- Type de données
- Catégories de personnes concernées
- Obligations et droits du RT



Devoirs du sous-traitant

- Respect des instructions
- Prise de mesures de sécurité (art. 32)
- Confidentialité imposée
- Respect des conditions de la sous-traitance ultérieure
- Aide le RT pour l'exercice effectif des droits des PC
- Aide le RT dans le respect de la notification des data breach et DPIA
- Supprime ou renvoie les données au RT au terme de ses prestations, détruit les éventuelles copies
- Met à disposition du responsable de traitement toutes infos pour preuve du respect du Règlement et permettre la réalisation d'audits

Loi Vie privée (art. 16)

Contenu de base

- Subject matter
- Duration
- Nature and purpose of the processing
- Type of data
- Categories of data subject
- Obligations and right of controller



Devoirs du sous-traitant

- Respect des instructions
- Prise des mesures de sécurité (art. 32)
- Ensure that workers are subject to confidentiality
- Respect sub-processing GDPR rules
- Assist the Controller when exercise of DS's rights
- Assist the Controller to ensure compliance (TM, Breach notif., PIA, prior consultation)
- Delete, destroy or return data to Controller at the end and delete existing copies
- Make available to Controller any necessary information to demonstrate compliance

+ fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement

Contrat avec le sous-traitant

Trop compliqué?



Possibilité de modèles européens



Droits des personnes concernées (PC)

- Modalités générales
- Information et accès aux données
- Rectification et effacement
- Droit à la portabilité des données
- Droit d'opposition
- Droit de ne pas être soumis à une décision automatisée/profilage

Recours, responsabilité et sanctions (Chap. VIII)

- Recours
- Représentation des personnes concernées
- Responsabilité
- Sanctions administratives

Contenu de l'info?



Information de base

- Obligatoire dans tous les cas

Information complémentaire

- Nécessaire pour assurer un traitement loyal et transparent

Informations de base obligatoires

Collecte directe

Collecte indirecte

Les finalités du traitement ainsi que les bases de légitimité

L'identité et les coordonnées du RT, de son représentant et du DPO le cas échéant

Lorsque le traitement est basé sur l'intérêt légitime du responsable de traitement, quel est-il

Les catégories de données traitées

Le cas échéant, les destinataires ou catégories de destinataires des données

En cas de transfert de données à l'étranger, l'existence ou non d'une décision d'adéquation ou les garanties appropriées mises en place et la manière dont on peut en obtenir une copie.

Information additionnelle éventuelle

Collecte directe

Collecte indirecte

La durée de conservation des données ou, si impossible, les critères de détermination de cette période

Lorsque le traitement est basé sur l'intérêt légitime du responsable de traitement, quel est-il

La possibilité d'exercer ses droits auprès du RT: droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition et de portabilité

Le droit de retirer son consentement à tout moment lorsque le traitement est fondé sur celui-ci

Le droit d'introduire une plainte auprès de l'autorité de contrôle

L'origine des données (source) et si possible, si cela provient d'une source publiquement accessible ou non

L'existence de décision automatisée, en ce compris le profilage, les informations utiles concernant la logique qui sous-tend ce traitement et l'importance et les conséquences pour la personne

Les autorités de contrôle

Missions harmonisées (Art. 57.1)

Contrôle l'application du GDPR

Sensibilise le public, Encourage les codes de conduite et la certification, Opère une veille technologique

Conseille (avis), Informe et Traite des plaintes

Encadre les flux transfrontières

(Co) régule: Data Protection Impact Assessment (DPIA), critères de certification, d'accréditation, et **Agrée/Accrédite**

Coopère avec les autres autorités de contrôle (e.a. investigations conjointes) et avec le Comité européen (CEPD)



Pouvoirs d'enquête (58.1)

- Ordonne de communiquer toute info
- Mène des enquêtes / audit
- Accède à toutes données et informations nécessaires
- Accède à tous les locaux , à toute installation et tout moyen de traitement

