

Doryan MENDY  
Timothée LONCHAMPT

## SAE 3: Droit des contrats et du numérique

## Sommaire

1. Introduction
2. Cartographie du traitement de données
3. Finalité du traitement de données
4. Durée de conservation
5. Gestion des différents droits des personnes concernées
6. Intégration des principes clés de sécurité des données  
personnelles de la CNIL
7. Conclusion

## Introduction

Dans le cadre de notre SAE 3 et en tant que responsables du traitement de données de celle-ci, la rédaction d'une documentation interne concernant le traitement de données est nécessaire. Nous allons avant tout définir ce qu'est le traitement de données.

D'après le site [data-droit.com](http://data-droit.com), *“Un traitement de données est défini comme toute opération ou tout ensemble d'opérations appliquées à des données.*

*Cela peut-être :*

- *Une collecte de données*
- *La conservation de données*
- *L'utilisation de données*
- *Toute forme de mise à disposition de données*
- *L'effacement de données*
- *La destruction de données”*

En vue de notre plateforme de ticketing interne, le traitement de données est une variable importante car elles sont pour certaines confidentielles à tout type de niveau. L'importance du traitement de données résulte dans la fluidité de celle-ci à être utilisée par l'ensemble de l'équipe.

L'objectif de cette documentation est de vous guider dans la compréhension et dans les rouages de l'utilisation complète de nos données ainsi qu'à la fiabilité de notre plateforme à respecter le RGPD et les obligations légales.

## Cartographie du traitement de données

Dans cette première partie nous allons nous intéresser à l'ensemble de la cartographie, tout d'abord nous allons nous intéresser à la nature du traitement de donnée mis en œuvre, la finalité de ce traitement. Nous allons par la suite nous intéresser aux catégories de données personnelles traitées et pour conclure, nous allons débriefer sur la durée de conservation de celle-ci.

Pour commencer, nous allons nous intéresser à la nature du traitement de données utilisé dans notre plateforme:

Concernant les informations sur le ticket :

- **description du problème:** un ticket possède toujours un libellé qui décrit brièvement le problème rencontré

- **statut de ticket:** un ticket à trois type de statut (ouvert, en cours de traitement et fermé)
- **priorité:** un ticket possède quatre types de niveau d'urgence (faible, moyen, important et urgent)
- **attribution:** un ticket est attribué à un technicien

Concernant les données utilisateurs:

- **Identifiant de l'utilisateur:** un utilisateur rentre un login à la création d'un compte utilisateur
- **mot de passe:** un utilisateur choisi un mot de passe après son login à la création de son compte utilisateur
- **coordonnée:** un utilisateur doit rentrer une adresse mail et un numéro de téléphone à la création de son compte

Concernant les données techniciens:

- **administration des tickets:** un technicien s'attribue lui même les tickets qui peut résoudre

Concernant les données de suivi:

- **Historique des actions:** des journaux d'activités pourront être consultés par les administrateurs. Ils contiennent pour la création d'un ticket, la date, l'adresse IP, le login de l'utilisateur qui a créé le ticket et le niveau d'urgence. Ces journaux d'activités vont recenser toutes les tentatives infructueuses de la plateforme. Ce sera les mêmes données que lors d'une création d'un ticket qui sera enregistré.

## Finalité du traitement de données

La finalité du traitement de données dans notre plateforme de ticketing interne est de faciliter et optimiser la gestions des tickets, la résolution des problèmes techniques liés à la plateforme, voici les objectifs clés :

- **Optimisation des processus internes:** En facilitant la gestion des tickets, le traitement de données n'en deviendra que plus efficace. Cela implique aussi une attribution rapide des tickets aux techniciens et une résolution rapide des problèmes.
- **Sécurité des données:** La plateforme doit garantir la sécurité des données, en particulier avec des informations sensibles comme les identifiants de connexion et les mots de passe (qui seront bien sûr cryptés). La finalité inclut donc la mise en place de mesures de sécurité robustes notamment avec l'implémentation du chiffrement RC4 lié à une fonction de hachage.
- **Conformité aux réglementations:** La finalité du traitement de données comprend la garantie que toutes les opérations respectent les réglementations du RGPD (règlement général sur la protection des données).

Voici l'ensemble des articles et leurs spécifications du RGPD en lien avec la conformité de notre plateforme:

- **Transparence et Licéité (Article 5 du RGPD):** la déclaration de confidentialité c'est-à-dire que la politique de confidentialité doit être accessible à tous les utilisateurs est un point important. L'autre point important est le consentement éclairé, cela signifie que la plateforme doit expliquer de façon clair, explicite et de manière volontaire que les données des utilisateurs seront utilisées
- **Minimisation des données (Article 5 du RGPD):** Le point important est la collecte des données pertinentes. Cela va de soi avec le fait de limiter la quantité de données traitées.
- **Intégrité et Confidentialité (Article 5 du RGPD):** Concernant la confidentialité, nous avons déjà défini les mesures cryptologiques mises en place afin de sécuriser les données les plus importantes.
- **Évaluation d'Impact sur la Protection des Données (Article 35 du RGPD):** Concernant ce point là nous devons réaliser un EIPD (Évaluation d'Impact sur la Protection des Données)

### Description complète de notre EIPD

#### **1. Identification du traitement de données**

- Description du traitement : Le traitement concerne la gestion des tickets sur une plateforme interne. Cela inclut la collecte, la conservation, et l'utilisation de données liées aux tickets, aux utilisateurs, et aux techniciens

#### **2. Evaluation des risques**

- Risque pour la confidentialité: Possibilité d'accès non autorisé aux informations des tickets notamment sur les détails des problèmes rencontrés par les utilisateurs.
- Risque pour la sécurité: Risques de violation de la sécurité des identifiants de connexion et des données des utilisateurs.
- Risques pour l'Exactitude des Données: Possibilité d'inexactitudes dans les données des utilisateurs ou des tickets.

#### **3. Mesures d'atténuation des risques**

- Chiffrement des Données: Mettre en place un chiffrement robuste pour protéger les données sensibles (RC4).
- Contrôle d'accès: Limiter l'accès aux données uniquement aux personnes autorisées (utilisateurs, administrateur web et système, techniciens).

## **Durée de conservation**

Une gestion appropriée de la durée de conservation de nos données va nous permettre d'assurer notre conformité aux réglementations de protection de données et du RGPD.

Nous avons sélectionné des critères de conservation de nos données. Ces critères sont :

- Finalité du traitement: En fonction de la finalité du pour laquelle nos données ont été collecté, une prise de décision a été nécessaire
- Obligations légales: Par rapport aux types de données collectés et aux juridictions de chacune, ce critère est nécessaire afin d'assurer la non conformité des données.

#### 1. **Information sur les tickets**

- Description du problème: Jusqu'à la résolution complète du ticket
- Statut du ticket et Priorité: Archivage pendant une période de 12 mois après la fermeture du ticket pour une analyse sur nos capacités de performance et nos statistiques

#### 2. **Données utilisateurs**

- Identifiant de l'utilisateur: Pendant la durée de vie du compte utilisateur
- Mot de passe: Stocké et crypté de manière sécurisé dans notre base de données et régulièrement mis à jour
- Coordonnée: Jusqu'à ce que l'utilisateur demande la suppression de ces derniers

#### 3. **Données techniciens**

- Administration des tickets: Jusqu'à ce que le technicien ne soit plus actif ou attribué à des tickets

#### 4. **Données de suivi**

- Journaux d'activités: Archivés pour une période de 12 mois à des fins de sécurité et de conformité. (date, adresse IP, utilisateur qui rentre le ticket, le niveau d'urgence)

## Gestion des droits des personnes concernées

### 1. **Visiteur**

Les visiteurs sont des personnes qui n'ont pas de compte spécifique sur la plateforme. Leurs droits incluent:

- Accès aux derniers tickets: les visiteurs ont accès aux 10 derniers tickets mis en place sur la plateforme

### 2. **Utilisateur**

Les utilisateurs standards sont les clients qui soumettent des tickets pour résoudre des problèmes. Leurs droits incluent:

- Création des tickets: Les utilisateurs peuvent créer de nouveaux tickets pour signaler des problèmes ou demander de l'assistance.

- Suivi de leur ticket: Accès à l'historique et au suivi des tickets qu'ils ont créés.

### 3. Technicien

Les techniciens sont responsables de la résolution des problèmes signalés par les utilisateurs. Leurs droits comprennent:

- Attribution et résolution des tickets: Les techniciens peuvent s'attribuer des tickets et les résoudre.
- Gestion des tickets assignée: Accès aux informations détaillées des tickets attribués et aux historiques d'actions associés.

