Privacy by design & by default

Sensibilisation aux principes de la protection des données dès la conception et par défaut

NEO DPO

Sommaire

1. Les principaux textes

- Convention internationale pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 et modernisée le 18 mai 2018 , dite « **Convention 108** » (55 pays signataires)

- Le Règlement européen n° 2016/679, dit « **Règlement général sur la protection des données** » ou encore « **RGPD** » adopté le 27 avril 2016 et entré en application le 25 mai 2018

✓ Renforcer les droits des personnes
✓ Renforcer les obligations de tous les acteurs traitant des données personnelles
✓ Renforcer la crédibilité des autorités de contrôle en leur octroyant un pouvoir de sanction financière très élevé

- **Art 7 et 8** de la Charte des droits fondamentaux de l'Union européenne , **Art 16** du traité sur le fonctionnement de l'Union européenne et **Art 8** de la Convention européenne des droits de l'homme

- La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « **Loi Informatique et Libertés** » et son décret d'application n° 2019-536 du 29 mai 2019

✓ Récemment modifiée pour s'adapter au RGPD

- **Art 9 du Code civil : « Chacun a droit au respect de sa vie privée…»**

2. Les notions clés

✓ **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable

- Les données **directement identifiantes** : nom et prénom, email nominatif, photo…
- Les données **indirectement identifiantes** : numéro client, numéro de téléphone, plaque d'immatriculation, numéro de sécurité sociale, adresse postale, voix ou image
- **Toute combinaison** d'information permettant d'identifier une personne
- Les **données qui peuvent être rattachées à une personne physique** : achats, déplacements réels ou virtuels, salaire, communication, centres d'intérêt, commentaires, etc.

2. Les notions clés

- ✓ **Traitement de données à caractère personnel :** est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement

  →Cela concerne les fichiers informatisés ou papier

  →Le traitement de données personnelles **N'EST PAS le traitement informatique.** Il faut ici raisonner en finalité et non en applications et logiciels.

2. Les notions clés

- ✓ **Responsable de traitement :** personne physique ou morale, autorité publique, ou autre organisme qui détermine les moyens et les finalités d'un traitement, c'est à dire l'objectif et la façon de le réaliser

- ✓ **Sous-traitant :** personne physique ou morale, autorité publique, ou autre organisme qui traite des données personnelles pour le compte du responsable de traitement

3. Les principes généraux (7)

1. **Licéité, loyauté et transparence** : les personnes doivent être informées de l'existence du traitement qui doit être fondé sur l'une des six bases légales visées à l'article 6 du RGPD (consentement, exécution d'un contrat/mesures précontractuelles, respect d'une obligation légale, sauvegarde des intérêts vitaux, mission de service public, intérêts légitimes)

2. **Limitation des finalités** : les objectifs poursuivis par le responsable de traitement doivent être déterminés à l'avance, explicites et légitimes + interdiction du traitement ultérieur des données pour une finalité incompatible à celle d'origine (Détournement de finalité)

3. **Minimisation des données** : seules les données strictement nécessaires à l'objectif poursuivi par le traitement ne peuvent être traitées

3. Les principes généraux (7)

4. **Exactitude des données** : les données doivent être exactes et si besoin être tenues à jour

5. **Limitation de la conservation** : les données sont en principe conservées que le temps nécessaire à la réalisation de l'objectif poursuivi

6. **Sécurité des données** : le responsable du traitement doit garantir l'intégrité et la confidentialité des données et empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y ait accès.

7. **Responsabilisation :** le responsable du traitement doit être en mesure d'apporter la preuve que tous ces principes sont bien respectés

4. L’obligation de respecter les principes de privacy by design et by default

Tenir et mettre à jour des registres de traitements	Désigner un DPO	**Respecter le principe du Privacy by design et by default**
Sécuriser les relations avec les sous-traitants	Mener des analyses d’impact pour les traitements à risques élevés	Sécuriser les transferts vers des pays tiers à l’UE
Obligation de sécurité	Notifier les violations de données dans les 72 H à la CNIL	Documenter sa conformité - Accountability

4. L'obligation de respecter les principes de privacy by design et by default

✓ **Art 25 RGPD** – **protection des données dès la conception** et protection des données par défaut

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.

4. L'obligation de respecter les principes de privacy by design et by default

✓ **Art 25 RGPD** – protection des données dès la conception et **protection des données par défaut**

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, **par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées**. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, **par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques** sans l'intervention de la personne physique concernée.

4. L’obligation de respecter les principes de privacy by design et by default

✓ **Considérant 78 du RGPD (extrait)**

(…) Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications **à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications** et, compte dûment tenu de l'état des connaissances, **à s'assurer que les responsables du traitement et les sous- traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données**. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.

