Actualités des pensions dans le secteur public

Jeudi 26 avril 2018

Le Règlement Général européen de Protection des Données (RGPD) : quel est son impact?

IFE by ABILWAYS

Nicolas Roland
Avocat-associé

blog.commyounity.be

younity AVOCATS | ADVOCATEN | LAWYERS

Programme

1. Pourquoi ce règlement?
2. Qu’est-ce qui change?
3. De quoi parle-t-on?
4. De qui parle-t-on?
5. Pourquoi est-ce important pour vous?
6. A quoi devez-vous faire attention pendant la carrière de votre agent ?
7. Et maintenant, comment procéder?

1. Pourquoi ce règlement?

- Nécessité de s'adapter à l'ère digitale (>< directive de 1995)
- Sanctions actuelles pas suffisamment efficaces
- Nécessité d'une harmonisation renforcée

Mais….

- Interprétation nationale par les instances nationales en matière de vie privée
- Nombreuses questions/thématiques qui sont gardées ouvertes pour les États membres et qui permettent encore la conclusion d'accords nationaux spécifiques jusqu'à un certain point

Illustrations: règles *« plus spécifiques »* pour les relations de travail (art. 88), numéro de registre national en Belgique et « mort numérique » en France

2. Qu'est-ce qui change?

- Continuation des éléments et principes essentiels qui s'appliquent aujourd'hui déjà dans la législation existante, mais également tout un nombre de concepts ajoutés et de modifications :

  - Importante mise à jour (p. ex. consentement)

  - Impact opérationnel significatif (p. ex. le principe d'*accountability*)

3. De *quoi* parle-t-on?

champ d'application

1. Données à caractère personnel: toutes les informations relatives à une personne physique identifiée ou identifiable (« la personne concernée »), qui peut être identifiée directement ou indirectement (y compris les numéros d'identification technologiques tels qu'une adresse IP)

   Illustrations: SPRL Nicolas ROLAND? Nationalité?

2. Catégories particulières (sensibles) de données à caractère personnel: les données à caractère personnel qui sont sensibles à la discrimination et qui doivent dès lors être traitées avec encore plus de précaution *(p. ex. race ou origine ethnique, données relatives à la santé, membre d'une organisation syndicale, données biométriques)*

   Illustrations: données financières?

3. Données pseudonymisées : les données à caractère personnel qui ne peuvent plus être liées à une personne concernée spécifique sans que des données complémentaires soient utilisées (i.e. une opération d'anonymisation *réversible*) *(p. ex. des données codées)*

4. Données anonymes : les informations qui ne peuvent en aucune manière être liées à une personne physique identifiable et qui ne permettent donc aucune identification

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

4. De *qui* parle-t-on?

- D'application à toutes les « personnes » qui traitent des données à caractère personnel et
  - qui le font dans le cadre des activités d'un établissement au sein de l'UE, ou
  - qui offrent des biens et des services au sein de l'UE, ou
  - qui procèdent au suivi du comportement des personnes au sein de l'UE

/!\ en ce compris les autorités publiques /!\

Illustration: quid de la simple accessibilité d'un site Internet depuis l'UE?

- Exceptions:
  - caractère exclusivement privé par une personne physique (i.e. sans lien avec une activité professionnelle ou commerciale)
  - traitements mis en œuvre aux fins de prévention/détection des infractions pénales

5. Pourquoi est-ce important pour vous?

- Confiance
  - Pas seulement une question de conformité, mais également une exigence pour la création d'un lien de confiance avec vos agents
- Responsabilités
  - Vous êtes le « responsable du traitement » des données que vous traitez (*vous collectez les données et déterminez comment vous les gérez, et/ou c'est la loi qui détermine ces finalités et les moyens du traitement*) et/ou le « sous-traitant »
- Sanctions
  - En cas d'infractions, plusieurs sanctions possibles, notamment une interdiction de traitement ou des condamnations pénales
  - 2 catégories générales d'amendes administratives:
    - Pour les infractions essentiellement « fonctionnelles » *(p. ex. registre des activités)*: jusqu'à 10M EUR ou 2 % du chiffre d'affaires annuel mondial
    - Pour les infractions qui sont davantage liées aux droits et libertés fondamentaux des personnes *(p. ex. obtention du consentement)* : jusqu'à 20M EUR ou 4 % du chiffre d'affaires annuel mondial

