Le RGPD

Glossaire

Règlement général sur la protection des données (RGPD)	Le Règlement général sur la protection des données est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Depuis 2018, ses dispositions sont directement applicables dans l'ensemble des 27 États membres de l'Union européenne, plus le Liechtenstein, la Norvège et l'Islande.
Anonymisation	Méthode permettant de traiter les données personnelles pour qu'elles ne permettent pas d'identifier la personne concernée. Cela nécessite une autorisation spécifique.
Commission nationale de l'informatique et des libertés (CNIL)	La CNIL est une autorité administrative indépendante, c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.
Responsabilité	Principe selon lequel les organisations doivent assumer leurs responsabilités. Elles doivent ainsi prouver que leur traitement des données est conforme au RGPD et qu'elles prennent les mesures obligatoires (tenue d'un registre des traitements par exemple).
Conformité au RGPD	Les entreprises conformes au RGPD respectent l'ensemble des directives inscrites dans ce dernier.
Personnes concernées	Personnes identifiables concernées par les données traitées. Le RGPD vise à les protéger efficacement contre l'utilisation frauduleuse de leurs données.
Données sensibles	Cela englobe les informations concernant l'origine ethnique, la religion ou la santé, qui bénéficient d'une protection accrue. Leur traitement est interdit, sauf obligation légale.

Le RGPD

Glossaire

Cookie	Il s’agit d’un petit fichier texte déposé sur le disque dur de votre ordinateur, tablette ou smartphone quand vous visitez un site Internet. Il y a différents types de cookies : certains servent à assurer le bon fonctionnement du site, d’autres à suivre l’activité des visiteurs sur un site ou sur Internet.
Règlementation sur les cookies	La loi sur les télécommunications permet aux utilisateurs de contrôler les cookies pouvant être déposés sur leur appareil.
Violation des données	On parle de violation des données quand celles-ci sont divulguées involontairement par l’organisation qui les a collectées.
Registre des violations des données	Le RGPD oblige les entreprises à enregistrer toutes les violations des données dans un registre dédié qui doit mentionner, entre autres, la nature et la gravité des faits, ainsi que les mesures prises pour y remédier.
Limitation des finalités	Les organisations qui collectent des données doivent avoir pour cela un *motif légitime* précisé en amont et expliqué clairement aux personnes concernées.
DPIA (analyse d’impact)	Cet instrument permet aux entreprises d’identifier quels sont les risques pour la vie privée avant même de procéder au traitement des données. Elle est obligatoire dans certains cas.
Cryptage	Le cryptage assure la protection des données en les rendant illisibles. Les données doivent être décryptées pour pouvoir être lues ou traitées.
Comité européen de la protection des données (CEPD)	Le Comité européen de la protection des données est un organe européen indépendant qui veille à ce que les règles relatives à la protection des données soient appliquées uniformément dans l'Espace économique européen. Il englobe tous les États membres de l'Union européenne, plus le Liechtenstein, la Norvège et l’Islande

Le RGPD

Glossaire

Délégué à la protection des données (DPD)	Le délégué à la protection des données veille à ce que son entreprise respecte le RGPD. Il travaille en toute indépendance et sa nomination est parfois obligatoire.
Bases	Les entreprises qui traitent des données doivent avoir pour cela un *motif légitime* qui s'appuie sur une des six bases suivantes : nécessité contractuelle, intérêt public, respect d'obligations légales, intérêt légitime, intérêt vital et consentement.
Authentification multi-facteurs (MFA)	Accès sécurisé qui nécessite au moins deux étapes pour pouvoir se connecter à un appareil ou un système (par exemple : un mot de passe plus une question de sécurité).
Conseil d'État	Cet organe indépendant et impartial doit traiter les plaintes émises par les agences gouvernementales, notamment la CNIL.
Données non personnelles	Données qui ne permettent pas à elles seules d'identifier, de suivre ou de localiser une personne. Il peut s'agir par exemple des adresses IP.
Opt-out/opt-in	Le RGPD a remplacé le principe de l'opt-out par le principe de l'opt-in. Pour résumer, il est interdit de cocher par défaut les cases destinées à indiquer l'intérêt des personnes. Les visiteurs doivent activement cocher les cases pour consentir au traitement de leur données et à divers envois.
Données à caractère personnel/ Données personnelles	Données qui permettent d'identifier, de suivre ou de localiser une personne. Cela inclut l'adresse e-mail, la date de naissance, ou encore le numéro de sécurité sociale.
Protection des données par défaut	L'idée est de définir les paramètres standard d'un site Internet dans le but de protéger au maximum les données. Les visiteurs vont par exemple devoir donner activement leur consentement, qui ne sera pas automatique.

Le RGPD

Glossaire

Protection des données dès la conception	Lors de la création ou de la refonte d'un site, on va avant tout privilégier la protection des données. On va donc collecter le moins de données possible et les protéger au maximum.
Responsable de la protection de la vie privée	Les organisations peuvent nommer un responsable de la protection de la vie privée, mais cela n'est pas obligatoire. Cette personne est chargée de gérer les données personnelles, de conseiller les employés en matière de protection des données, et d'organiser des formations pour renforcer les connaissances en interne.
Droits relatifs à la vie privée	Les personnes concernées peuvent invoquer huit droits : droit d'accès, droit à l'oubli, droit de rectification et d'ajout, droit à la portabilité des données, droit à la limitation du traitement, droit d'opposition, droit à l'information et droit à une intervention humaine.
Déclaration de con identialité	Document destiné à informer les personnes concernées (clients, employés, partenaires commerciaux) sur le traitement de leurs données personnelles. Les organisations doivent indiquer quelles sont les données traitées, dans quel but, et elles doivent préciser si ces données sont transmises à des tiers.
Pseudonymisation	Méthode visant à sécuriser les données à l'aide d'un algorithme qui va remplacer les données personnelles par des données cryptées illisibles (le pseudonyme). Le processus peut être inversé en appliquant à nouveau un algorithme pour décrypter les données et identifier une personne.
Certi icat SSL	SSL est l'acronyme de *secure sockets layer*. Les organisations qui traitent des données personnelles doivent protéger leur site Internet à l'aide d'un certificat SSL. Ce petit fichier de données va enregistrer tous les échanges entre le site et le visiteur.
Données sur la criminalité	Données relatives à des condamnations et des infractions. Le traitement de ces données est interdit, sauf obligation légale.

Le RGPD

Glossaire

Devoir de responsabilité	Le devoir de responsabilité oblige les organisations à démontrer que le traitement des données respecte les règles établies par le RGPD et que les mesures nécessaires ont été prises (tenue d'un registre des traitements par exemple).
Sous-traitant	Entité qui traite les données pour le compte d'une autre organisation. Par exemple : une agence marketing ou un cabinet comptable.
Contrat de sous-traitance	Les entreprises responsables du traitement des données et les entreprises sous-traitantes doivent signer un contrat, faute de quoi elles peuvent être accusées d'enfreindre la réglementation.
Registre des traitements	Document dans lequel les organisations consignent toutes les informations relatives au traitement des données. Cela inclut le type de données traitées, leur durée de conservation et les mesures de protection prises. Il est obligatoire dans de nombreux cas.
Responsable du traitement des données	Il s'agit de l'organisation qui détermine les finalités du traitement des données. Elle reste responsable, même si elle a confié le traitement des données à une autre entité.
Gestionnaire de mots de passe	Coffre-fort numérique dans lequel sont enregistrés les identifiants et mots de passe. Ces systèmes s'appuient sur le cryptage pour stocker les données en toute sécurité.