4. L'obligation de respecter les principes de privacy by design et by default

- ✓ Le CEPD (EX G29) a adopté le 20 oct. 2020 des **lignes directrices** relatives au privacy by design et au privacy by default

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

4. L'obligation de respecter les principes de privacy by design et by default

- ✓ **Origine du concept de Privacy by design** : né à la fin des années 90, à l'initiative de la commissaire à l'information et à la protection de la vie privée de l'état de l'Ontario (Canada), Ann Cavoukian

- ✓ **Signification** **:** Afin de limiter les risques de traitements abusifs et de violation de données portant atteinte à la vie privée des personnes concernées, l'approche Privacy by design, impose au responsable de traitement de mettre en place un ensemble de mesures préventives de sécurité en amont de la création de son produit, de son service impliquant des traitements de données à caractère personnel

4. L'obligation de respecter les principes de privacy by design et by default

✓ **Contenu du concept de Privacy by design** : L'approche Privacy by design a été décliné en sept (7) principes et constitue une solution permettant aux technologies d'évoluer sans porter atteinte à la vie privée des individus :

1. **Être proactif et non réactif, préventif et non correctif**
(Consiste à prévoir et à prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent)
2. **Protection par défaut**
(Garantir le maximum de protection possible de façon implicite, sans que la personne concernée n'ait à intervenir)
3. **Protection de la vie privée intégrée dès la conception**
(La protection de la vie privée doit être prise en considération dés le début et coexister avec les idées innovantes sans les paralyser)
4. **Conciliation des intérêts**
(Le PBD n'a pas pour but d'assurer la protection des données au détriment des technologies innovatrices et du progrès technique)
5. **Sécurité de bout en bout, durant tout le cycle de vie de la donnée**
6. **Visibilité et transparence assurées par le RT**
(Vise à rassurer les personnes concernées sur l'utilisation sécurisée de leurs données)
7. **Respect de la vie privée des utilisateurs**
(Place les individus en centre de la protection)

4. L'obligation de respecter les principes de privacy by design et by default

→ **En résumé, les exigences de l'article 25 impose à :**

- ✓ **Tout responsable de traitement qui souhaite réaliser un nouveau produit ou service impliquant un traitement de données à caractère personnel de mettre en œuvre en amont des mesures techniques et organisationnelles pour garantir le respect des principes fondamentaux et les droits des personnes**

- ✓ **Tout responsable de traitement de s'assurer que, par défaut, c'est à dire sans que la personne concernée n'ait à intervenir, la quantité de données collectées, la diversité des finalités, la durée de conservation, et le nombre de personnes habilitées à accéder aux données personnelles se limite au strict minimum**

4. L'obligation de respecter les principes de privacy by design et by default

→ Exemples d'une approche PBD&BD :

✓ **Une société souhaite créer pour ses propres besoins, un nouveau logiciel de gestion de réclamation :**

- Privilégier un menu déroulant ou des cases à cocher plutôt que des zones de commentaires libres
- Mettre en place un mécanisme de pseudonymisation des données lorsqu'il n'est pas strictement nécessaire de les conserver sous une forme identifiantes
- Intégrer des mécanismes de purge automatique à l'issue d'une certaine durée

✓ **Une société souhaite développer une application mobile de e-commerce :**

- Par défaut, cette application ne devra pas collecter les coordonnées GPS de ses clients puisqu'elles ne sont pas nécessaires à l'achat de produits. Néanmoins, il sera possible de laisser le choix à l'utilisateur d'autoriser leur collecte pour une utilisation spécifique, par ex pour trouver le point de livraison le plus proche de chez lui

4. L'obligation de respecter les principes de privacy by design et by default

→ Exemples de cas non conformes :

- L'application informatique déployée récemment ne prévoit pas de purge automatique des DCP dont le traitement n'est plus nécessaire
- Les DCP restent stockées dans la base de données active pour une durée illimitée alors qu'elles devraient basculer dans une base de données intermédiaire, voire dans une base d'archivage en fonction de la finalité du traitement et du cadre légal applicable aux DCP concernées
- L'application informatique ne prévoit pas de chiffrement des DCP permettant de limiter leur lisibilité aux seuls professionnels habilités à y accéder
- Les DCP échangées en pièce jointe de courriel ne sont pas chiffrées ou protégées contre une lecture illicite notamment lors de l'usage de la messagerie sur internet
- Les traces embarquées dans les applications informatiques sont difficilement exploitables (si elles existent) pour identifier l'origine d'une violation de données
- Les supports amovibles (exemple : clé USB) utilisés par les utilisateurs contiennent des DCP et ne sont pas protégés en cas de perte ou de vol

5. Les avantages d'une approche privacy by design & by default

- Permettre **une réduction des risques juridiques** liés à un manquement à la règlementation

- Démontrer sa capacité à fournir des services conformes à la législation

- Constitue dès lors **un avantage compétitif** et peut permettre **une réduction des coûts de développement des services** dans la mesure où la protection des données n'est pas prise en compte seulement en toute fin de projet

- Tout le travail réalisé pourra être conservé car il contribuera à la documentation du traitement et donc à démontrer **le respect des principes de Privacy by Design** et d'**accountability,** soit **la capacité pour le responsable de traitement à démontrer sa conformité au RGPD**.

