LE GDPR (GENERAL DATA PROTECTION REGULATION) OU RGPD (RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES)

Le GDPR c'est quoi ?

Le **GDPR (General Data Protection Regulation)**, aussi désignée sous son acronyme français **RGPD (Règlement général de protection des données)** a été publié en mai 2016.
Il s'agir du nouveau règlement européen sur la protection des données et entre en application le 25 mai 2018 et concerne toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens. Il s'agit d'un règlement européen, le texte entre donc en application directement et en même temps dans tous les Etats membres de l'Union européenne, sans transposition dans une loi locale.

Objectifs de la règlementation

Le GDPR poursuit plusieurs objectifs ambitieux :

- **Uniformiser au niveau européen la réglementation sur la protection des données.**
- **Responsabiliser davantage les entreprises en développant l'auto-contrôle.**
- **Renforcer le droit des personnes (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).**

Les **DCP concernées – Données à caractère personnel**, sensibles sont, selon le GDPR, « toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement »

L'immense majorité des entreprises Proposant des **biens et services** sur le marché de l'UE **Collectant et traitant des données à caractère personnel sur les résidents de l'UE** sont donc concernées par les dispositions du GDPR:

Périmètre

Le GDPR concerne uniquement la protection des données personnelles rattachées à des personnes physiques. Ce qui signifie que la RGPD ne s'applique pas aux entreprises ne traitant que des données relatives à des personnes morales, **sauf si celles-ci sont amenées à collecter des données sur des représentants des personnes morales**.

LES BASES

Le consentement

Le consentement des individus quant à la collecte et au traitement des données à caractère personnel les concernant doit être explicite et « positif ». Ce consentement pourra être retiré à tout moment par les individus le demandant. Les entreprises faisant du traitement de données devront, être en mesure de prouver le recueil de ce consentement en cas de contrôle de la CNIL.
Sur le thème du consentement, le GDPR prévoit une autre évolution majeure : l'encadrement du profilage. Il notamment le recueil d'un consentement explicite de la part des personnes. Le profilage sera par ailleurs soumis à compter de mai 2018 au droit d'opposition.

Le droit des personnes

- Un droit d'accès facilité pour tous les utilisateurs.
- Un droit l'oubli pour tous les utilisateurs. Les entreprises disposent d'un délai réduit d'un mois, et non plus de deux mois, pour supprimer les données à la suite d'une demande.
- Un droit à la limitation du traitement, applicable dans quelques cas précis.
- Un droit à la portabilité des données. Il s'agit d'un nouveau droit qui permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers

Il revient aux entreprises de garantir le droit des personnes par la mise en place de mesures, d'outils et de processus appropriés.

La transparence

Les entreprises doivent – et ce dès la phase de collecte – fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données seront traitées. Ces informations devront être fournies de façon concise, compréhensive et accessible par tous.

La responsabilité

Le GDPR vise à responsabiliser davantage les entreprises dans leur traitement des données à caractère personnel:

- L'obligation faite aux entreprises de documenter toutes les mesures et procédures en matière de sécurité des DCP.
- Le renforcement des mesures de sécurité.
- La mise en avant du principe de « Privacy By Design ».
- L'encadrement des sous-traitants.
- La notification en cas de faille de sécurité (data breach).
- L'obligation de désignation d'un Data Protection Officer (en français : « Délégué à la Protection des Données »).
- La suppression de l'obligation de déclaration préalable à la CNIL.

GDPR et ESI

Périmètres qui peuvent concerner ESI

Une partie des obligations GDPR peut être couverte par de l'organisation, du management et des adaptations contractuelles. L'éditeur peut proposer des outils pour faciliter une partie de ces obligations et doit couvrir ce que le client ne peut absolument pas faire autrement que par le logiciel.

Fonctions communes fournies en standard dans le produit

- Mémorisation de l'état par rapport au GDPR:
- Traces, résiliations, saisies et consultations
- Gestion et sécurisation forte des accès aux bases de données
- Sécurisation des accès Web
- Renforcement des protections sur la perméabilité des logiciels avec la participation de nos clients.

Les packs GDPR (Fonction du niveau souhaité par le client)

HSL1

- Encryptage de la Base de données
- Protection des données en cas de d'extraction ou de mirroring par des outils externes tels que VMWare et assimilés avec clé de chiffrement.
- Encryptage des données sur la réplication, les backups, les export via DBM, avec administration des clés de chiffrement.
- Encryptage des canaux de communication UGI.
- Sécurisation étendue des accès systèmes et logiciels à la BDD, cloisonnement des droits BDD par application M1.

HSL2

- Nouvelles traces utilisateurs:
  - En réussite et échec avec l'horodatage, l'identifiant, l'emplacement...
  - Traçabilité de l'accès en visualisation des données:
  - Traçabilité des accès aux outils d'export/ import:
- Alerte d'utilisation de masse de données personnelles
- Cryptage des Vidéo enregistrées sur V1 et AV1.
- Cryptage des audio enregistrées sur RC1 et IPBX

Contact
tel : +33 (0) 4 93 94 84 10
mail : info@esigroup.eu
www.esigroup.eu

ESI GROUP
Le Sun Eden
362, Avenue du Campon
06110 Le Cannet

version 1.0.1.0518