RGPD ORLY?

Da Règlement Général sur la Protection des Données

De quoi parle t’on ?

- D’un **règlement** européen ;
- Entré en vigueur en Mai 2016, en application à partir de Mai 2018 ;
- S’appliquant à tout responsable de traitement ayant une activité dans l’Union ou ciblant une personne de l’Union ;
- Relatif à la protection des personnes à l'égard du **traitement** des données à **caractère personnel** et à leur libre circulation.

Règlement : acte juridique de l'Union obligatoire dans tous ses éléments dès son entrée en vigueur, ne pouvant donc s'appliquer de manière incomplète ou sélective.

Traitement ?

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.

La collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Art. 4

Donnée à caractère personnel ?

- « Toute information se rapportant à une personne physique identifiée ou identifiable » :
  - Nom, prénom, adresse, courriel, … ;
  - Mais aussi adresse IP, données d'usage d'une application, enregistrement de voix, vidéo de drone, … ;
  - Et également ensemble de données pouvant par croisement permettre l'identification de la personne.

Art. 4

Données sensibles 🚫

- Les données relatives à la santé des individus ;
- les données concernant la vie sexuelle ou l'orientation sexuelle ;
- les données qui révèlent une prétendue origine raciale ou ethnique ;
- les opinions politiques, les convictions religieuses, philosophiques ou l'appartenance syndicale ;
- les données génétiques et biométriques utilisées aux fins d'identifier une personne de manière unique.

Recueil et utilisation interdite sans consentement exprès de la personne.

Nécessite une autorisation CNIL, voire le recours à un hébergeur de données de santé certifié pour les données de santé à caractère personnel.

Principes relatifs au traitement

- Licite, loyal et **transparent** au regard de la personne concernée ;
    - Implique le consentement au traitement, la nécessité à l'exécution d'un contrat ou à une obligation légale ;
- Données collectées pour des **finalités déterminées**, explicites et **légitimes**, et non traitées ultérieurement d'une manière incompatible avec ces finalités ;
- Conservées pour une durée n’excédant pas celle nécessaire au regard des finalités de traitement ;
- Traitées de façon à garantir une **sécurité** appropriée des données.

- Licite : + mission d’intérêt public ou sauvegarde des intérêts vitaux
- Donc données minimisées

Art. 5

Le consentement est…

- Manifestation de volonté libre — ne peut être forcé par l’utilisation du service ;
- Spécifique — lié à une ou plusieurs finalités ;
- Éclairé — la personne doit être informée, y compris des types de données collectées et utilisées ;
- Univoque — nécessite une déclaration de la part de la personne ou un acte positif clair, que ne sont pas l’inactivité ou le simple fait d’utiliser le service ;
- Et peut être retiré à tout moment.

Case à cocher pré-cochée

Art. 4

Responsabilités ?

- Le responsable du traitement est responsable du respect des principes précédents…
- Et est en mesure de démontrer qu’ils sont respectés ;
- Il doit garantir un niveau de sécurité adapté au risque ;
- Il doit notifier à la CNIL toute violation de données dans les 72h.
- À partir de 250 salariés, la tenue d’un registre des activités de traitement est obligatoire.
- Le sous-traitant doit respecter le règlement, et le contrat le liant doit prévoir objet, durée, nature et finalités du traitement.

« Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. »

Des droits pour le citoyen

- Droits d’accès et de rectification — y compris retrait du consentement ;
- Droit à l’effacement et à l’oubli ;
- Droit à la portabilité des données, dans un format structuré, couramment utilisé, lisible par machine et interopérable ;
- Être notifié en cas de violation des données à caractère personnel.

Anonymisation

- Anonymisation : rendre impossible toute identification des personnes au sein de jeux de données, y compris par corrélation ou inférence :
  - Agrégation, randomisation, etc.
- Pseudonymisation : l'identification des personnes reste possible par recours à des informations supplémentaires :
  - Utilisation d'un numéro de classement, hachage cryptographique des données de l'individu.

Anonymisation

- Les données anonymisées sortent du cadre du règlement ;
- Les données pseudonymisées sont toujours considérées comme données personnelles ;
    - C’est néanmoins un bon moyen de protection des données lors du traitement.

Quelles sanctions ?

- Principe de sanctions graduelles entrainées par la CNIL :
  - Avertissement ou mise en demeure de l'entreprise accompagné d'un rappel des règles concernant la mise en conformité ;
  - Injonction, ordre de cessation immédiate des violations constatées ;
  - Limitation ou suspension temporaire des traitements ou des flux de données ;
  - Sanctions administratives pour les entreprises qui n'ont pas respecté l’injonction :
    - Amendes effectives, proportionnées et dissuasives, pouvant aller jusqu’à 4 % du CA mondial de l’entreprise.

5 amendes à ce jour en France — démarchage téléphonique abusif, accès à des données d’autres clients, vidéo surveillance, accès à des pièces justificatives téléchargées par bidouille de l’URL, Google.

Europe : 175 amendes

DPO ?

- Membre du personnel du responsable du traitement ou du sous-traitant, ou exerçant ses missions sur la base d'un contrat de service ;
- Compétent dans le domaine du droit ;
- Obligatoire pour les traitements à « grande échelle » ;
- Conseille, contrôle le respect du règlement, point de contact avec l’autorité de contrôle (la CNIL).

Documentation de la conformité

- Les traitements : registre des traitements, analyses d’impact pour les traitements susceptibles d'engendrer des risques élevés, encadrement des transferts hors UE ;

- Les mentions d’information des personnes, les modèles de recueil du consentement, les procédures d’exercice des droits individuels ;

- Les contrats avec les sous-traitants, les procédures internes en cas de violations de données.

La déclaration CNIL

La loi Informatique et Libertés précédemment en vigueur obligeait les entreprises procédant à des traitements de données à effectuer des déclarations à la CNIL.

Ce n’est plus le cas.

(Mais chaque entreprise doit être en mesure de prouver la conformité de ses traitements aux dispositions du RGDP.)

Q&A

Quid des logs ?

- Les logs en tout genre font partie des données, et les adresses IP sont des données personnelles ;
- Néanmoins, le traitement de données aux fins de garantir la sécurité du réseau et des informations et considéré légitime ;
- Il conviendra toutefois d'en protéger l'accès et de ne pas les conserver éternellement.

Considération 49, Art. 5

Combien de temps peut-on garder les données ?

- Le moins longtemps possible 😄
- À déterminer en fonction des finalités de traitement et des contraintes légales ;
- Le registre des activités de traitement se doit de mentionner les délais prévus pour l'effacement des différentes catégories de données.

Art. 5, Art. 30

Le bouton « se connecter » sur l'admin des comptes est-il RGPD ❤️ ?

- Chaque collaborateur ne doit pouvoir accéder qu’aux informations dont il a besoin, avec les droits dont il a besoin, ce qui peut impliquer une gestion des habilitations ;

- La journalisation des accès aux données personnelles serait la bienvenue comme moyen d’audit.

« le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement » — Art. 24

Comment informer l’utilisateur ?

- Lors de la collecte des données si collecte directe, dès que possible en cas de collecte indirecte ;
- L’information doit être facile d’accès ;
- L’information doit être détaillée sur les finalités et les modalités de conservation.

Par où commencer ?

- Identifier les données personnelles (lieu de stockage, période de rétention),
- Et les traitements les manipulant.
- Toutes les équipes sont concernées, car nous manipulons tous des données utilisateurs — y compris l'infra 😛
- Commencer à se poser la question pour tous les nouveaux développements.

Quid des Rich ?

Références

- **Le règlement : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679**
- Lignes directrices sur le consentement : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf
- Avis sur les Techniques d'anonymisation : https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr.pdf
- GDPR enforcement tracker : https://www.enforcementtracker.com
- Registre des traitements simplifié : https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods