Règlement général sur la protection des données
CEJMA
BTS SIO 1

Le règlement général sur la protection des données (RGPD)

1. Les personnes concernées

Le règlement général sur la protection des données constitue le texte de référence en matière de protection des données à caractère personnel.
Il s'applique à toute organisation, publique et privée, qui traite des données personnelles de résidents de l'Union européenne.

2. Le droit des personnes

Toute personne a un droit d'accès à ses données. Elle peut les rectifier et s'opposer à leur utilisation.

Droit à la portabilité des données	Toute personne peut récupérer, sous une forme réutilisable (format lisible sur tout ordinateur), les données qu'elle a fournies à une organisation. Elle peut les transférer à un tiers.
Droit à l'oubli	Toute personne peut demander l'effacement de ses données et leur déréférencement.
Droit à la notification	En cas de violation de la sécurité des données comportant un risque élevé pour les personnes, le responsable du traitement doit avertir ces dernières rapidement. Il doit également le notifier à la CNIL dans les 72 heures.

3. Les obligations des organisations

Obligation générale de sécurité et de confidentialité	Le responsable du traitement des données doit mettre en œuvre les mesures de sécurité des locaux et des systèmes d'information et fixer une durée raisonnable de conservation des informations personnelles.
Obligation d'information	L'entreprise qui détient des données personnelles doit informer la personne concernée de : • l'identité du responsable du fichier ; • la finalité du traitement des données ; • le caractère obligatoire ou facultatif des réponses ; • les droits d'accès, de rectification, d'interrogation et d'opposition ; • la portabilité des données. L'objectif de la collecte d'informations doit être précis, et les données en accord avec cette finalité.
Transferts de données à l'extérieur de l'UE	Les transferts de données à l'extérieur de l'UE ne sont plus interdits, à condition d'assurer un niveau de protection suffisant (voir chapitre V du RGPD).
Délégué à la protection des données	Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au RGPD au sein de l'organisation. Il doit : • informer et conseiller le responsable du traitement des données et ses employés ; • contrôler le respect du règlement européen et du droit français en matière de protection des données ; • conseiller l'organisation sur la réalisation d'une analyse d'impact et en vérifier l'exécution.
Autres obligations	Toutes les organisations de plus de 250 salariés doivent tenir un registre des activités des traitements, sauf si ces traitements sont occasionnels.

4. La base légale des traitements des données

Le RGPD prévoit six bases légales d'application.

La sauvegarde des intérêts vitaux	Par exemple à des fins humanitaires, lorsque le traitement des données est nécessaire pour suivre des épidémies et leur propagation.
L'intérêt public	Le traitement est nécessaire à l'exécution d'une mission de service public. En cas de menace contre la sécurité publique, le DPO peut transmettre à une autorité compétente des données à caractère personnel.
Le contrat	Le traitement des données personnelles est nécessaire à l'exécution du contrat auquel les personnes ont consenti.
Le consentement	L'acceptation du traitement des données personnelles doit faire l'objet d'un consentement exprès de la personne (case à cocher, clic, etc.).
L'intérêt légitime	L'organisation a un intérêt à traiter des données qui est justifié, équilibré et ne porte pas atteinte à la vie privée.
L'obligation légale	Le traitement des données personnelles est rendu obligatoire par un texte de loi.

La CNIL

1. La mission de la CNIL

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité indépendante chargée de veiller à ce que l'informatique ne porte pas atteinte aux libertés fondamentales des citoyens français.
La loi Informatique et Libertés, votée en 1978 et renforcée par la RGPD, encadre les questions liées à la protection de la vie privée en ligne. Elle définit les missions de la CNIL.
La CNIL a un rôle de conseil auprès des entreprises, des autorités publiques et du grand public. Elle fournit ainsi à l'ensemble des acteurs concernés des outils et des référentiels, pour se mettre en conformité avec le RGPD.
La CNIL est dotée d'un pouvoir de sanction renforcé avec la mise en place du RGPD : les sanctions administratives peuvent comporter des amendes jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise.

2. Les cinq principes fondamentaux définis par la CNIL

Le principe de finalité	Le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime.
Le principe de proportionnalité et de pertinence	Les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier.
Le principe d'une durée de conservation limitée	Il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. La durée de conservation précise doit être fixée en fonction du type d'information enregistrée et de la finalité du fichier.
Le principe de sécurité et de confidentialité	Le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations.
Les droits des personnes	L'organisme collectant des données doit informer les individus concernés des finalités de la collecte et leur permettre d'exercer leurs droits.