6. A quoi devez-vous faire attention pendant la carrière de votre agent ?

1. A la tenue et au maintien d'un registre des activités
2. Aux bases juridiques des traitements de leurs données
3. Communication informative transparente envers les agents
4. Droits des agents
5. Obligation de notification des violations de leurs données
6. Protection de leurs données
7. Transmission à des pays 1/3
8. Délégué à la Protection des Données (DPD)
9. Sous-traitants
10. Analyse d'impact
11. Privacy « by design » & « by default »

6.1 Registre des activités

- Plus de déclaration préalable obligatoire à la Commission de la protection de la vie privée (CPVP) mais obligation de tenir un registre en ce qui concerne les données à caractère personnel que vous traitez (art. 30), en version électronique, avec notamment :
  - Les coordonnées du responsable du traitement/sous-traitant
  - Les finalités du traitement: clairement et avec précision

Illustration: « contrôle sur le lieu de travail » vs « sécurité IT »

  - Catégories de données à caractère personnel *(p. ex. les données relatives aux études et à l'emploi)*
  - Catégories de destinataires *(p. ex. la sécurité sociale)*
  - Délais de conservation visés *(p.ex. « pendant toute la durée du contrat de travail »)*
  - Mesures techniques et organisationnelles
- Recommandé d'y intégrer des informations *complémentaires* (p. ex. la mention de la base légale du traitement et le relevé de violations de données à caractère personnel)
- Même pour les organisations de < 250 personnes (!) car la gestion du personnel n'est pas un traitement « occasionnel »

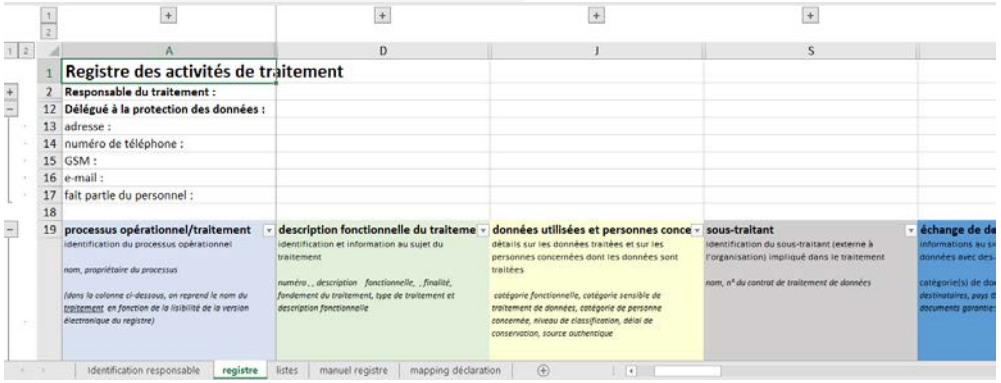
Recommandation n°06/2017 du 14 juin 2017 de la CPVP
https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf

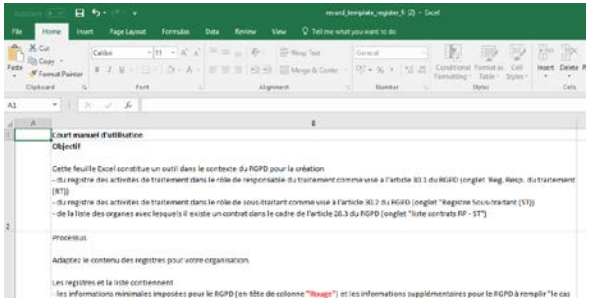
6.1 Registre des activités

- Pas « que » pour les nouveaux traitements entamés à partir de mai 2018 mais également ceux existant de longue date
- Pas destiné au public, ni à la personne concernée, mais à la CPVP
- Veillez à ce que tout ce que vous ajoutez puisse également être tenu **à jour**. Il est recommandé de **réviser** et de mettre à jour le registre au moins 1 fois par an
- Pas obligatoirement en FR, NL ou DE, mais la CPVP peut demander une traduction à vos frais
- Modèles édités par la CPVP et la Banque Carrefour de la Sécurité Sociale (BCSS):

https://www.privacycommission.be/fr/registre-des-activites-de-traitement

https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/general-data-protection-regulation





6.2 Bases juridiques des traitements

- 6 fondements juridiques que vous pouvez utiliser comme base pour justifier le traitement des données à caractère personnel d'une manière légitime :
  - Le consentement de la personne concernée
  - L'exécution d'un contrat
  - Une obligation légale
  - Les intérêts vitaux de la personne concernée
  - L'exécutiond'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
  - La réalisation d'intérêts légitimes

/!\ considérant n° 47 et article 6.1 *in fine*: pas pour les autorités publiques « *dans l'accomplissement/l'exécution de leurs missions* » /!\

- Le consentement n'est qu'un de ces fondements ; il devrait être évité le plus possible dans le contexte des RH par exemple et ne devrait servir qu'en dernier recours

Illustration: quid du consentement obtenu avant l'entrée en vigueur du RGPD?

