Data Protection institute

5 mois après le 25 mai 2018

Quelles expériences?

Morceaux choisis

DPO Forum – 23 Octobre 2018

Florence de VILLENFAGNE

FORMATRICE DP-INSTITUTE
DATA PROTECTION CONSULTANT
florence@ictlex.be

Data Protection institute

Florence de VILLENFAGNE

- Law degree (UCL), DES in IT Law (Univ Namur), DPO Certification (DP-Institute)
- 18 years of experience in IT law and more specifically data protection
  - Lot's of experience in the private sector – multinationals or SMEs (retail, print services, services to children, industry, real estate)
  - Public sector (hospital)
- 18 years of training experience (cybercrime, data protection)
  - University of Namur
  - Infosafe (ICHEC, UNamur)
  - European Commission (2007-2017)
  - **DP-Institute – Formation en français (2017…)**
- **Founder of ICTLex in 2012 – GDPR compliance implementation, data protection legal expertise**

Data Protection institute

https://www.dp-institute.eu/nl/home

Prochaines formations DP-INSTITUTE

- 26-30 novembre 2018 – Zaventem
- 17-21 décembre 2018 – LLN
- 18-22 février 2019 – Zaventem
- 6-10 mai 2019 – LLN

Quelles expériences?

- Morceaux choisis
  - DP by default & by design
  - Respect des droits
  - conservation

- Point de vue juridique
- Exemples de la pratique

5 mois après le GDPR …

PROTECTION DES DONNÉES DÈS LA CONCEPTION
ET
PROTECTION PAR DÉFAUT

Protection des données dès la conception

Art. 25.1

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement

ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques,

le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même,

des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont **destinées à mettre en œuvre les principes** relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

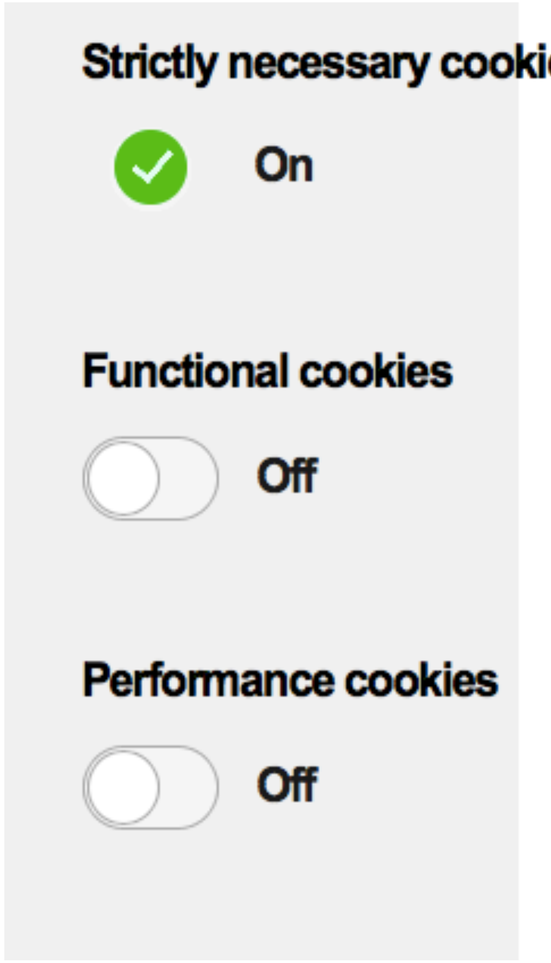
- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement a**ppropriate technical and organisational measures**, such as pseudonymisation, which are **designed to implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Protection des données par défaut

- Article 25.2
- Par défaut, seules les données nécessaires pour les finalités sont traitées
- Plusieurs paramètres sont possibles
- La personne concernée agit pour étendre la quantité de données, l'étendue du traitement, la durée de conservation, l'accessibilité

- Article 25.2
- By default, only process data necessary for purpose
- Several parameters
- Individuals intervention to extend amount, retention period, access

Protection des données par défaut



These cookies are essential so that you can move around the website and use its features. Without these cookies services you have asked for cannot be provided.

