# Le Paquet « Protection des données à caractère personnel » adopté


Le Paquet « Protection des données à caractère personnel » adopté

**Le règlement général sur la protection des données ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives ont été adopté le 14 avril…**

Ce Paquet vise à réformer la législation communautaire d'une part et à remplacer la directive générale sur la protection des données qui datait de 1995 d'autre part.

## 1. Les nouveaux principes à mettre en oeuvre par le règlement

Le règlement européen sur la sur la protection des données (2) consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés.
Si les formalités administratives sont simplifiées pour mettre en œuvre un traitement, les obligations sont en revanche renforcées pour assurer une meilleure protection des données personnelles :

• la démarche de « Privacy by design » (respect de la protection des données dès la conception) (Règlement, art. 25 §1) ;
• la démarche de « Security by default » (sécurité par défaut) (Règlement, art. 25 §2) ;
• les règles d'accountability (obligation de documentation) (Règlement, art. 24) ;
• l'étude d'impact avant la mise en œuvre de certains traitements (Règlement, art. 35) ;
• la désignation obligatoire d'un Data Protection Officer (DPO) (Règlement, art. 37) ;
• les nouveaux droits fondamentaux des personnes (droit à l'oubli, droit à la portabilité des données, etc.) sur lesquels nous reviendrons dans un prochain article.

### 1.1 Le respect de la protection des données dès la conception ou « Privacy by design »

Le règlement européen sur la protection des données consacre le principe de « Privacy by design » qui impose aux entreprises publiques comme privées de prendre en compte des exigences relatives à la protection des données dès la conception des produits, services et systèmes exploitant des données à caractère personnel.
Cette obligation requiert que la protection des données soit intégrée par la Direction des systèmes d'information dès la conception d'un projet informatique, selon une démarche « Privacy by design ». Elle rend également nécessaire la coopération entre les services juridiques et informatiques au sein des entreprises
.

### 1.2 La sécurité par défaut ou « Security by default »

Le règlement européen sur la protection des données pose une nouvelle règle, la « sécurité par défaut ». Cette règle impose à tout organisme de disposer d'un système d'information ayant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes (enregistrement, exploitation, administration, intégrité et mise à jour).
La sécurité du système d'information doit être assurée dans tous ses éléments, physiques ou logiques (contrôle d'accès, prévention contre les failles de sécurité, etc.).
Par ailleurs, cette règle implique que l'état de la sécurité du système d'information puisse être connu à tout moment, par rapport aux spécifications du fabricant, aux aspects vulnérables du système et aux mises à jour.

### 1.3 L'étude d'impact

Le règlement européen sur la protection des données consacre l'obligation par les organismes de réaliser des analyses d'impact relatives à la protection des données.
Cette obligation impose à tous les responsables de traitements et aux sous-traitants d'effectuer une analyse d'impact relative à la protection des données personnelles préalablement à la mise en œuvre des traitements présentant des risques particuliers d'atteintes aux droits et libertés individuelles.
Dans un tel cas, le responsable du traitement ou le sous-traitant, doit examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et apporter la preuve que le règlement sur la protection des données est bien respecté.

### 1.4 L'obligation de documentation ou « accountability »

Le règlement européen sur la protection des données met à la charge du responsable de traitement des règles d'accountability qui constituent la pierre angulaire de la conformité « ab initio » avec la règlementation en matière de données personnelles.
Il s'agit pour le responsable du traitement de garantir la conformité au règlement en adoptant des règles internes et en mettant en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.
Les mesures prévues en matière de données personnelles et d'accountability vont de la tenue de la documentation, à la mise en œuvre des obligations en matière de sécurité en passant par la réalisation d'une analyse d'impact.
Cette démarche anglo-saxonne connue sous le terme d'accountability est une obligation pour le responsable du traitement de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues du règlement.
Il devra démontrer qu'il a rempli ses obligations en matière de protection des données. C'est une charge de la preuve qui l'oblige à documenter l'ensemble des actions de sa politique de protection des données de manière à pouvoir démontrer aux autorités de contrôle ou aux personnes concernées comment il s'y tient.

## 2. La protection des données à caractère personnel traitées à des fins répressives

Les pratiques en matière pénale sont très différentes d'un Etat à l'autre. Jusqu'à présent il n'y avait pas de cadre commun aux services répressifs des Etats membres.
La directive relative à la protection des données à caractère personnel à des fins répressives (3) prévoit que chaque Etat membre doit suivre un cadre commun tout en développant sa propre législation qui devra reprendre toutes les règles de base en matière de protection des données notamment en matière de sécurité.
Ce n'est pas une chose aisée dans la situation actuelle avec les menaces terroristes qui pèsent en Europe.
Parmi les nouveaux éléments importants de cette directive, figure la nécessiter de se préoccuper en permanence de la protection des données et de la vie privée. A ce titre, toutes les institutions liées aux services répressifs devront se doter d'un « Data protection officer ».
Il ne devrait plus y avoir de collecte de données personnelles sans objectif clair, sans durée limitée et les justiciables auront des droits clairs, comme celui de savoir quelles sont les données collectées, à quelle fin, et combien de temps elles seront conservées.
La directive permet de prendre en compte les spécificités liées aux services répressifs tout en préservant les droits universels des citoyens justiciables. Ces deux textes font partis d'un même paquet « protection des données ».
La tâche n'a pas été simple de réformer la directive de 1995 et d'en faire un règlement unifié directement applicable par les Etats membres. C'est probablement une grande première que d'avoir réalisé un tel texte qui s'applique directement à toute l'Union européenne dans un domaine qui règlemente un droit aussi fondamental que la protection des données.
Le règlement entrera en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne. Ses dispositions seront directement applicables dans tous les Etats membres deux ans après cette date, soit en avril 2018.
En ce qui concerne la directive relative à la protection des données à caractère personnel à des fins répressives, les Etats membres auront deux ans pour transposer les dispositions qu'elle contient dans leur droit national.
Il s'agit là d'une grande avancée pour l'Union européenne tant pour les citoyens consommateurs que pour les entreprises.
Notes :
(1) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption du règlement général sur la protection des données.
(2) Règlement général sur la protection des données révisé le 8 avril tel qu'adopté par le Parlement européen le 14 avril 2016.
(3) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption de la directive relative à la protection des données à caractère personnel à des fins répressives… [Lire la suite]

---



Réagissez à cet article

Source : *Adoption du Paquet « Protection des données à caractère personnel »*