6.2 Bases légales des traitements

- Le RGPD durcit les conditions. Chaque consentement doit :
  - Être donné librement, ce qui est très difficile dans un contexte d'emploi en raison de la relation hiérarchique
  - Spécifique et dans un langage clair et simple
  - Par un acte positif clair

  Illustration: quid de cases cochées par défaut ou d'inactivité?

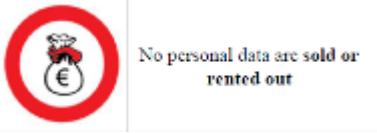
- Par ailleurs,
  - Le consentement doit pouvoir être retiré simplement à tout moment et vous devez mettre un terme au traitement s'il s'agissait du seul fondement
  - Le consentement doit être clairement distingué des autres questions

  Illustration: quid dans les conditions générales ou dans une déclaration de confidentialité faisant partie d'un logiciel?

Lignes directrices du groupe de travail article 29
https://www.privacycommission.be/sites/privacycommission/files/documents/Consentement.pdf

6.3 Communication informative transparente

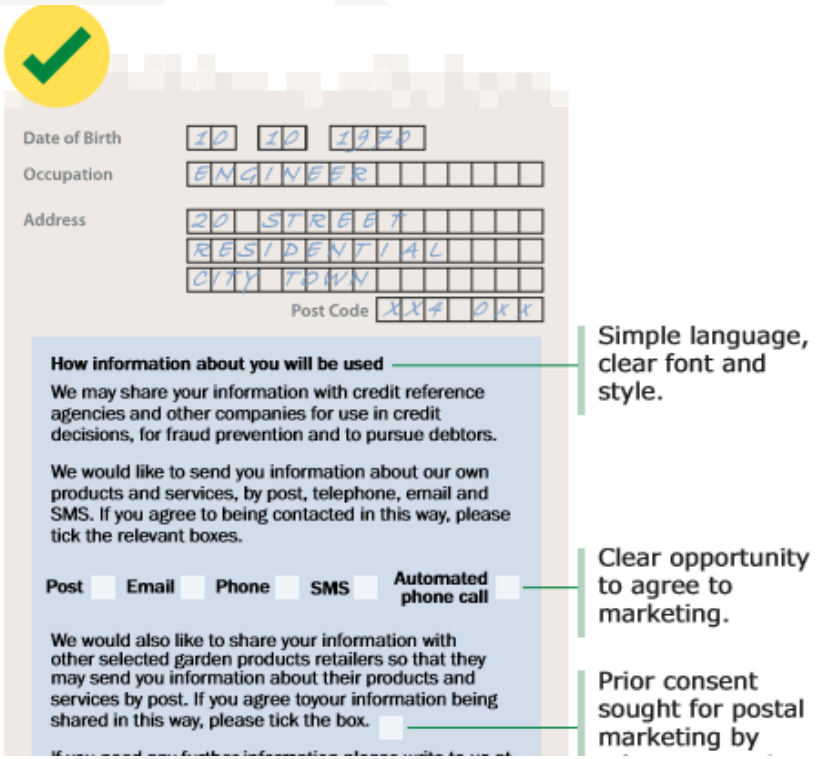
- Une obligation comparable existe déjà
- Le RGPD est plus explicite (art. 12 à 14) quant à la façon de procéder. Les informations relatives au traitement doivent être :
  - Concises
  - Facilement accessibles et compréhensibles
  - Exprimées dans un langage clair et simple et de préférence à l'aide d'une visualisation complémentaire

