RODIER Matis, CHIRON Jules, GODINEAU Thomas
17/12/2023

UVSQ université PARIS-SACLAY
IUT de Vélizy-Rambouillet
CAMPUS DE VÉLIZY-VILLACOUBLAY
CAMPUS DE RAMBOUILLET

SAÉ 3.01 - Droits des contrats et du numérique

Protection des données personnelles

La mise en place d'une application web dédiée à la gestion des demandes de dépannage sur les salles machines, dans le cadre du projet SAÉ IN3SA01, impose une importante responsabilité quant à la protection des données personnelles des utilisateurs, comprenant tant les étudiants que les professeurs. En conformité avec le Règlement Général sur la Protection des Données (RGPD) et la législation Informatique et Libertés (I&L), le principe de Privacy by Design devient donc notre approche. Cette documentation interne vise à offrir une vue détaillée sur la cartographie du traitement des données personnelles, la gestion des droits des personnes concernées, et la mise en œuvre des principes de sécurité, tout en s'inspirant du guide de la CNIL. L'objectif est de démontrer notre engagement envers la confidentialité des données et d'assurer la conformité rigoureuse aux réglementations en vigueur.

La cartographie du traitement des données personnelles au sein de notre application web pour la gestion des demandes de dépannage reflète notre engagement envers la protection et la confidentialité des informations des utilisateurs, que ce soient des étudiants, professeurs ou d'autres personnels. La collecte d'éléments tels que le nom, le prénom, la photo de profil, la date de naissance et le groupe (professeur ou élève) vise principalement à personnaliser l'expérience utilisateur en affichant des informations spécifiques sur leur page de profil. Cela contribue non seulement à créer une interface conviviale mais aussi à enrichir leur interaction avec la plateforme. Ces données, appartenant à la catégorie des données d'identité, sont conservées jusqu'à la suppression du compte, témoignant de notre engagement envers une gestion transparente et responsable des informations personnelles.
De même, la collecte de l'adresse électronique et du mot de passe est guidée par la nécessité d'attribuer à chaque utilisateur un login personnel et de sécuriser leurs connexions. Ces informations cruciales, classées dans la catégorie des données de connexion, sont conservées jusqu'à la suppression du compte ou le changement de mot de passe pour le dernier mot de passe utilisé, suivant ainsi les meilleures pratiques de sécurité.
La ville de résidence, une donnée de localisation, est enregistrée dans le but d'améliorer la personnalisation de l'interface utilisateur en fournissant des informations contextuelles liées à la localisation. De plus, cela permet de rendre plus interactif notre plateforme de ticketing. Sa durée de conservation est également alignée sur la suppression du compte, garantissant une gestion responsable des données liées à la localisation. Notre approche garantit que nous respectons strictement les règles du RGPD et de la législation sur l'Informatique et les Libertés, renforçant ainsi la confiance des utilisateurs dans la protection de leurs données personnelles.

La gestion des droits des différentes personnes concernées sur notre plateforme de ticketing est très importante.
Pour les Utilisateurs Non Connectés, le droit d'accès est accordé, leur permettant de consulter les informations publiques de l'application, notamment les 10 derniers tickets. De plus, ils ont le droit de se connecter ou de créer un compte pour accéder à des fonctionnalités supplémentaires.
Les utilisateurs connectés bénéficient d'un ensemble de droits essentiels. Le droit d'accès leur donne la possibilité d'explorer leurs propres données personnelles, tandis que le droit de rectification leur permet de mettre à jour ces informations en fonction de leurs besoins. En outre, le droit à l'effacement confère aux utilisateurs connectés le pouvoir de supprimer leur compte, assurant ainsi la suppression de toutes leurs données personnelles enregistrées.
Les administrateurs Web disposent de droits étendus, leur permettant d'accéder aux données personnelles des techniciens, de gérer les tickets de tous les utilisateurs, et d'accéder aux détails des interventions liées aux tickets. Ils ont également le droit de gestion des techniciens, ce qui leur donne la possibilité de créer de nouveaux comptes techniciens et d'attribuer des tickets à ces derniers.
Les Administrateurs Système ont un accès privilégié à l'historique des connexions et à l'historique des tickets fermés et créés, renforçant ainsi la surveillance et la gestion globale du système.
Enfin, les Techniciens détiennent des droits spécifiques liés à la gestion des tickets. Le droit de prise en charge des tickets leur confère le pouvoir de gérer les tickets en vue de leur résolution, tandis que le droit de clôture de ticket leur permet de marquer un ticket comme clos une fois la résolution complétée.
Cette structure des droits est conçue pour assurer une gestion transparente, sécurisée et efficace des informations personnelles, tout en respectant les rôles et responsabilités spécifiques de chaque type d'utilisateur au sein de notre plateforme de ticketing.

La sécurité de l'authentification des utilisateurs sur notre plateforme de ticketing est une priorité essentielle pour garantir un accès sécurisé et personnalisé aux données personnelles. Conformément aux recommandations de la CNIL, nous mettons en œuvre des mécanismes d'authentification basés sur des facteurs de connaissance. Cela inclut l'utilisation de mots de passe et de login (nom d'utilisateur).
Nous avons mis en place des précautions élémentaires, telles que la définition d'identifiants uniques (le login) par utilisateur.
Concernant les mots de passe, nous suivons rigoureusement les recommandations de la CNIL. Nous les conservons de manière sécurisée, n'exigeons pas de renouvellement périodique pour les simples utilisateurs, et imposons une complexité appropriée en fonction des cas d'usage. Nous vérifions régulièrement la robustesse de notre politique de mots de passe en utilisant l'outil fourni par la CNIL.
Pour renforcer la sécurité, nous sensibilisons nos utilisateurs aux pratiques à éviter, comme la communication de mots de passe personnels, le stockage non sécurisé ou l'utilisation de mots de passe liés à des informations personnelles.

La sécurité des données sur notre plateforme de ticketing est renforcée par la mise en place de précautions élémentaires, alignées sur les recommandations de la CNIL.
L'accès aux outils et interfaces d'administration est restreint aux personnes habilitées, en particulier en limitant l'utilisation des comptes administrateurs aux équipes informatiques, uniquement pour les actions d'administration nécessaires. Nous avons un seul et unique administrateur système, de même pour l'administrateur web. Nous nous conformons également à la réglementation en recueillant le consentement de l'internaute avant le dépôt de cookies non essentiels au service.
Nous mettons en œuvre une veille constante sur le nombre de composants utilisés, en limitant leur nombre et en assurant des mises à jour régulières. En revanche, nous évitons plusieurs pratiques à risque, notamment le transit de données à caractère personnel dans une URL (avec les méthodes GET) et l'utilisation de services non sécurisés.
La sécurité des données sur notre plateforme de ticketing est renforcée par l'application de précautions essentielles en matière de fonctions cryptographiques.
Nous suivons scrupuleusement les recommandations en matière d'algorithme. En effet pour la SAE de cryptographie nous avons créé nos propres fonctions de chiffrement apprises en cours de cryptographie. Nous protégeons soigneusement les clés secrètes (qui nous permettent de chiffrer et de déchiffrer le message) en appliquant des droits d'accès restrictifs et en utilisant des mots de passe robustes pour les utilisateurs ayant des droits importants. Une procédure détaillée est rédigée pour la gestion des clés et des certificats, prenant en compte les éventualités telles que les cas d'oubli de mot de passe de déverrouillage (Cette page est toujours en construction).
Pour finir, en évitant l'utilisation d'algorithmes obsolètes tels que DES, 3DES, MD5 et SHA-1, nous nous assurons que notre approche cryptographique reste robuste.

Pour conclure, notre démarche pour la mise en place d'une application web dédiée à la gestion des demandes de dépannage, dans le cadre du projet SAÉ IN3SA01, se distingue par un engagement envers la protection des données personnelles des utilisateurs utilisateurs tels que les élèves et les professeurs. Suivant le principe de Privacy by Design et en respectant le RGPD et la législation Informatique et Libertés, notre documentation interne offre une vision complète de la cartographie du traitement des données, de la gestion des droits des personnes concernées, et des principes de sécurité.

Annexes

Type d'utilisateur	Type de droit	Description
Utilisateurs Non Connectés	Droit d'accès	Possibilité d'accéder aux informations publiques de l'application (les 10 derniers tickets).
	Droit de rectification	Capacité à corriger des informations erronées ou demander la suppression de certaines données.
Utilisateurs Connectés	Droit d'accès	Accès aux données personnelles de l'utilisateur.
	Droit de rectification	Possibilité de mettre à jour les informations personnelles.
	Droit à l'effacement	Demande de suppression des données personnelles sur demande.
	Droit d'opposition	Possibilité de s'opposer à certains traitements de données.
Administrateur Web	Droits spécifiques	Accès et gestion des données des utilisateurs dans le cadre de ses responsabilités.
Administrateur Système	Droits spécifiques	Gestion des données personnelles avec un focus sur la sécurité et les autorisations.
Techniciens	Droits spécifiques	Accès aux demandes de dépannage et gestion des interventions, conformément à leurs responsabilités spécifiques.

Annexe 1 : Gestion des différents droits des personnes concernées

Sources

Principes clés de la CNIL

- Authentification des users
- Sécuriser le site
- Chiffrage des données