NOM: PRÉNOM: CLASSE:

MR ROLIN 2025

[DIVERS] RGPD

Objectifs

- Définir ce qu'est une donnée personnelle et une donnée sensible.
- Comprendre les obligations légales du RGPD dans le cadre du métier de technicien.
- Savoir appliquer une méthodologie sécurisée pour récupérer et manipuler des données.
- Identifier les risques (juridiques, éthiques, techniques) liés à une mauvaise manipulation.
- Être capable d'expliquer les droits des utilisateurs et de les respecter.

Qu'est-ce que le RGPD ?

Le RGPD (Règlement Général sur la Protection des Données – en anglais GDPR) est une réglementation européenne entrée en vigueur le 25 mai 2018.

Son but est de protéger la vie privée des citoyens en leur donnant plus de contrôle sur leurs données personnelles et en imposant des règles strictes aux entreprises, administrations et professionnels qui manipulent ces données.

En Belgique, c'est l'Autorité de Protection des Données (APD) qui est chargée de surveiller son application.
Ce règlement est né après plusieurs scandales liés à des fuites massives d'informations ou à des utilisations abusives par de grandes sociétés.

Les données personnelles, de quoi parle-t-on ?

Une donnée personnelle est toute information qui permet d'identifier une personne :

- Directement : nom, prénom, adresse postale, numéro de téléphone, adresse e-mail.
- Indirectement : identifiant, adresse IP, historique de navigation, localisation.

Il existe aussi les données sensibles (RGPD art. 9), qui regroupent par exemple :

- les données de santé,
- les opinions politiques ou religieuses,
- les données biométriques ou génétiques.

👉 Dans le cadre du métier de technicien, la récupération de données peut concerner des fichiers simples (documents, photos, mails) mais parfois aussi des données sensibles, ce qui impose une vigilance encore plus grande.

Le RGPD appliqué au métier de technicien

Le RGPD repose sur des principes clés. Pour nous, ils se traduisent directement dans nos interventions :

- Transparence : l'utilisateur doit savoir ce que nous faisons avec ses fichiers.
- Finalité : on ne copie que dans un but précis (sauvegarde, migration, dépannage).
- Minimisation : inutile de tout transférer si seulement un dossier est demandé.
- Intégrité : les données copiées doivent rester exactes et non altérées.
- Confidentialité : interdiction de consulter les fichiers par curiosité.
- Limitation de conservation : suppression des copies temporaires après usage.

Exemple concret :
Lors d'une migration d'ordinateur, on informe l'utilisateur, on transfère uniquement ses documents et mails professionnels, puis on efface la copie locale après vérification du transfert.

Rôle et responsabilités du technicien

La dimension légale et professionnelle est essentielle. Une simple erreur peut avoir des conséquences importantes : perte de données, plainte d'un utilisateur, voire amendes pour l'entreprise.

Le technicien doit donc respecter trois grandes obligations :

- Confidentialité : ne jamais consulter ou divulguer des fichiers personnels.
- Sécurité : utiliser des supports chiffrés, des mots de passe, des serveurs sécurisés.
- Traçabilité : garder une trace de l'intervention (ticket, note de suivi, signature).

👉 Exemple : Si un technicien récupère un disque dur en panne et accède à des photos personnelles, il n'a pas le droit de les conserver ni de les copier. Il doit uniquement restituer les fichiers demandés et documenter l'intervention.

Méthodologie de récupération

La récupération de données ne se fait pas au hasard. Pour être conforme au RGPD et garantir un travail professionnel, le technicien doit suivre une démarche claire et structurée. Cela permet d'assurer la sécurité des données tout en réduisant les risques d'erreurs.

Avant l'intervention :

- Informer l'utilisateur de ce qui va être fait et obtenir son accord.
- Déterminer avec lui quelles données doivent être récupérées (documents, mails, photos, etc.).
- Préparer un support adapté et sécurisé : clé USB chiffrée, disque dur de l'entreprise, serveur de sauvegarde.

Pendant l'intervention :

- Utiliser des logiciels ou outils fiables de copie ou de sauvegarde.
- Vérifier régulièrement que les données copiées sont complètes et non corrompues (intégrité).
- Ne jamais utiliser un support personnel (clé USB privée, cloud personnel).

Après l'intervention :

- Restituer les données à l'utilisateur et vérifier avec lui que tout est présent.
- Supprimer immédiatement les copies temporaires.
- Documenter l'opération dans un rapport ou un outil de suivi.

👉 Exemple : Lors d'une migration de poste, on transfère uniquement le dossier "Documents" et les mails professionnels sur un support chiffré, puis on supprime toute copie locale une fois la vérification effectuée.

Risques en cas de non-respect

Ne pas appliquer correctement les règles peut avoir des conséquences graves. Le technicien doit être conscient de ces risques pour mesurer l'importance de son rôle.

Risques techniques :

- Perte définitive de données (mauvaise manipulation, effacement accidentel).
- Altération des fichiers (corruption pendant le transfert).

Risques juridiques :

- Amendes prévues par le RGPD pouvant aller jusqu'à 20 millions € ou 4 % du chiffre d'affaires mondial.
- Responsabilité civile ou pénale en cas de faute grave.

Risques éthiques :

- Atteinte à la vie privée de l'utilisateur.
- Perte de confiance vis-à-vis du technicien ou de l'organisation.

Risques professionnels :

- Sanctions disciplinaires (avertissement, licenciement).
- Perte de réputation professionnelle.

👉 Exemple : Copier des données sensibles sur une clé USB non sécurisée et la perdre peut coûter très cher à une entreprise et mettre en cause directement le technicien.

Les droits des utilisateurs

Le RGPD a été pensé pour protéger les citoyens et leur donner plus de contrôle sur leurs informations. Lors d'une récupération de données, le technicien doit connaître et respecter ces droits.

Principaux droits :

- Droit d'accès : toute personne peut demander à savoir quelles données une organisation possède sur elle.
- Droit de rectification : corriger ou compléter des données inexactes.
- Droit à l'effacement (droit à l'oubli) : possibilité de demander la suppression de ses données.
- Droit à la portabilité : obtenir ses données dans un format exploitable pour les transférer vers un autre service.
- Droit à la limitation du traitement : imposer que les données ne soient utilisées que pour certaines finalités.

👉 Exemple : un employé qui change de société peut demander une copie de ses mails professionnels. Le technicien doit fournir ces données dans un format lisible et supprimer les copies une fois l'opération terminée.