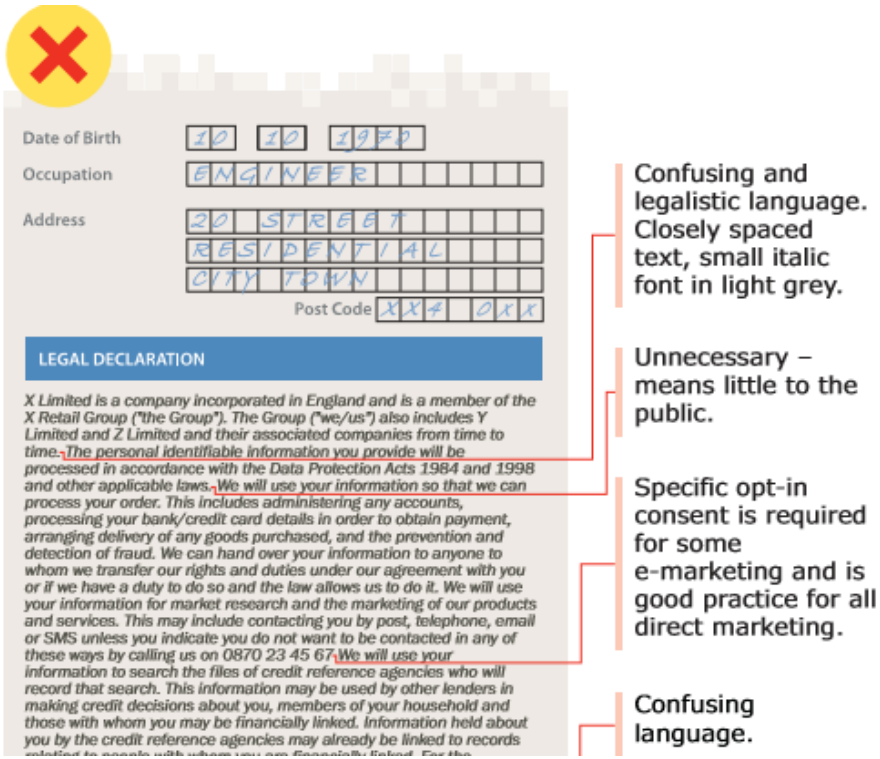


Lignes directrices du groupe de travail article 29

https://www.privacycommission.be/sites/privacycommission/files/documents/Transparency.pdf

6.3 Communication informative transparente





https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

6.4 Droits des personnes concernées

- Informations sur le **droit d'accès et de rectification**, ainsi que sur la **limitation du traitement**. Droit existant, mais nouvelles catégories obligatoires d'informations :
  - Délais de conservation

    /!\ délais de prescription applicables /!\
  - Informations sur le droit de déposer une plainte auprès de la CPVP
  - Source des données (si non obtenues auprès de la personne concernée elle-même)

    /!\ flux complexe de données en matière de pensions /!\
- Gratuit (sauf en cas de demandes répétitives ou excessives – art. 12(5))

6.4 Droits des personnes concernées

- Nouveau **droit de portabilité** pour la personne concernée principalement pour améliorer le libre choix des services en ligne (i.e. éviter tout blocage suite à la « perte » de données)
- La personne concernée peut demander d'obtenir les données qu'elle a elle-même fournies (p. ex. les relevés de compte bancaire) *« dans un format structuré, couramment utilisé et lisible par machine »* (p. ex. XML, JSON, CSV) et a le droit de transmettre ces données à un autre responsable du traitement *« lorsque cela est techniquement possible »*
- Uniquement d'application au traitement automatisé si le traitement est basé sur (i) le consentement de la personne concernée ou sur (ii) un contrat

/!\ pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement /!\

Opinion (WP242) du groupe de travail « article 29 » du 13 décembre 2016 & HR: on a case-by-case basis
https://www.privacycommission.be/sites/privacycommission/files/wp242_rev01_enpdf_Data%20portability.pdf

https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

6.4 Droits des personnes concernées

- Introduction d'un **droit à l'effacement des données** : la personne concernée a le droit de faire effacer des données si:
  - les données ne sont plus nécessaires au regard des finalités du traitement
  - la base légale du traitement est le consentement de la personne concernée qui le retire, ou
  - la personne concernée s'oppose au traitement et s'il n'existe pas de motif légitime impérieux pour sa poursuite
- Également d'application aux sous-traitants à qui vous avez transmis les données
- Pas absolu : doit être équilibré par rapport aux autres droits et obligations tels que le respect d'autres obligations légales, en vue de l'archivage dans l'intérêt général, de la recherche scientifique ou historique et des finalités statistiques
- Éléments importants dans ce cadre :
  - Délais de conservation pour d'autres obligations (comme motivation pour ne pas effacer les données)
  - Procédures pour effacer les données (aussi chez les sous-traitants)