See list of strictly necessary cookies

These cookies allow the website to remember choices you make to give you better functionality and personal features.

See list of functional cookies

These cookies help to improve the performance of

See list of performance cookies

Protection des données dès la conception –DP by design

- Approche basée sur le risque
  - Risque pour les droits et libertés des personnes
- Au moment
  - De la détermination des moyens
  - Lors de la mise en œuvre du traitement
- garanties nécessaires
  - Pour répondre aux exigences du GDPR
  - Pour protéger les droits de la personne concernée

Points de vue: responsable du traitement

- Équipe (IT, DP, business)
  - ➔ *déterminer les risques*
  - ➔ *Définir la ou les finalité(s)*
  - ➔*mesures techniques et organisationnelles pour le respect des principes*
    - Limiter:
      - Pseudonymiser si possible
      - Finalité atteinte en limitant l'utilisation de données pers.
    - *Sécurité*
    - *Respect des droits*

- Sous-traitant éventuel
  - ➔ *garanties nécessaires*
  - ➔ *possibilités de l'outil?*

Bien sûr : + transparence, formation

Point de vue du sous-traitant

- **Sous-traitant: création de logiciel**

  - Prévoir les paramètres qui permettent de respecter les principes:

    Pour les droits des personnes
    - Effacement possible?
    - limitation (*freeze*)
    - Opposition: conservation, mais respect de l'opposition
    - Portabilité
    - Décisions automatiques - exceptions

    Pour les obligations du RT
    - Preuve de consentement (temps/lieu)
    - Définition de la durée de conservation (plusieurs!)
    - Effacement ou copie en fin de contrat

    AVANTAGE CONCURRENTIEL….

Exemples de mesures

- Techniques
  - Chiffrement/encryption
  - Pseudonymisation
  - Gestion et contrôle des accès aux systèmes et physiques (pw, ID & access mngt)
  - Effacement automatiques
  - Back-ups automatiques (protection contre la perte de données)
  - Utilisation de systèmes certifiés
  - Fonctions techniques pour répondre aux demandes des personnes concernées (droits)
  - Timestamps et preuve automatique de consentement
- Organisationnelles
  - Project management : DP inclus dès le départ
  - Documentation des finalités, des bases légales
  - Documentation des mesures de minimisation
  - Documentation des consentements (stratégie d'opt in,…)

