

RGPD Règlement européen sur la protection des données : Une conformité basée sur la transparence et la responsabilisation

✕	RGPD Règlement européen sur la protection des données : Une conformité basée sur la transparence et la responsabilisation
---	--

Ainsi que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (privacy by design)

Les responsables de traitement doivent mettre en œuvre toutes les mesures techniques et organisationnelles raisonnables 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 traitées dès le départ (principe dit de « minimisation »).

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles et/ou le traitement de manière continue, les responsables de traitement et les sous-traitants devront mettre en place des mesures de protection des données appropriées et documenter cette conformité à tout moment (accountability). Le caractère de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être remplacé par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la certification de l'absence de transfert des données et personnes concernées
- la certification de traitement
- l'adhésion à des codes de conduite
- le DPI (relatif à la protection des données)
- le DPI (relatif à la vie privée (DPIV))

Les « études 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, les données relatives à la vie sexuelle), des données génétiques ou biométriques, et de traitements relatifs à l'identification systématique et approfondie d'éléments personnels des personnes physiques. C'est-à-dire notamment de profilage.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

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

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées. L'absence de conformité des responsables de traitement doit résulter de l'absence 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.

Le Délégué à la Protection des données (Data Protection Officer)

- Les responsables de traitement et les sous-traitants doivent obligatoirement désigner un délégué :
- s'ils appartiennent au secteur public ;
 - si leurs activités principales les amènent à traiter (souvent à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
- En outre, de cas en cas, la désignation d'un délégué à la protection des données sera bien sûr possible.
- Les responsables de traitement peuvent opter pour un délégué à la protection des données internal ou externe.
- Le délégué devient le « secrétaire » chef d'orchestre et de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :
- d'informer et de conseiller la responsable de traitement ou le sous-traitant, ainsi que ses employés ;
 - de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
 - de conseiller l'organisme sur la réalisation d'une analyse d'impact (FAI) et d'en vérifier l'adéquation ;
 - de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Besoin d'un accompagnement pour vous mettre en conformité avec le RGPD ?

Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?

Contactez-nous

à lire aussi :

- Plus en conformité RGPD : Mode d'emploi
- Formation RGPD : L'essentiel sur le Règlement Européen pour la Protection des Données Personnelles
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
- DIRECTIVE (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016
- Le RGPD, règlement européen de protection des données. Comment passer le RGPD ?
- Comprendre le Règlement Européen sur les données personnelles en 6 étapes
- Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des Données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation et d'aide, nous faisons passer les dirigeants et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement européen relatif à la Protection des Données à caractère personnel (RGPD) ou vous assistent dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement... (Autorisation de la Direction du Travail de l'Enfance et de la Formation Professionnelle n°33 24 0341 24)

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

CIL

Revenez à cet article

Source : Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL