UVSQ université PARIS-SACLAY

IUT de Vélizy-Rambouillet

CAMPUS DE VÉLIZY-VILLACOUBLAY

SAE S3- Développement d'une application

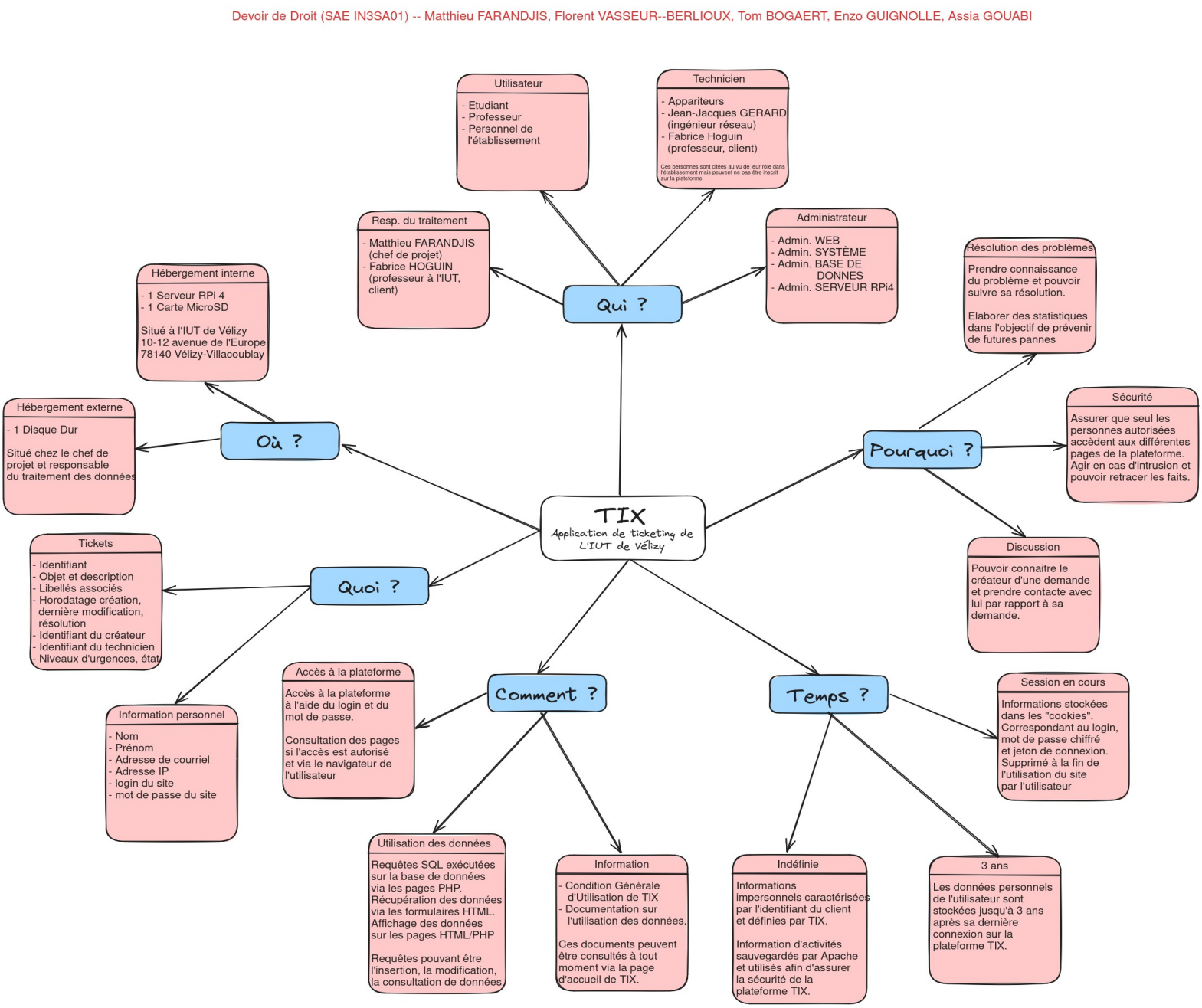
INF2A - 2023-2024

Florent VASSEUR–BERLIOUX
Tom BOGAERT
Assia GOUABI
Enzo GUIGNOLLE
Matthieu FARANDJIS

Droit des contrats et du numérique

Document joint :

- Cartographie du traitement des données (résumant et illustrant ce document)
  cartographie_inf2a_sae_droit_farandjis_bogaert_vasseur–berlioux_guignolle_gouabi.png



