CLEMENTZ EUROMÉGRAS IDEAL

ENTRÉE EN VIGUEUR DU RÈGLEMENT GÉNÉRAL DE LA PROTECTION DES DONNÉES

# RGPD

## Ce qu'il faut savoir

L'Union Européenne a modifié sa règlemention en termes de protection des données. Ces modifications sont maintenant inscrites dans la loi et **seront introduites en Europe le 25 mai 2018.**

Le Règlement Général de la Protection des Données (RGPD) s'applique de manière très large et concerne la protection des données personnelles au sein de l'Union Européenne. Il définit un cadre strict à la collecte, au traitement et à la gestion des informations privées.

Désormais, les établissements publics et les entreprises doivent **intégrer la protection des données et des documents confidentiels dans la conception et l'organisation de leurs systèmes d'information sous peine de se voir infliger de lourdes amendes.**

Le RGPD s'adresse à tous les acteurs économiques, privés, publics ou sociaux, à savoir les :

- Entreprises
- Administrations publiques
- Services publics
- Associations

Lorsque l'on parle de données personnelles, on inclut les informations concernant les :

- Employés
- Clients & prospects
- Partenaires
- Fournisseurs

Le règlement s'applique pour toutes les données personnelles, quel que soit le support :

- Données personnelles sur **supports numériques**
- Données personnelles sur **supports papiers**

À l'heure où les volumes d'informations échangées et stockées croissent de façon exponentielle, il apparaît nécessaire et primordial de protéger les informations sensibles ou de les détruire de manière sécurisée.

Le RGPD a pour but de renforcer, de simplifier et d'unifier la protection des données à caractère personnel des individus dans les 28 pays membres de l'UE. **Il s'applique à tous les établissements publics ou privés qui collectent, traitent et stockent des documents confidentiels dont l'utilisation peut directement ou indirectement identifier une personne.** Il repose sur le droit fondamental inaliénable que constitue, pour chaque citoyen, la protection de sa vie privée et des ses données personnelles.

## Quatre directives principales du RGPD...

Le RGPD entrera en vigueur le 25 mai 2018 ; cela va arriver très vite, d'autant que **les nombreuses nouvelles règles vont obliger les établissements privés et publics à modifier en profondeur leurs systèmes de collecte et de traitement des informations confidentielles.** Ils doivent donc d'ores et déjà se tenir prêts. Parmi les nombreuses nouvelles règles, en voici quatre assez significatives :

| | |
|---|---|
|  | L'obligation pour les établissements de **demander l'autorisation de collecte de données à caractère personnel** auprès des individus. Ces derniers doivent donner leur autorisation de manière libre, spécifique et non ambiguë. Les établissements doivent également **être en mesure de démontrer que l'autorisation a effectivement été donnée.** |
|  | L'obligation pour les établissements de **mettre en œuvre toutes les règles techniques et d'organisation indispensables pour sécuriser les données à caractère personnel,** et ce dès la conception des produits, services ou systèmes exploitant cesdites données («Privacy By Design»). Le destructeur de documents joue ici un rôle primordial. |
|  | L'obligation de **déclarer dans les 72 heures, toute violation de données à caractère personnel** auprès des autorités compétentes et des personnes concernées. La violation des données peut prendre de nombreuses formes comme **la perte, la destruction accidentelle, la modification, le piratage, l'accès non autorisé, etc.** |
|  | L'obligation de **désigner un Responsable de la Protection des Données (RPD)** au sein de l'établissement ou de déléguer la protection des données à un organisme en charge du contrôle de la conformité des traitements (pour les établissements publics et les entreprises de plus de 250 salariés). |

Plus simplement, les établissements doivent veiller à ce que les données à caractère personnel soient en permanence — c'est à dire à tout moment et en tous lieux — sécurisées, **afin de lutter contre les risques de perte, de vol ou de divulgation.**

Pour connaître en détail toutes les directives du RGPD, consultez le site de la Commission Européenne : http://tinyurl.com/hl2ax9k

# Quels risques en cas de non respect de la réglementation ?

Les obligations du RGPD supposent qu'**une entreprise doit à tout moment savoir de quelles données elle dispose, où elles sont localisées, l'objectif de leur collecte, leur mode de gestion, leur stockage, leur sécurisation, leur éventuel transfert, effacement ou destruction.** Au delà du traitement administratif des données, les différentes obligations du RGPD imposent aux entreprises une approche résolument proactive en intégrant la sécurité au cœur de leurs systèmes d'information, sous peine de lourdes sanctions.