6.5 Obligation de notification des violations

- Nouvelle obligation générale de notifier les « violations » de données à caractère personnel à la CPVP et parfois même aux personnes concernées
- Applicable de façon générale, et plus spécifique à un secteur
- Notification à la CPVP si *«risque pour les droits et libertés des personnes physiques»* (p. ex. une perte de confidentialité de données à caractère personnel protégées par le secret professionnel)
- Sans retard injustifié et au plus tard dans les **72h** après en avoir pris connaissance
- Egalement aux personnes concernées en cas de risque *élevé*, sauf

  Opinion WP248 du groupe de travail « article 29 » du 4 avril 2017

  https://www.privacycommission.be/sites/privacycommission/files/wp248_enpdf_DPIA.PDF

  - si mesures de protection techniques et organisationnelles appropriées rendant ces données incompréhensibles (p. ex. le chiffrement), ou
  - si mesures ultérieures prises garantissent que le risque élevé ne sera pas susceptible de se concrétiser, voire encore
  - si communication exigerait des « efforts disproportionnés » et que dans ce cas il sera procédé à une communication publique « ou à une mesure similaire ».
- Exigence de documenter toutes les violations, y compris les faits liés à la violation de données à caractère personnel, à ses conséquences et aux mesures de correction prises.

https://www.privacycommission.be/fr/notification-fuites-de-donnees-general

6.5 Obligation de notification des violations

- Le retard, voire l'absence, de notification peut donner lieu à uneamende
- Si vous travaillez avec dessous-traitants, il est indiqué de reprendre cette obligation dans les contrats, et ce même si le règlement leur impose une obligation directe (i.e. « *dans les meilleurs délais* »)
- Tous les collaborateurs qui traitent des données à caractère personnel doivent être conscients de l'obligation de signaler les violations le plus vite possible
- Besoin d'une procédure pour le signalement et la gestion de telles violations : vérifiez s'il existe une en interne!

6.5 Obligation de notification des violations

EQUIFAX®

YAHOO!

Orange vous informe :
rubrique mon compte

Cher(e) Client(e),

Orange a été la cible d'une intrusion informatique le 16 janvier 2014 à partir de la page « Mon Compte» de l'Espace Client du site orange.fr. Même si **aucune action de votre part n'est requise**, nous avons souhaité vous informer en toute transparence de l'existence et de la résolution de ce fait.

Vos mots de passe ne sont pas concernés, leur intégrité n'est pas mise en cause.

Cet incident a consisté en la récupération éventuelle d'un nombre limité de données personnelles vous concernant ou concernant votre foyer. Il peut s'agir des noms, prénoms, adresse postale, adresse mail de contact, numéro de téléphone (fixe ou mobile) ou des informations que vous auriez pu déclarer (composition du foyer, nombre d'abonnements Orange ou concurrents, informations concernant vos préférences de contact).

Des actions techniques, immédiatement mises en œuvre, ont mis fin à l'intrusion.

Les intrusions de ce type servent principalement au « phishing ». Cette technique consiste à se faire passer pour des organismes officiels ou des entreprises et à utiliser des informations partielles vous concernant pour tenter de récupérer auprès de vous des informations plus sensibles.

C'est pourquoi **nous vous invitons à la plus grande prudence en cas de sollicitation douteuse** par email, sms, ou téléphone.

Pour en savoir plus sur le phishing, n'hésitez pas à consulter l'assistance en ligne sur orange.fr.

Nous restons à votre entière disposition pour toute question complémentaire. Vous pouvez demander à être rappelé à ce sujet en cliquant sur le bouton ci-dessous.

Nous vous prions d'accepter, cher(e) Client(e), toutes nos excuses pour ce désagrément, et nous vous confirmons que la protection de vos données reste une priorité de chaque instant pour Orange.

Merci pour votre confiance.