6. Les sanctions encourues

✓ 6.1 Les sanctions pécuniaires :

Les amendes administratives sont réparties en deux catégories en fonction de la nature de la violation

10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial de l'exercice précédent dans le cas d'une entreprise(le montant maximum étant retenu)

- Les obligations des responsables de traitement et des sous-traitants (l'accountability, **le privacy by design et by default**, représentation en UE, registres des traitements, l'analyse d'impact, la consultation préalable, règles de la sous-traitance, responsabilité conjointe, désignation d'un DPO, la notification des violations, la sécurité etc.)
- Les obligations des organismes de certification et des organismes en charge du suivi des codes de conduite

20 millions d'euros ou de 4 % du chiffre d'affaires annuel mondial de l'exercice précédent dans le cas d'une entreprise (le montant maximum étant retenu)

- Les droits des personnes concernées (par exemple en cas de défaut de réponse à une demande de droit d'accès, d'absence d'une mention d'information sur un formulaire de collecte, etc.)
- Les principes fondamentaux des traitements
- Transferts de données hors Union européenne ou vers une organisation internationale
- Obligations prévues par le droit des États membres en application du chapitre IX du RGPD (concernant des traitements spécifiques)
- Le non respect d'une mesure corrective de la CNIL ou le refus d'un accès

6. Les sanctions encourues

✓ **6.2 Les sanctions pénales :**

- Art 226-16 et suivants du code pénal
- Les infractions suivantes sont assorties d'une amende de 300 000€ et de 5 ans d'emprisonnement :
  - Le détournement de finalité du traitement
  - Le traitement du NIR en dehors des cas autorisés
  - Le fait de traiter des DCP en méconnaissance des articles 24 (accountability), **25 (privacy by design et by default)**, 30 (registre des traitements) et 32 (obligation de sécurité)
  - Le fait de ne pas notifier une violation de données personnelles
  - Le fait de collecter des DCP par un moyen frauduleux, déloyal ou illicite
  - Le fait de procéder à un traitement de prospection, notamment commerciale, alors que la personne s'y est opposée
  - Le fait, hors cas prévues par la loi, de traiter des données sensibles sans le consentement explicite de la personne
  - Le fait de conserver des DCP pour une durée excessive
  - Le fait de ne pas respecter les dispositions relatives aux transferts hors UE ou vers une organisation internationale

6. Les sanctions encourues

✓ **6.3 Bilan des sanctions**

Amendes administratives	Sanctions pénales	Sanctions civiles et économiques
✓ Jusqu'à **10 millions d'euros ou 2 % du CA mondial** de l'entreprise, le chiffre le plus élevé étant retenu	✓ Jusqu'à **300 000 euros** d'amende et **5 ans d'emprisonnement**	✓ Dommages-intérêts, perte de clientèle, atteinte à l'image et à la réputation

6. Les sanctions encourues

✓ 6.4 Exemples de sanctions prononcées (1/2)

Date	Organisation	Montant	Autorité de contrôle	Motifs
10/2019	Deutsche Wohnen SE Real estate company	**14, 5 M €**	BCDP Allemagne	• **Atteinte au principe de limitation de la conservation des données personnelles** • **Impossibilité de suppression des données personnelles** • **Violation des principes de privacy by design & by default**
« the supervisory authority found that the company used an archive system for the storage of personal data of tenants **that did not provide the possibility of removing data that was no longer required**. Personal data of tenants was stored without checking whether storage was permissible or even necessary. »				

6. Les sanctions encourues

✓ 6.4 Exemples de sanctions prononcées (2/2)

Date	Organisation	Montant	Autorité de contrôle	Motifs
10/2019	Municipality of Oslo	**120 000 €**	Datatilsynet.no Norvège	• **Violation de l'obligation de sécurité des données personnelles** • **Violation des principes de privacy by design & by default**
« One of the intended uses of the app is for parents to send messages regarding their children and absence from school using a free-text field. This enables communication of special category personal data, such as health data, regarding the children. There are no technical measures to prevent this from happening, and no information is given within the app that such transmission should be avoided. **In line with data protection by design and default**, alternative measures such as drop-down lists and tick boxes are more appropriate. »				

Des questions ?

N’hésitez pas à me contacter

Rani ZAIDI – Consultant RGPD
DPO certifié Bureau Veritas

contact@neo-dpo.fr
06.63.61.38.68

www.neo-dpo.fr

NEO DPO