Pénalités allant jusqu'à **20 millions d'euros** ou 4% du CA annuel global de l'entreprise

En cas d'infraction, les entreprises s'exposent à des sanctions et **des amendes pouvant atteindre 4% du chiffre d'affaires global annuel** — dans une limite de 20 millions d'euros — ce qui représente un coût considérable. Le RGPD n'est donc à pas à prendre à la légère !

De même, en principe, tout individu qui a subi un préjudice suite à une violation des nouvelles règles peut faire valoir un droit d'indemnisation après des personnes ou entités qui contrôlent ou traitent les données à caractère personnel en question. Vu les pénalités prévues par le RGPD pour une infraction, surtout lorsqu'il s'agit d'une violation de données, **les entreprises doivent s'efforcer de minimiser les demandes d'indemnisation potentielles.**

# Se conformer au RGPD en deux étapes

Pour se conformer au RGPD, **les établissements privés et publics doivent d'ores et déjà analyser de manière approfondie l'état actuel de leurs systèmes d'information et les process existants** afin d'établir un budget et de planifier la mise en place des ressources humaines, informatiques et matérielles nécessaires avant l'entrée en vigueur du règlement, le 25 mai 2018.

## Étape 1 Analyser, planifier et modifier les process liés aux données à caractère confidentiel...

| | | | | | |
|---|---|---|---|---|---|
| **Analyser et cartographier les données** à caractère personnel sur supports numériques ou papiers et évaluer les risques à tous les niveaux d'exploitation desdites données. | **Modifier le système d'information** et mettre en place des règles techniques et d'organisation pour assurer la sécurisation des données à caractère personnel. | **Appliquer les nouvelles règles concernant le consentement libre** et non ambigu pour la collecte et le traitement de données à caractère personnel. | **Mettre en place des procédures de notification en cas de violation** de données (en incluant la capacité de détection et de réaction) et réaliser des tests d'intrusion. | **Envisager de désigner un Responsable de la Protection des Données** garant de la conformité des pratiques en matière de collecte et de traitement des données. | **Former et sensibiliser l'ensemble du personnel** aux notions de risque, de confidentialité et de responsabilité qui lui incombe. Tout le monde est concerné ! |

Les supports (numériques ou papiers) contenant des données confidentielles devenues obsolètes ou tout simplement inutiles ne doivent jamais être jetés à la poubelle ; **ils doivent être scrupuleusement détruits avec un matériel adapté, afin de prévenir les risques de vol, de divulgation ou d'utilisation frauduleuse par des tiers.**

## Étape 2 S'équiper de matériels dédiés à la destruction sécurisée de données à caractère confidentiel...

### Données personnelles sur **supports papiers**

Un destructeur de documents permet de détruire de manière sécurisée les papiers contenant des données personnelles et confidentielles.

La norme DIN 66399 définit les niveaux de sécurité P-1 à P-7 qui correspondent à la taille des particules de papier qui résultent de la destruction. Plus petites sont les particules, plus haut est le niveau de sécurité.

Les destructeurs de documents IDEAL existent en de nombreux modèles adaptés à une utilisation individuelle, collective ou industrielle.

Ils peuvent également détruire les cartes magnétiques ou à puces et dans une moindre mesure des disquettes et des CD/DVDs.


### Données personnelles sur **supports numériques**

Un destructeur de médias permet de détruire de manière sécurisée et intensive les supports optiques (CD/DVDs) ou magnétiques (disques durs) contenant des données personnelles et confidentielles.

Effacer simplement les données n'est plus un gage de sécurité.

La destruction physique de ces supports est nécessaire afin d'empêcher toute reconstitution des données qu'ils contiennent.

Les destructeurs de médias IDEAL ont été spécialement conçus à cette fin, avec des niveaux de sécurité élevés (H-3 et O-5) selon la norme DIN 66399.


**À propos de CLEMENTZ-EUROMÉGRAS :** filiale du groupe allemand IDEAL Krug & Priester — l'un des leader mondiaux sur le marché des destructeurs de documents — la société CLEMENTZ-EUROMÉGRAS, en activité depuis plus de 50 ans, n'a cessé d'évoluer en proposant à ses clients des produits de haute qualité dans de nombreux domaines d'activités. CLEMENTZ-EUROMÉGRAS est aujourd'hui le leader de la distribution sur le marché français de solutions professionnelles pour la destruction de documents papiers.

CLEMENTZ EUROMÉGRAS

IDEAL

CLEMENTZ-EUROMÉGRAS • 5a Rue de Picardie - Reichstett • BP 33432 • 67455 MUNDOLSHEIM Cedex
Tél. 03 88 20 58 55 • Fax 03 88 81 98 84 • info@clementz-euromgras.com • www.clementz-euromegras.com

RC STRASBOURG B 598501518
Imprimé en France 03/2017