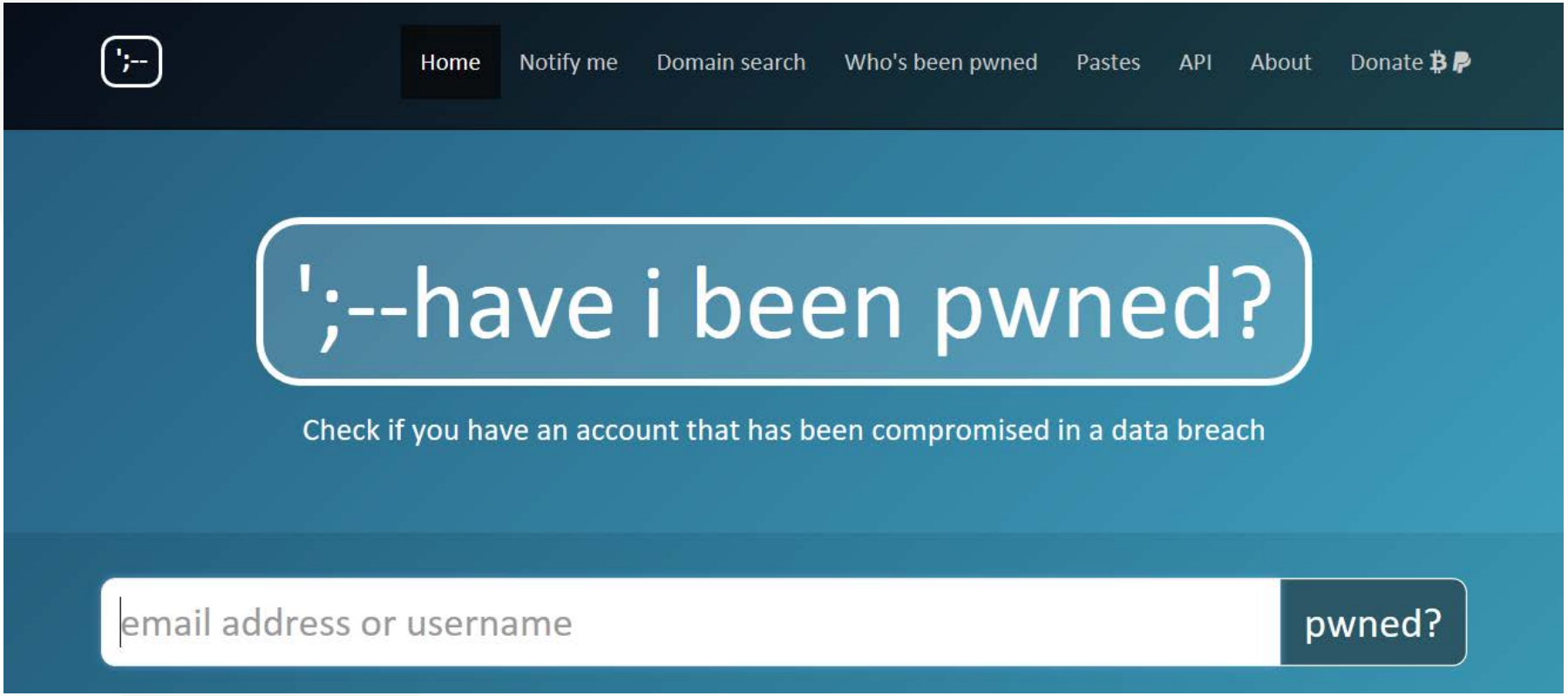
Laurence Thouveny
Directrice de la Relation Clients

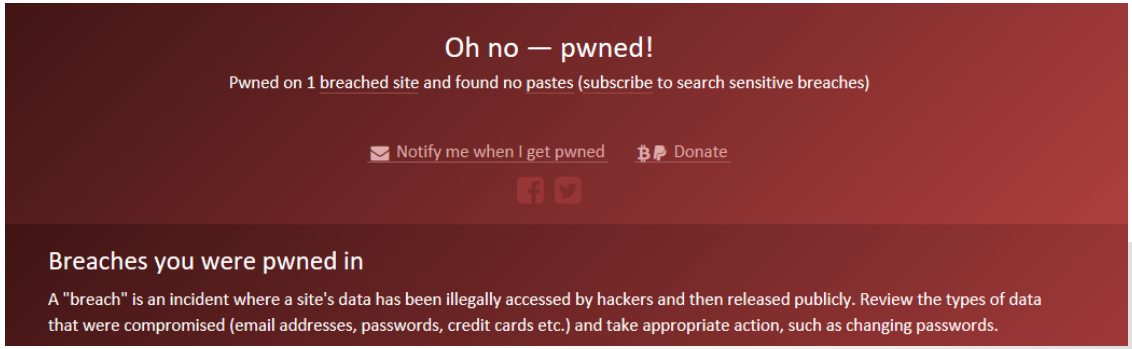
Adobe®

citi

verizon✓

6.5 Obligation de notification des violations





6.6 Protection

- Les mêmes principes subsistent : évaluer les risques compte tenu de l'état de la technique, des frais d'exécution, ainsi que de la nature, de l'ampleur, du contexte et des finalités du traitement

- Le RGPD met plus l'accent sur
  - Le chiffrement
  - La pseudonymisation
  - Le lien avec les principes de gestion des risques (« risk-based approach »)

Illustrations: « normes minimales » de la BCSS

https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/publications/normes-minimales

Cybersécurité: guide pour les PMEs

http://www.ccb.belgium.be/sites/default/files/documents/CCB-FR%20-F.pdf

- Le responsable du traitement doit veiller à disposer de garanties suffisantes: obligation de contrôler un sous-traitant
  - Application recommandée d'un code de conduite ou d'un mécanisme de certification approuvé

6.6 Protection

- Politique du bureau rangé et de l'écran vide : ne laissez aucune information confidentielle sans surveillance sur votre bureau
- N'imprimez que si c'est nécessaire et implémentez une impression de sécurité (utilisez un code ou badge pour lancer l'impression)
- Prévoyez une déchiqueteuse de qualité pour détruire les informations confidentielles sur papier
- Accès aux archives papier : bien protégé et vérification périodique des logs d'accès
- Mots de passe forts, voire même authentification (multifacteur) forte
- Attention en cas de travail à distance (directives nécessaires)
- Etc.

6.7 Transmission à des pays 1/3

- Les principes existants restent d'application : les données à caractère personnel ne peuvent être transmises qu'aux pays tiers en dehors de l'UE :
  - qui sont reconnus par la Commission européenne comme « *offrant une protection adéquate* »

  Illustration: USA? Argentine? Israël? Suisse?
  https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
  - dans des circonstances spécifiques moyennant le suivi des exigences de conformité nécessaires (p. ex. clauses contractuelles types, règles d'entreprise contraignantes)
- Nouveaux schémas : transmission sur la base de codes de conduite ou d'une certification (art. 46)
- Points d'attention :
  - Stockage des données des clients à l'étranger?
  - Sous-traitants
  - Fournisseurs de logiciels cloud

  Illustration: https://cispe.cloud/publicregister/

6.8 Délégué à la Protection des Données (DPD)

- Obligatoire pour les instances publiques et pour les entreprises privées sices dernières ont des *« activités de base »* (art. 37):
  - qui requièrent de par leur nature, de par leur portée et/ou de par leurs finalités***une observation régulière et systématique*** à ***grande échelle*** des personnes concernées, ou
  - qui traitent ***à grande échelle*** de ***catégories particulières*** de données

  Illustration: compagnie de gardiennage? Programmes de fidélité clients ?

- Il peut s'agir d'un service tant externe (contrat de services) qu'interne (collaborateur) et un groupe d'entreprises peut désigner un seul DPD pour l'ensemble du groupe

- Pas besoin de « diplôme » mais « connaissances spécialisées » et « qualités professionnelles »

- Contact principal pour les personnes concernées ainsi que pour la CPVP

- Rôle indépendant et protégé contre le licenciement ou des sanctions dans le cadre de l'exécution de ses tâches

6.8 Délégué à la Protection des Données (DPD)

- Vérifiez qui va assumer ce rôle

- Doit disposer d'une situation indépendante dans l'organisation (*pas de conflits d'intérêts*) et rendre directement compte au management supérieur

Illustration: Responsable RH et DPO?

- Plus d'informations dans les directives du groupe de travail « article 29 » et de la CPVP :
  - https://www.privacycommission.be/sites/privacycommission/files/wp243_rev01_enpdf_DPO_3.pdf
  - https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf

6.9 Sous-traitants

- Les sous-traitants ont été expressément visés dans le RGPD
  - Responsabilité accrue
  - Toute une série d'obligations supplémentaires et directes

- Les obligations suivantes méritent une attention supplémentaire dans ce cadre:

  - Il est de la responsabilité finale du responsable du traitement de donner des garanties suffisantes que les données sont bien protégées et d'en assurer le suivi

  - Vous avez, en tant que responsable du traitement, le droit d'être informé de la sous-traitance du traitement à des sous-contractants et vous pouvez vous y opposer (ou résilier cette partie du contrat)

  - Un sous-traitant doit suivre les instructions du responsable du traitement, mais restez réaliste et tenez également compte des obligations du sous-traitant à cet égard

- Relecture, voire révision, des contrats existants !

