



GSB_Mission_1

Étude concernant le RGPD au sein du projet

Cette page contient l'étude réalisée pour contrôler la conformité au RGPD durant la réalisation du projet au sein du laboratoire pharmaceutique Galaxy Swiss-Bourdin, ou GSB.

Conformité au RGPD : Sécurisation des données

Pour garantir la sécurité des données à caractère personnel au sein de l'entreprise GSB, plusieurs mesures techniques et organisationnelles ont été établies, en conformité avec le RGPD.

Tout d'abord, concernant l'accès à la base de données sur le serveur, il n'existe que trois comptes pouvant se connecter ailleurs qu'en local. Ces comptes possèdent chacun un mot de passe qui a été généré aléatoirement, avec **une longueur de 10 caractères qui alternent majuscules, minuscules et chiffres**. Le compte root (ou superutilisateur) de la base de données possède un mot de passe suivant les mêmes critères, assurant la sécurisation au niveau de l'accès aux données conservées dans la base de données.

Ensuite, concernant l'intégrité et la disponibilité des données à caractère personnel stockées dans la base de données, un **système de sauvegarde automatique quotidien avec rotations hebdomadaires** assure la capacité de pouvoir conserver une copie récente, à jour de la base de données. De plus, un **script de restauration** permet de remettre la base de données à un état antérieur mais récent en cas de détérioration volontaire. Dans ces cas, l'intégrité et la disponibilité sont garantis au sein de GSB.

Conformité au RGPD : Procédures en cas de violation de données

Dans l'éventualité où un scénario de violation de données se concrétise, plusieurs mesures ont été mises en place, en conformité avec le RGPD.

Pour cela, et **sous 72 heures au maximum**, la CNIL est notifiée de la violation de données, avec une notification initiale qui avertit la CNIL de l'incident, puis, après avoir réuni ou déterminé les éléments suivants, une seconde notification à la CNIL est envoyée:

- La nature de la violation
- Le nombre approximatif de personnes touchées
- Les conséquences probables de la violation
- Les mesures envisagées ou à prendre

Après avoir notifié la CNIL sous les plus brefs délais, les personnes concernées par la violation de données sont **averties** dans un but de *transparence* et pour leur demander d'être très prudent tout en nous excusant de la violation rencontrée.

Enfin, l'accès au serveur physique deviendra plus restreint, et les connexions entrantes au serveur de base de données seront plus limitées et contrôlées.

Avec ces mesures et procédures de notification en cas de violation des données, le laboratoire pharmaceutique GSB est en conformité totale avec le RGPD.

Conformité au RGPD : Collecte de données personnelles

Les données à caractère personnel collectées par l'application "Catalogue" sont : le nom , le numéro , le prénom, la rue ,

la ville , la région , le code postale du praticien .

Assurer que la collecte de ces données est transparente et que les utilisateurs sont informés de la finalité de la collecte. Pour cela, nous mettons en place une approche qui garantit la transparence et qui permet aux utilisateurs de comprendre pourquoi leurs données sont collectées et comment elles seront utilisées. Cette approche concerne un formulaire de collecte.

“Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par [identité et coordonnées du responsable de traitement] pour [finalités du traitement]. La base légale du traitement est [base légale du traitement]. Les données collectées seront communiquées aux seuls destinataires suivants : [destinataires des données]. Les données sont conservées pendant [durée de conservation des données prévue par le responsable du traitement ou critères permettant de la déterminer]. Vous pouvez accéder aux données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données. (en fonction de la base légale du traitement, mentionner également : Vous pouvez retirer à tout moment votre consentement au traitement de vos données ; Vous pouvez également vous opposer au traitement de vos données ; Vous pouvez également exercer votre droit à la portabilité de vos données) Consultez le site cnil.fr pour plus d’informations sur vos droits. Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter (le cas échéant, notre délégué à la protection des données ou le service chargé de l’exercice de ces droits) : [adresse électronique, postale, coordonnées téléphoniques, etc.] Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.”

Conformité au RGPD : Base légale pour le traitement des données

base légale sur laquelle les données personnelles sont traitées. Cela concerne le consentement explicite de l'utilisateur . Afin d'assurer que la collecte de ces données est transparente et que les utilisateurs sont informés de la finalité de la collecte , un message devrait s'afficher à l'ouverture de l'application expliquant que leur données sont collectées et ce message devrait être coché ou non par le visiteur afin d'assurer son consentement explicite à cette collecte .

Les 6 bases légales prévues par le RGPD sont : le consentement, l'exécution d'un contrat (ou les mesures précontractuelles), l'obligation légale, la sauvegarde des intérêts vitaux, la mission d'intérêt public et l'intérêt légitime.

Pour rappel, un traitement correspond à une finalité, il doit donc répondre à une base légale.

Conformité au RGPD : Finalités du traitement des données :

Il est nécessaire de documenter clairement les finalités pour lesquelles on traite les données personnelles. Il est important de s'assurer qu'elles sont en adéquation avec les objectifs déclarés de l'application "Catalogue". Dans ce cadre, les données collectées peuvent contribuer à la recherche médicale.

Conformité au RGPD : Les mesures techniques et organisationnelles mises en place (ou à mettre en place) pour garantir la sécurité des données

Les mesures techniques et organisationnelles pour garantir la sécurité des données personnelles sont essentielles pour se conformer au Règlement Général sur la Protection des Données (RGPD). Les pratiques mises en œuvre sont : Sensibiliser les utilisateurs en leur faisant prendre conscience des enjeux en matière de sécurité et de vie privée par des campagnes de sensibilisation. Les utilisateurs sont également protégés, par la mise en place de mécanismes d'authentification. L'application GSB utilise l'authentification à 2 facteurs (2FA). Voici la procédure à laquelle vous pouvez vous attendre une fois l'authentification 2FA activée.

- Vous accédez au point de connexion via l'application ou le site Web.
- Vous saisissez votre mot de passe.
- Vous êtes invité à fournir le second facteur d'authentification. Il peut s'agir d'un code PIN envoyé à votre adresse électronique ou à votre téléphone par SMS, à moins que vous ne deviez consulter votre application d'authentification.
- Vous saisissez le code.

- Vous avez accès au compte.

rgpd_pages.txt · Dernière modification : 2024/03/18 07:46 de maissane