La Protection des données à caractère personnel

Privacy by Design et Privacy by Default

02/11/2016

Aïssatou SARR

Sensibilité : Interne almerys

Référence :

SOMMAIRE

- Partie I:
  - ✓ Principes
- Partie II:
  - ✓ Définitions
- Partie III:
  - ✓ Application

Partie I: Les Principes

- L'article 25 du Règlement Général sur la Protection des Données (RGPD)
- Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois **dès la conception** du produit ou du service et **par défaut**.
- Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).
- Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément attestant du respect des exigences du Privacy by Design et by Default.

- Le Privacy by Design est basé sur l'approche de l'ingiénierie des systèmes qui prend la vie privée en compte tout au long des projet (avant, pendant et après avec le Privacy by Default).

- C'est un fondement mondialement connu duquel découle 7 principes fondamentaux:
  - ✓ 1. Proactive et non réactive; Préventive pas correctives
  - ✓ 2. Confidentialité comme paramètre par défaut
  - ✓ 3. Confidentialité intégré dans la conception
  - ✓ 4. La fonctionnalité complète - à somme positive, et non pas à somme nulle
  - ✓ 5. End-to-end de sécurité - une protection complète du cycle de vie
  - ✓ 6. Visibilité et transparence - le garder ouvert
  - ✓ 7. Respect de la vie privée des utilisateurs - garder centrée sur l'utilisateur

Partie II: Les Définitions

- Privacy by Design: (Protection des données dès la conception)

- Définition fournie à l'article 25-1 du RGPD

- 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.

- Privacy by Default: (Protection des données par défaut)

- Définition fournie par l'article 25-2 du RGPD

- 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.

Partie III: L'application

- Le considérant 78 du RGPD donne des exemples de moyens permettant la bonne application du Privacy by Design et by Default:

  - ✓ réduire à un minimum le traitement des données à caractère personnel,
  - ✓ pseudonymiser les données à caractère personnel dès que possible,
  - ✓ garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel,
  - ✓ permettre à la personne concernée de contrôler le traitement des données,
  - ✓ permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer.
  - ✓ faire des Etudes d'Impacts sur le Vie Privée (EIVP : PIA) avant la mise en œuvre des projets

- La CNIL considère que certains outils de conformités permet la bonne applicabilité de ces deux fondements:

  - ✓ L'application du principe d'accountability
  - ✓ La tenue d'un Registre des traitements mis en ouvre
  - ✓ La notification de failles de sécurité (aux autorités et personnes concernées)
  - ✓ La certification de traitements
  - ✓ L'adhésion à des codes de conduites
  - ✓ Le DPO (délégué à la protection des données)
  - ✓ Les études d'impact sur la vie privée (EIVP)

- Les Etudes d'Impact sur la Vie Privée (EIVP ou PIA)

- Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître
  - ✓ les caractéristiques du traitement,
  - ✓ les risques et les mesures adoptées.

- Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale**, les données concernant la santé** ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

- Si l'organisme ne parvient pas à réduire ce risque élevé par des mesures appropriées, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement.

- Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences

- Les notifications des violations de données personnelles

- Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

- Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

A PREVOIR DANS NOS PROJETS

- Le consentement
  - ✓ Prouver l'obtention
  - ✓ Doit être express
  - ✓ Doit être distinct
  - ✓ Doit être éclairé
  - ✓ Doit pouvoir être révoqué facilement

- Les données des mineurs
  - ✓ Consentement du tuteur légale
  - ✓ Compréhension du traitement
  - ✓ Possibilité de récupérer la main sur la gestion à la majorité

- La possibilité d'appliquer les droits:
  - ✓ Doit à l'oubli
  - ✓ Droit d'accès
  - ✓ Droit de rectification
  - ✓ Droit de suppression
  - ✓ Droit d'opposition
  - ✓ Droit de limitation
  - ✓ Droit de portabilité des données

- La mise en œuvre d'une Etude d'Impact sur la Vie Privée (EIVP ou PIA)
  - ✓ Faite par le chef de projet
  - ✓ Validé par la sécurité
  - ✓ Validé par la DPO
  - ✓ Mise à la disposition de la CNIL si besoin

- La pseudonymisation ou anonymisation
  - ✓ Prévoir l'anonymisation des données

Ce document est propriété d'almerys, il est mis votre disposition à des fins informatives.

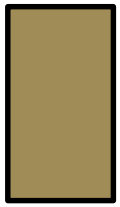
Toute utilisation de présentations dont les contenus sont élaborés par almerys doit être soumise à demande auprès de

marketing@almerys.com

Rappels – couleurs autorisées par la charte graphique almerys

Univers coloriel principal

RVB pour écran - *Pantone pour impression papier*



R : 160
V : 140
B : 87

C : 32
M : 33
J : 66
N : 02

Univers coloriel complémentaire

RVB pour écran - *Pantone pour impression papier*

R : 96
V : 99
B : 103

C : 62
M : 52
J : 49
N : 20

- Ce modèle est destiné à un usage interne almerys ; *utilisez le modèle dédié pour vos supports à destination de l'externe.*