Guide pratique de la CNIL

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

6.10 Analyse d'impact

- La « *privacy impact assessment* »(PIA) est obligatoire en cas de risques élevés pour les droits et libertés des personnes concernées (p. ex. le profilage, le traitement à plus grande échelle des catégories particulières de données à caractère personnel, l'utilisation d'une nouvelle technologie)
  - Cela nécessite d'examiner si une activité déterminée présente un risque élevé ou non (p. ex. monitoring IT au travail)
  - Vérifier les listes de la CPVP (p. ex. une évaluation pour*« analyser ou prévoir des prestations professionnelles »* mais PAS pour *« l'administration du personnel en service»* au sens strict)

- Obligation d'évaluer lesrisques du point de vue de la personne concernée, contrairement à l'analyse typique des risques d'entreprise qui tient généralement compte de l'intérêt de l'organisation

- Pour la CPVP, la décision de (ne pas) procéder à une analyse doit être officiellement soumise aux membres de la direction!

Lignes directrices du groupe de travail « article 29 » et de la Commission et outils de la CNIL et de la BCSS

ec.europa.eu/newsroom/document.cfm?doc_id=47711

https://www.privacycommission.be/consultation-publique-sur-la-recommandation-concernant-lanalyse-dimpact-relative-a-la-protection

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/general-data-protection-regulation

6.11 Privacy « by design » & « by default »

- Développer des produits et des services qui intègrent, dès le début, la protection de la vie privée (« by design »)
  - Toujours tenir compte de la protection de la vie privée de l'agent dès le début et impliquez, en cas de doute et si nécessaire, votre DPD

Illustration: « minimisation » des données: c'est-à-dire? L'exemple de « formulaires en ligne »

  - Veillez à y consacrer de l'attention dans toutes les étapes du cycle de vie d'un service/produit

- /!\ Les paramètres en matière de protection de la vie privée doivent être actifs par défaut, et non facultatifs

- Tout doit pouvoir être démontré: veillez donc bien à ce que tout ce que vous faites en tant que partie d'un projet soit bien documenté !

7. Et maintenant, comme procéder?

- Parcourez la documentation élaborée par les autorités de contrôle
  - Plan en 13 étapes élaboré par la Commission de la protection de la vie privée

https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

  - Plan en 12 étapes élaboré par l'ICO (Royaume-Uni)

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

  - Plan en 10 étapes élaboré par l'AP (Pays-Bas)

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

  - Plan en 7 étapes élaboré par la CNPD (Luxembourg)

https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Une-responsabilite-accrue-des-responsables-du-traitement/guide-preparation-rgpd/index.html

  - Plan en 6 étapes élaboré par la CNIL (France)

https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

  - Site de la Commission européenne

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr

Documentez!

- Allouez du temps et des ressources (internes et/ou externes) à ce projet multidisciplinaire
- Sensibilisez vos agents et votre management
- Identifiez « vos » données à caractère personnel et « vos » traitements, en Belgique et à l'étranger (y compris par rapport à « vos » sous-traitants)
  - Sur base des modèles existants
- Désignez votre DPD puisqu'obligatoire pour les organismes publics/autorités publiques
  - Utile notamment pour une analyse d'impact et les contacts à ce sujet avec les travailleurs et l'autorité de contrôle
- Etablissez et mettez en place un « plan d'action » (p. ex. actualiser la base légale d'un traitement?, révision des mentions d'information vis-à-vis des personnes concernées et des contrats avec les sous-traitants, modalités d'exercices des droits, etc.)
- Réfléchissez à la certification et/ou l'adhésion à un code de conduite

- Vous avez dit…« opportunités »?
  - Se « réapproprier» en interne les données et les processes par les départements concernés ;
  - Inciter à la transformation digitale (p. ex. sécurisation renforcée des dossiers des personnes concernées, surveillance facilitées des délais de conservation, etc.);
  - Diminution du risque de vulnérabilité informatique (p. ex. en sensibilisant les équipes et en révisant les mesures techniques et organisationnelles appropriées);
  - Protéger les données, c'est protéger un actif de la société;
  - Obtenir la confiance des personnes concernées;
  - Etc.

Pour rester informé, consultez notre blog:

blog.commyounity.be

Merci pour votre attention et bonne continuation!

younity
AVOCATS | ADVOCATEN | LAWYERS

Nicolas Roland
Avocat-associé

nicolas.roland@younity.be