SAE S3 : Droit RGPD , Brouillon

Fiche n°1 : Identifier les données à caractère personnel (12 / 13 / 17)

- Définition : finalité

- Via définition on sait que les données collectées doivent être pertinentes et limitées à ce qui est strictement nécessaire pour atteindre la finalité.

- Anonymisation

- L'anonymisation des données à caractère personnel permet de rendre impossible toute identification des individus via les données. Lorsque cette anonymisation est réalisée ces données ne sont plus considérées comme données personnelles et les exigences du RGPD ne sont plus applicables.
- Jeux de données brutes = pas anonymes. Toujours utiliser un processus d'anonymisation, que ce soit par [Individualisation | Corrélation | Inférence] ?
- Attention il n'existe pas de solution universelle pour l'anonymisation des données et ces traitements impliquent souvent une perte de qualité sur le jeu de données produit. En conclusion il faut choisir au cas pas par les techniques d'utilisation selon les contextes d'usage et de besoin (risque pour les personnes, utilité des données)

- Pseudonymisation

- Compris entre **conservation des données** brutes et **production de données anonymisées**
- On ne doit plus pouvoir attribuer des données à une personne physique sans avoir recours à des infos supplémentaires. Ces infos supplémentaires doivent être conservées **séparément**.
- En principe on remplace les noms, prénoms, etc.. par des pseudos, des n° d'utilisateurs, etc.. afin de réduire la sensibilité des données. On pense aussi à faire un **hachage cryptographique des données des individus**, tels que son adresse IP, son login et son adresse mail.
- Cependant, ces données sont toujours considérées comme des données à caractère personnel et **restent soumises aux obligations du RGPD**.

Fiche n°2 : Préparer son développement (rgrp fiche 11)

- Choix méthodologiques

- Réaliser une analyse d'impact sur la protection des données (AIPD). Cela nous permettra d'identifier et de traiter tous les risques en amont. Pour ce faire nous pouvons utiliser un site gratuit que la CNIL nous met à disposition : Lien

- Architecture et fonctionnalités

- La sécurisation des données doit influer dès la conception de l'application sur l'architecture et les fonctionnalités. Les paramètres par défaut de l'application doivent respecter les exigences minimales de sécurité mais également être en conformité avec la loi. Pour exemple, la complexité des mots de passe utilisateurs doit respecter au minimum la recommandation de la CNIL relative aux mots de passe.

- Garder un système simple que nous maîtrisons afin d'en assurer le bon fonctionnement
- Avoir plusieurs lignes de défense, sécuriser à plusieurs niveaux. Par exemple lors de la réalisation d'un formulaire en ligne contrôler les entrées n'est que la 1ère ligne de défense.

● Outils et pratiques

- Respecter des normes de codage qui prennent en compte la sécurité.

Fiche n°4: Gérer son code source (regrp fiche 10)

- " Mettez en place des procédures de développement pour travailler efficacement même si plusieurs personnes développent en même temps. Par exemple, vous pouvez décider de ne pas travailler sur la même branche (master ou main), mais de mettre en place des branches par fonctionnalité, qui seront fusionnées dans la branche principale au fur et à mesure du développement. De telles stratégies de développement sont déjà bien documentées, par exemple dans Git Flow. Par ailleurs, certains gestionnaires de code source proposent de configurer des branches protégées qui empêchent des modifications non autorisées sur les fichiers contenus dans ces branches. "

Fiche n°6: Sécuriser vos sites web (regrp 18)

Sécuriser les communications

● Sécuriser les authentifications

- se protéger contre des injections de requêtes illégitimes par rebond.
- Avoir une politique spéciale pour les mots de passe des administrateurs. (mdp entre 3 et 32 caractère avec 1 majuscule)

● Limiter la divulgation..

- Généraliser les messages d'erreurs d'authentification pour qu'on ne pas renseigner sur l'existence d'un compte. ("le compte ou le mdp est erroné")
- Pareil lors de la réinitialisation d'un mot de passe : "Si un compte existe avec cette adresse alors un mail lui a été envoyé pour.."

● Sécuriser les infrastructures

-
- Se protéger des attaques par injection de code SQL ou encore de scripts, etc..

Fiche n°7 : Minimiser les données collectées (rgrp 14)

- Associer des durées de conservation pour chaque catégorie de données, en fonction de la finalité du traitement et des lois associées à leur conservation. Documenter ces durées de conservation.
- Supprimer automatiquement les données à l'expiration de la durée de conservation (possible en SQL). Journaliser ces procédures d'effacement automatique.

Fiche n°8 : Gérer les utilisateurs

- Utiliser des identifiants uniques et propres à chaque individu.
- Authentification obligatoire avant d'avoir accès à des données personnelles.
- Créer des rôles pour des groupes d'utilisateurs, afin que ceux-ci aient différentes possibilités (écriture, lecture, suppression ,etc…) en fonction des besoins.
- Réaliser un système de journalisation (logs) afin de tracer les activités de connexion etc..
- L'utilisation du compte root est à éviter le plus possible car trop dangereux, utiliser un mot de passe fort pour éviter sa compromission.