BERSOT AVOCATS
RESEAU LEMAN LEXINT

Barreau de Thonon-les-Bains, du Léman & du Genevois

Règlement général sur la protection des données (RGPD)

Contexte juridique

- Nouveau texte de référence dans l'UE
- Remplace une directive de 1995
- Consacre et renforce les grands principes de la loi « Informatique et Libertés » de 1978
- Entrée en vigueur le 25 mai 2018
- Règlement : obligatoire et applicable directement dans les Etats membres (=/= directive)

Sanctions

- Amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent (montant le plus élevé)
- Attitude nuancée de la CNIL dans les premiers mois suivant l'entrée en vigueur du RGPD :
  - Principes fondamentaux : contrôle rigoureux
  - Nouvelles obligations : contrôle « préventif » dans un esprit d'accompagnement des entreprises de bonne foi
  - **= > En priorité : se mettre en conformité avec les règles essentielles**

I. Champ d'application

Qui est concerné ?

« Toute entité manipulant des données personnelles concernant des Européens » : très large

- Entreprises situées sur le continent européen + entreprises hors UE qui manipulent des données personnelles européennes
- Toute forme sociale (entreprise, association…), **peu important la taille ou le secteur d'activité**

Notion de « donnée personnelle »

« une information se rapportant à une personne physique identifiée ou identifiable »

- Nom
- Photographie
- Adresse IP
- Numéro de téléphone
- Identifiant de connexion informatique
- Adresse postale
- Empreinte
- Enregistrement vocal
- Numéro de sécurité sociale
- Etc

Notion de « traitement »

Le règlement s'applique :

- Au traitement de données personnelles automatisé en tout ou partie

- Au traitement non automatisé de données personnelles contenues ou appelées à figurer dans un fichier

Grands principes

- Données traitées de manière licite, loyale et transparente
- Collectées pour des finalités déterminées
- Limitées à ce qui est nécessaire : principe de minimisation
- Exactes et tenues à jour
- Durée raisonnable
- Garantir une sécurité appropriée

= > Ces principes s'appliquent dès lors que les données d'une personne sont collectées (internaute, client, employé, fournisseur…)

Nouvelles mesures

- **Intégrer les concepts de protection des données dès la conception de nouveaux produits ou services**
- **Se conformer au principe d'accountability qui impose à l'entreprise de se pré-constituer la preuve de sa conformité**
- Notifier à la CNIL toute violation de données à caractère personnel
- Désigner un Délégué à la protection des données si nécessaire (voir plus loin)
- S'assurer de la conformité des sous-traitants à la réglementation (voir plus loin)

II. Droits des personnes concernées, obligations des entreprises

Consentement de l'internaute

- Fin des cases d'acceptation cochées par défaut
- Opt-in : l'internaute doit cocher lui-même la case
- Attention : dispositions particulières pour le consentement des enfants
- Attention en matière de collecte de données dites « sensibles » (origine raciale ou ethnique, convictions religieuses, appartenance syndicale, opinions politiques…)

<u>Pensez-y</u> : dès lors que votre Site internet propose un formulaire de contact, vous collectez des données personnelles et devez en informer l'utilisateur et recueillir son consentement

Information de l'utilisateur

- Information claire et transparente, notamment :

  - Identité et coordonnées du responsable du traitement et le cas échéant du représentant du responsable du traitement
  - Les finalités du traitement et la base juridique du traitement
  - Durée de conservation des données
  - Existence des droits de l'internaute (droit d'accès, rectification, d'effacement des données, droit de retirer son consentement, de s'opposer à la portabilité des données…)
  - Etc

Droits à…

- La rectification des données inexactes
- L'effacement (droit à l'oubli) : l'internaute doit justifier d'un motif (données plus nécessaires au regard de la finalité, retrait du consentement, opposition au traitement). Attention : doit se concilier avec les autres obligations légales (archivage par exemple)
- La limitation du traitement : l'internaute doit justifier d'un motif (données inexactes, traitement illicite…)
- La portabilité des données : droit pour l'internaute de recevoir les données à caractère personnel le concernant et de les transmettre à un autre responsable du traitement
- L'opposition : données traitées à des fins de prospection (sans motif)
- Ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage = > A atténuer
- **= > Mettre en place / mettre à jour les formulaires d'information et d'adhésion**

BERSOT AVOCATS
RESEAU LEMAN LEXINT

Barreau de Thonon-les-Bains, du Léman & du Genevois

III. Les acteurs en interne

Responsable du traitement	Délégué à la protection des données
Obligatoire de fait (sous-traitance possible mais ne dégage pas le donneur d'ordres de sa qualité de responsable du traitement)	Obligatoire dans certains cas, conseillé dans les autres
Personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel = organe dirigeant	Membre du personnel du responsable du traitement ou de son sous-traitant ou **prestataire externe**
Met en œuvre les mesures techniques et organisationnelles appropriées pour être en mesure de démontrer que le traitement est effectué conformément au RGPD	Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés sur les droits et obligations du RGPD Point de contact : pour les personnes concernées, pour l'autorité de contrôle

En pratique : 2 personnes différentes

Le sous-traitant

= Toute personne qui traite des données personnelles pour le compte du responsable du traitement (prestataire informatique, comptable, éditeur de logiciel…)

- S'assurer qu'il présente des garanties suffisantes
- Existence/élaboration d'un contrat/d'un avenant

➢ **Rapprochez-vous de vos sous-traitants afin de faire le point sur ces questions et conserver les écrits**

IV. Se préparer efficacement : les étapes à respecter

1. Désigner un pilote

Chef d’orchestre : mission d’information, de conseil et de contrôle en interne

= > Délégué à la protection des données le cas échéant

2. Cartographier les risques

Qui ?	Cordonnées du responsable du traitement et du délégué à la protection des données Liste des sous traitants
Quoi ?	Catégories de données traitées Identifier les données pouvant être sensibles
Pourquoi ?	Finalité de la collecte ou du traitement des données
Où ?	Lieu où les données sont hébergées Pays dans lesquels les données sont transférées
Jusqu'à quand ?	Durée de conservation des données
Comment ?	Mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données (mot de passe, bureaux fermés à clef…)

<u>Pensez-y</u> : en qualité d'employeur, vous collectez les données personnelles de vos salariés !

3. Prioriser les actions à mener

- Collecte des données strictement nécessaires uniquement
- Base juridique sur laquelle se fonde le traitement
- Mentions d'informations
- Surveillance des sous-traitants
- Modalités d'exercice des droits des personnes concernées (rectification, retrait du consentement…)
- Mesures de sécurité mises en place

!! Vigilance renforcée sur certains points (données sensibles, surveillance à grande échelle, transfert données hors UE…)

4. Gérer les risques et s’organiser

En cas de risques élevés : effectuer une analyse d’impact

Qu’est ce qu’un risque élevé ? 9 critères

Organiser la mise en conformité

5. Documenter la conformité

Registre des traitements : non obligatoire mais conseillé pour se pré constituer une preuve

Analyses d'impact

Encadrement des transferts de données hors UE

Informations des personnes (mentions d'informations, recueil du consentement, procédures mises en place pour l'exercice des droits)

Contrats (sous-traitants, procédures internes en cas de violation des données, preuve du consentement)