EXEMPLES

CNIL
Exemples

ICO
Commentaires et check list

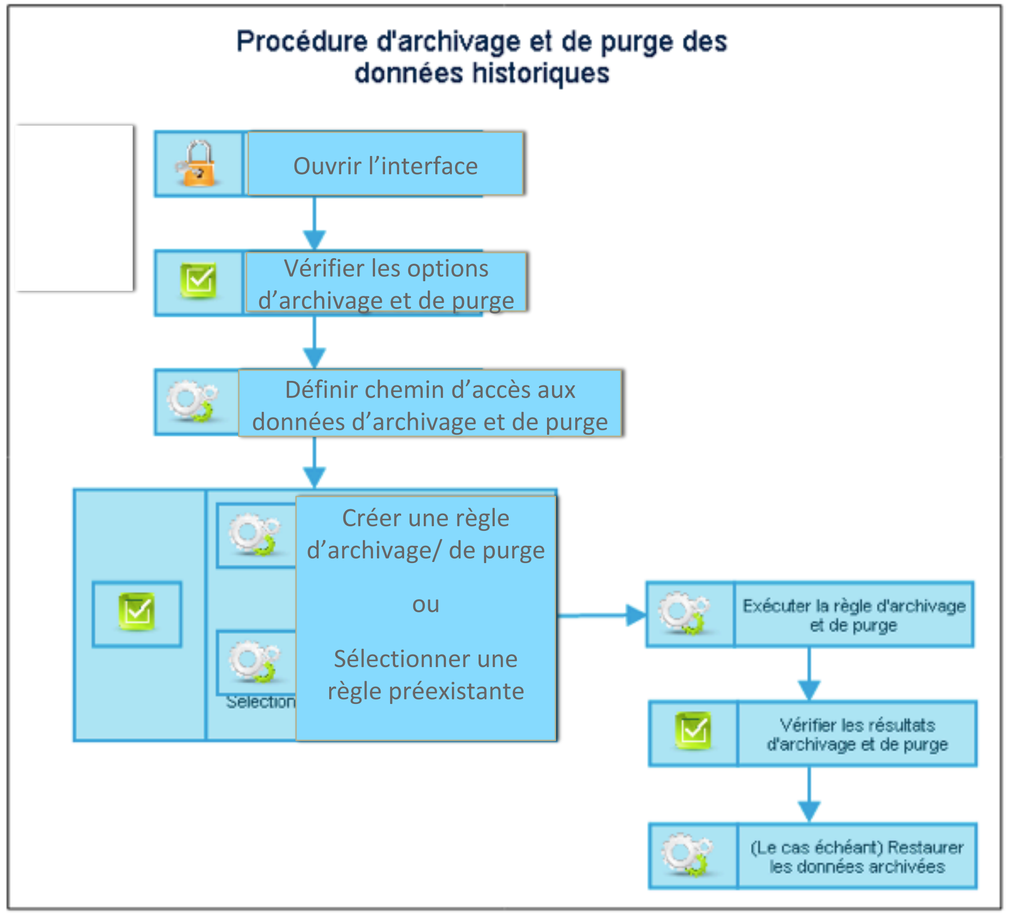
Autres expériences/other experiences
HR
Analytics

Exemple de la CNIL

Un éditeur de logiciel doit s'interroger dès la création de son outil sur les champs que ses clients pourront remplir dans le cadre de son objet. Dans un outil de gestion clients (CRM ou ERP), la présence de champs de texte libre pour insérer des commentaires suite à un contact client peut conduire, par exemple, à inscrire des propos excessifs ou non pertinents. Il est donc utile de prévoir des listes déroulantes de motifs de contacts à la place, qui seront objectifs et neutres.

Exemple de la CNIL

- *Un hébergeur de données doit proposer à ses clients de purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée*



ICO Comments

« Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability»

Checklist ICO

- ☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- ☐ We make data protection an essential component of the core functionality of our processing systems and services.
- ☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- ☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- ☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- ☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- ☐ We adopt a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data.

Checklist ICO/2

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

AUTRES EXPÉRIENCES

DATA PROTECTION BY DESIGN
RESPECT DES DROITS
CONSERVATION DES DONNÉES

Système permettant un suivi du personnel sur des chantiers

- Sous-traitant
- Le RT reçoit la maîtrise totale des données (le RT devra répondre à toutes les demandes concernant les droits des personnes ➔ il devra mettre des procédures en place)
  - Effacement possible?
  - Export possible (interopérable)?
  - Blocage possible – freeze?
  - Durée de conservation prévue? (combien de temps?) – à vérifier: plusieurs durées? Évolution (ex: recrutement)
  - Fin de contrat: exportation possible et effacement?

Logiciel pour les médecins du travail

Confidentialité des données

- Données chiffrées
- pas d’accès par le sous-traitant.
- Attention aux accès par des admin IT ou des services de support

Support IT et systèmes RH

Questions de confidentialité et de conservation des données

- Masquage des noms pour le service IT (support, test)
- emergency user – logging de tous les accès du service de support
- Effacement de données n'est pas toujours possible à cause des liens existant entre les tables
- Volonté de répondre aux demandes de personnes proches de la pension : quelle solution?
  - archivage, limitation d'accès, logs… documentez votre décision

Merci

Florence de Villenfagne

ICTLEX

florence@ictlex.be