La collecte et le traitement des données personnelles sont des aspects cruciaux de la gestion des données dans le monde numérique actuel. Il est impératif de suivre les cinq grands principes fondamentaux énoncés sur le site officiel de la CNIL pour garantir le respect de la confidentialité, la transparence et la collecte licite des données. Le client doit être pleinement informé de la durée et de la raison du prélèvement de ses données personnelles que ce soit pour personnaliser l'expérience de l'utilisateur ou mener des analyses statistiques. De plus, les collecteurs d'informations doivent assurer la sécurité des données qu'ils détiennent et de les prélever uniquement si elles sont nécessaires. Ces idées constituent les règles de protection des données. Nous nous sommes appuyés sur ses principes pour réaliser notre application impliquant les données confidentielles de nos utilisateurs. Dans un premier temps, nous détaillerons les types de données recueillies dans notre application en mettant en évidence leur nature et la finalité de cette cueillette. Par la suite, nous explorerons les différents droits attribués aux personnes concernés par cette application ainsi que la durée de conservation des données et nous terminerons avec la sécurité des données personnelles du site web.

Les données collectées sur les utilisateurs par certaines plateformes englobent une quantité indénombrable d'informations personnelles pouvant en inquiéter plus d'un.
Avec l'application TIX, seules les données personnelles nécessaires pour la résolution des tickets et la sécurité du système sont collectées.
Parmi les catégories de données recueillies, nous trouvons des données liées à l'utilisation telles que l'adresse IP, l'horodatage ou encore l'identifiant de l'utilisateur. Les données de compte regroupant le login et le mot de passe chiffré qui permettent à l'utilisateur de se connecter, mais aussi des informations liées à l'identité de la personne sont collectées. Nous pouvons citer le prénom, nom et l'adresse de courriel pour identifier une personne. Lorsqu'une personne tente de se connecter à l'application, mais que la tentative échoue, l'adresse IP, le login et le mot de passe entré par la personne qui a tenté cette action seront récoltés.
L'application commence par rassembler les données personnelles entrées par la personne pour s'inscrire à la plateforme. Les catégories de données énumérées au-dessus telles que les données liées à la connexion sont enregistrées temporairement dans un fichier de type cookie, indépendant de la base de données afin de reconnaître un utilisateur pour de potentielles futures utilisations. Ce stockage, cette conservation vis-à-vis de l'utilisateur permettra sa connexion automatique après l'insertion de ses données personnelles dans le formulaire de connexion. Ainsi, il économise du temps et peut avoir accès aux différentes fonctionnalités en tant qu'utilisateur de l'application.
Simultanément, les informations confidentielles sont stockées dans la base de données. Elles seront utilisées par l'application web afin de pouvoir fournir ses différents services à l'utilisateur. L'accès à ces données est limité à l'utilisateur concerné. L'administrateur web a également accès à ces renseignements excepté le mot de passe. Certaines de ces données sont accessibles par les techniciens dans le cadre de la résolution de tickets. La modification et la suppression de ces informations sont limitées à l'utilisateur concerné et l'administrateur web. Les données personnelles seront associées aux différents tickets par le biais de l'identifiant unique de l'utilisateur. L'identifiant unique sera par ailleurs utilisé dans le cadre du journal d'activité afin d'associer une action à un utilisateur.

Dans le cadre de notre projet, ces informations confidentielles nous permettront de recueillir des informations sur les utilisateurs qui fréquentent notre application pour pouvoir personnaliser leurs expériences et assurer le succès continu de l'application web. Le fait de constamment récupérer des informations confidentielles, nous oblige à sécuriser au maximum notre application pour éviter la perte de clients. L'analyse approfondie des données collectées facilitera l'identification de potentielles améliorations en évaluant la performance et les retours clients. Les données anonymisées pourront être utilisées dans le cadre d'études statistiques. Cependant, les données ne peuvent être utilisées pour une autre utilisation que celle prévue. Il est considéré que l'inscription de la personne sur la plateforme signifie qu'elle a lue, approuvée et consentie clairement et explicitement les documents liés au traitement de ses données personnelles. En conséquence, l'utilisateur se doit d'être âgé d'au moins de 15 ans pour s'inscrire sur la plateforme. L'âge minimum de consentement en France est de 15 ans selon la CNIL https://www.cnil.fr/fr/recommandation-4-rechercher-le-consentement-dun-parent-pour-les-mineurs-de-moins-de-15-ans.

En explorant plus en détails la composition de notre site web, on retrouve une variété de profils d'utilisateurs. Le visiteur initial, restreint à la page d'accueil, ne peut accéder aux fonctionnalités du site de ticketing. En s'inscrivant ou se connectant, il devient un utilisateur, il aura accès à son profil, incluant certaines informations personnelles. Il a la possibilité de modifier son adresse Email et son mot de passe et possède aussi l'accès au tableau de bord présentant les tickets techniques émis par les utilisateurs. L'utilisateur peut créer des tickets pour signaler aux techniciens des problèmes techniques. Les techniciens, en revanche, peuvent modifier les tickets pour se les attribuer et résoudre les problèmes signalés. Ils ont également accès à leurs informations personnelles. L'administrateur web, unique et distinct des techniciens, a des privilèges supplémentaires. En plus de gérer les tickets, il peut administrer la plateforme en ajoutant des techniciens et des libellés. Enfin, l'administrateur système, unique comme l'administrateur web, possède des droits liés au fonctionnement de la plateforme en plus de ceux des utilisateurs. Sa page d'administration lui offre la possibilité de consulter l'historique des connexions des utilisateurs, y compris les tentatives invalides, ainsi que les tickets fermés.
Les utilisateurs de l'application mentionnés ci-dessus possèdent des droits juridiques à prendre en compte par les concepteurs de la plateforme pour garantir le succès de celle-ci tels que le droit à l'information. Nous devons nous engager à informer l'utilisateur qu'une collecte de données est à prévoir et d'indiquer la raison de cette collecte et sa durée. En prenant en compte les idées défendues sur le site officiel de la CNIL concernant la durée de conservation des informations Les durées de conservation des données | CNIL, les données personnelles des individus inactifs ne peuvent être conservées plus de 36 mois, soit trois ans. En revanche, par leur importance majeure, les comptes administrateurs ne peuvent être supprimés. Ces comptes sont impersonnels et ne comportent pas d'informations confidentielles. Seul le personnel autorisé peut se connecter avec ces comptes. Sur notre projet d'application web de ticketing, nous possédons un historique de l'activité des utilisateurs. Il nous est donc possible de déterminer la durée de l'inactivité d'un utilisateur pour ensuite vider ses informations personnelles de notre base de données. Relatifs aux cookies, ils ne peuvent être légalement conservés plus de 13 mois, il est donc nécessaire de demander de nouveau l'accord des utilisateurs une fois cette durée dépassée. Tout cookie utilisé sur notre application aura une durée de vie maximale de 34,187,399 secondes. De plus, aucune donnée n'est prévue d'être stockée par l'intermédiaire des cookies. Les données récupérées par l'intermédiaire des traceurs

ont une durée de vie de 25 mois. Ces informations ont été récupérées des sites suivants : Cookies : solutions pour les outils de mesure d'audience | CNIL et RGPD en pratique : maîtrisez votre relation client | CNIL.
Par la suite, les utilisateurs ont le droit de modification et rectification manuellement de certaines de leurs informations personnelles de façon instantanée. En ce qui concerne les autres données, ils pourront faire la demande auprès du responsable des fichiers et de la plateforme à l'adresse de courriel suivante : contact.mfarandjis@orange.fr. L'utilisateur possède le droit à l'oubli numérique. Il est conscient des informations qui lui seront prélevées dès son inscription et pourra être effacé de la base de données s'il supprime son compte. La radiation d'un compte utilisateur entraîne la suppression des informations personnelles associées à ce compte. Les tickets et actions de l'utilisateur sauvegardés dans le journal et la base de données seront conservés au même titre que l'identifiant unique rattaché à ce compte. Par la suppression des données personnelles, ces données sont anonymisées, ce qui veut dire qu'il ne sera plus possible de retrouver les informations confidentielles à partir de l'identifiant du compte supprimé. La déconnexion de l'usager de la plateforme n'entraîne que la suppression du contenu des fichiers de type cookie.

Enfin, en ce qui concerne la sécurité des données personnelles de notre application web, une bonne partie de notre temps était dédiée à la base de données pour garantir sa sécurité. En premier lieu, chaque utilisateur, technicien ou administrateur possède son propre profil dans le système de gestion de bases de données MariaDB. Chaque profil est associé à un rôle qui lui accorde des droits et des accès.
Pour un utilisateur, son profil MariaDB est créé et son rôle d'utilisateur est accordé lors de son inscription. L'administrateur web est la seule personne pouvant attribuer le rôle de technicien à un utilisateur. Cependant, un utilisateur ne peut pas devenir administrateur web ou administrateur système. Le rôle permet de donner l'accès à des fragments des tables du système de gestion de bases de données et de leur donner des droits dessus. Ces fragments sont appelés des "vues".
Par exemple, l'une des vues empêche l'utilisateur d'avoir accès aux informations des autres utilisateurs stockés dans la table "Utilisateur". Cette vue ne lui permet que de voir ses informations sans lui permettre de les modifier. Cette sécurité est garantie par le fait que toute personne ayant accès à la plateforme possède son propre profil MariaDB, et donc ses propres accès et droits. La base de données est conçue pour que chaque usager ne puisse l'utiliser que de la manière dont le site est conçu. Si un utilisateur arrive à outrepasser les limites fixées par le site PHP via l'injection de code SQL par exemple, il ne pourra rien faire de plus. Notre base de données ne stocke pas les mots de passe d'une quelconque manière ou sous une quelconque forme. Les mots de passe sont gérés directement par le SGBD MariaDB. L'usager ne peut que modifier son propre mot de passe. Personne ne peut récupérer ou décrypter un mot de passe chiffré par MariaDB ni même les administrateurs web et système. Cela limite le risque de fuite de mot de passe en cas de piratage de la base de données. Le compte administrateur de la base de données "root" a la permission de les réinitialiser, mais pas de les voir en clair. Ce compte administrateur à un accès intégral en lecture et écriture sur la totalité de la base de données. Il n'est pas et ne sera jamais utilisé lors de l'utilisation de la plateforme. Ce compte est réservé à l'administrateur de la base de données et n'est associé à aucun compte sur la plateforme. Le mot de passe de ce compte est très fort et introuvable par attaque par brute force. Par son pouvoir, l'administrateur de la base de données est tenu de ne pas enregistrer, partager, extraire d'une quelconque manière les données de celles-ci. Il ne peut qu'agir que pour le bon fonctionnement de l'activité de la plateforme ou dans un rôle de modération de celle-ci.

Cependant, les pages web PHP sont amenées à manipuler le mot de passe de l'utilisateur en clair. Ces pages ne peuvent pas être modifiées par les utilisateurs systèmes du serveur. Seul le compte administrateur le peut, muni d'un mot de passe jugé très fort. Pour empêcher l'utilisateur de se connecter de nouveau dès qu'il change de page, une version chiffrée de son mot de passe est stockée sous la forme d'un fichier cookie.
La manière dont sera chiffré ce mot de passe fera l'objet d'un devoir de cryptographie pour cette SAÉ. Nous pouvons assurer cependant que la version chiffrée de ce mot de passe aura une durée de vie. Étant donné que c'est une plateforme locale, le chiffrement dépendra sûrement de l'ordinateur s'étant connecté à la plateforme. En cas de copie de ce fichier cookie par un pirate, celui-ci ne pourra donc pas y accéder sur un autre ordinateur ou à un autre moment sur la même machine. Dans tous les cas, ce fichier est détruit à la déconnexion de l'utilisateur. Seul l'administrateur système a accès aux journaux d'activités, et uniquement en lecture. Ce journal ne sera pas stocké dans la base de données. La plateforme inscrit les actions à la suite du document, elle peut éditer son nom, mais pas son contenu. Les données sont hébergées sur le serveur Raspberry Pi 4 à l'IUT de Vélizy. L'accès physique au serveur est réservé au client, Monsieur HOGUIN. L'accès à distance au serveur est réservé au client, et aux membres de l'équipe chargée de la création et de la maintenance de la plateforme TIX. Les accès sont sécurisés. Avec l'accord du client, une copie hebdomadaire des données est faite sur un disque dur détaché du serveur afin d'assurer au mieux l'intégrité des données en cas de panne du serveur. Les moyens fournis ne peuvent permettre une sauvegarde en temps réel des données.

En conclusion, la gestion des données personnelles dans le contexte numérique occupe un rôle crucial en établissant les bases d'une expérience utilisateur fiable, respectueuse de la vie privée et conforme aux normes éthiques. Notre application de ticketing s'inscrit pleinement dans ces cinq principes en respectant les normes de la CNIL pour assurer la confidentialité, la transparence et la légitimité de la collecte des données. Les catégories de données que nous recueillons, allant de données d'utilisation aux informations d'identité sont soigneusement détaillées afin de garantir une vision claire de la nature et de la finalité de cette cueillette et d'instaurer un climat de confiance entre l'application et ses utilisateurs.
La diversité des profils utilisateurs de la plateforme, allant du visiteur aux administrateurs, contribue à fournir des services variés en respectant les droits juridiques des utilisateurs et de proposer une expérience utilisateur adaptée à chaque catégorie d'utilisateurs.
Cependant, la sécurité des données demeure au cœur de nos préoccupations d'où la préférence accordée aux accès restreints pour protéger les informations sensibles de la base de données. Les rôles et vues spécifiques garantissent un accès et des droits appropriés et limités. De plus, le stockage des données sensibles dans des fichiers temporaires et la gestion des cookies sont conçus pour maximiser la sécurité. En résumé, notre engagement envers la protection des données se manifeste à chaque étape de la conception à la réalisation de l'application.