### 4. Administrateur web

Les administrateurs ont des droits étendus pour superviser l'ensemble du système. Leurs droits incluent:

- Gestion des libellés affectés : l'administrateur web peut gérer la liste des libellés affectés aux différents problèmes qui peuvent être rencontrés dans les salles informatiques.
- Modification des statuts: l'administrateur web peut modifier le statut du ticket en fonction de son état (ouvert, en cours d'exécution, fermé)
- Modification des niveaux d'urgences: Si le niveau d'urgence d'un ticket ne lui semble pas adapté, l'administrateur web peut le modifier afin de fluidifier et de prioriser la gestion des tickets

### 5. Administrateur système

L'administrateur web n'a qu'un rôle très particulier:

- Accès aux journaux d'activités: L'administrateur web est le seul utilisateur qui a accès à l'entièreté des journaux d'activités

## Système de gestion des droits

- Attribution basée sur les rôles: La plateforme utilise un système de gestion des droits basé sur les rôles pour garantir une attribution appropriée des droits. Chaque utilisateur est associé à un rôle spécifique, déterminant ses privilèges.
- Flexibilité et agilité: Le système de gestion des droits est conçu pour être flexible, cela permet de réaliser des ajustements rapides en fonction des changements de personnel ou des besoins opérationnels. Les administrateurs peuvent rapidement modifier les droits d'accès pour s'adapter aux évolutions de l'équipe. Cela nous permet de contrôler l'agilité de la gestion des droits utilisateurs.

## Intégration des principes clés de sécurité des données personnelles de la CNIL

### 1. Principe de Finalité (Article 5 du RGPD):

- **Extrait du Guide CNIL:** "Les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes."
- **Intégration dans la plateforme:** La collecte des données de notre plateforme est alignée sur des finalités spécifiques liées à la gestion des tickets notamment grâce à la création de rôle spécifique sur le processus complet de gestion d'un ticket. Ces finalités sont communiquées aux utilisateurs par notre transparence et par notre respect à l'ensemble des obligations liées au RGPD.

## **2. Principe de pertinences des données (Article 5 du RGPD)**

- **Extrait du Guide CNIL:** "Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées."
- **Intégration sur la plateforme:** La plateforme prend parti sur la limitation des données des utilisateurs notamment avec un formulaire d'inscription très spécifique à la gestion ou la création de tickets.

## **3. Principe de transparence (Article 5 du RGPD)**

- **Extrait du Guide CNIL:** "Les personnes dont les données sont collectées doivent être informées de manière transparente, précise et accessible."
- **Intégration dans la plateforme:** La politique de confidentialité de notre plateforme est basée sur la transparence avec nos clients. La collecte est l'utilisation de nos données sont limité et strictement nécessaire par rapport à l'utilisation de celle-ci

## **4. Principe de Sécurité (Article 32 du RGPD)**

- **Extrait du Guide CNIL:** "Les données personnelles doivent faire l'objet de mesures de sécurité appropriées."
- **Intégration dans la plateforme:** L'ensemble de nos mesure prise pour sécuriser l'ensemble des données de notre plateforme ont été travaillé spécifiquement pour les besoins de chaque utilisateurs. En passant par le cryptage des mots de passe utilisateurs, par la gestion des rôles de chaque utilisateur qui est limité mais aussi par une sécurité renforcée au niveau de la connexion. Notre plateforme assure le principe de sécurité.



# Conclusion

En conclusion de cette documentation interne sur le traitement de données dans notre plateforme de ticketing interne, nous soulignons l'importance cruciale du respect des principes du RGPD et des obligations légales en matière de protection des données.

La cartographie du traitement de données a permis de détailler la nature du traitement, les catégories de données personnelles traitées, et la durée de conservation spécifique pour chaque type d'information.

La finalité du traitement, axée sur l'optimisation des processus internes, nous permet de démontrer notre engagement envers une gestion transparente et éthique des informations sensibles de nos utilisateurs. L'utilisation d'un EIPD met en valeur notre engagement à évaluer les risques pour la confidentialité et la sécurité de nos données.

La gestion des droits des différentes catégories d'utilisateurs, intégrant les principes clés de la CNIL, démontre notre dévouement à garantir des droits appropriés en fonction des responsabilités de chacun.

En résumé, notre engagement envers la protection des données se reflète dans chaque aspect de notre plateforme, garantissant à nos utilisateurs un environnement sécurisé, transparent et conforme aux réglementations en vigueur