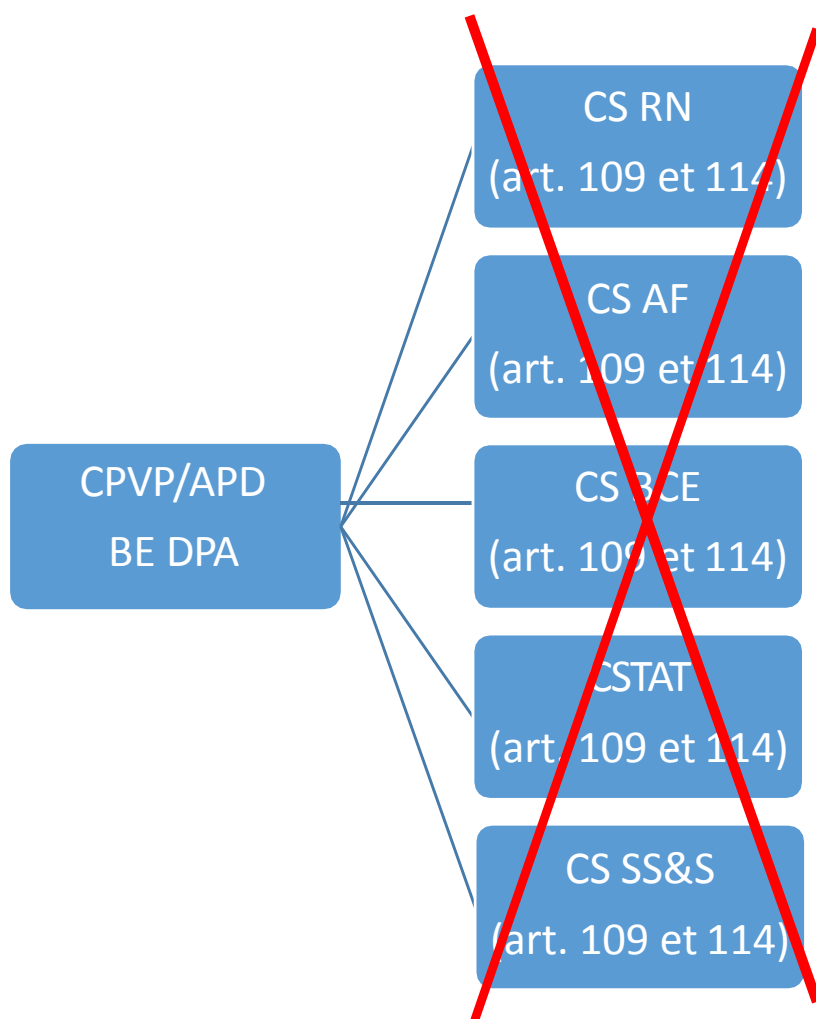
- Conseille / consultation
- Emet des avis
- Autorise préalablement des traitements (droit national)
- Avis et approbation des codes de conduite
- (Agrée les organismes de certification)
- Approuve critères de certification et certifie
- Adopte des clauses type de protection des données
- Autorise les clauses contractuelles (ad hoc)
- Approuve les BCRs



Pouvoirs correctifs (58.2)

- Adresse avertissement au RT ou du ST
- Rappel à l'ordre
- Ordonne de satisfaire aux demandes des PC (droits)
- Ordonne la mise en conformité
- Ordonne la communication d'un data breach aux PC
- Impose une limitation temporaire ou définitive, y compris une interdiction de traitement
- Ordonne la rectification, l'effacement ou la limitation de données
- Retire une certification ou ordonne à l'organisme de certification de le faire
- Impose des sanctions administratives
- Ordonne la suspension des flux

Nouveau paysage



Conseil de réflexion
indépendant
(art. 35)

Vlaamse Toezicht Commissie
Commission bruxelloise
Commission wallonne d'échange
des données

Organe de contrôle
de l'information policière (COC)
(art. 4 § 2 al.3)

Autorité de protection des données (17)

Service de 1ere ligne

(Sensibilisation
Information,
Médiation)

Secrétariat général

(Tâches
horizontales
d'appui – Tâches
exécutives)

Centre de connaissances

(Avis et
recommandations)

Service d'inspection

(Enquêtes)

Chambre contentieuse

(Contentieux
administratif)

Directeur

Directeur

Présidence de
l'APD (3 ans)

Directeur

(+ 6 membres)
Présidence de l'APD
(3 ans)

**Inspecteur
général**

Président

(+ 6 membres)

Comité de direction (5)

Les conditions pour être membre de l'APD



Compétence

- Compétence et expérience en matière de protection des données (APD)
- Indépendance
- Autorité morale
- Connaissance des langues: FR, NL, DE et ENG
- Equilibre linguistique et de genre

Durée - Indépendance

- Mandat de 6 ans renouvelable 1X
- Incompatibilités: membre d'un parlement , d'un exécutif, d'une cellule stratégique ministérielle, d'une fonction publique
- Indépendance dans l'exercice de leur fonction: conflit d'intérêt, démission

