Retour à Proc#179 - Développement : règles et bonnes pratiques	
Sujets connexes	Proc#15 - Exercice des droits des personnes (RGPD) Proc#181 - Faille de sécurité et violation de données Proc#168 - Chaîne de qualification et de livraison CNIL : guide RGPD du développeur

Protection des données dans le développement

Document technique	Rattaché à Proc#179 - Développement : règles et bonnes pratiques. Non soumis à approbation.

Principe

LoGeAs traite pour ses clients des données personnelles : membres, donateurs, contacts. Pour des associations cultuelles, l'appartenance même à la structure peut révéler une conviction religieuse : **toutes les données personnelles gérées par LoGeAs sont considérées comme sensibles** au sens de l'article 9 du RGPD.
La protection des données est donc prise en compte **dès la conception** de chaque évolution (« privacy by design », article 25 du RGPD), et non après coup. Ces règles s'appliquent à tous les développements : interfaces Angular, serveurs et client lourd.

Règles

Domaine	Règle
Minimisation	On n'ajoute une donnée personnelle que si elle sert une finalité identifiée dans le ticket d'évolution. On préfère une liste de valeurs à un champ libre, et un âge ou une année à une date de naissance quand cela suffit. On ne crée pas de champ appelant une donnée sensible (religion, santé, opinions) non nécessaire au service.
Déclaration	Tout champ contenant une donnée personnelle est déclaré « information nominative » dans le format de la base et apparaît comme tel dans la cartographie fonctionnelle, qui tient lieu de modèle de données (MCD) et de cartographie des flux.
Champs libres	Les champs texte libre (mémo, observations) affichent un rappel : ne pas y saisir de données sensibles ni d'appréciations sur les personnes.
Droits des personnes	Toute nouvelle donnée personnelle est couverte par les fonctions existantes de droit d'accès, de portabilité, de rectification et d'effacement, et leur exécution est tracée dans la piste d'audit. Le développeur vérifie que le nouveau champ est bien repris dans l'export « droit d'accès ».
Consentement	Quand un traitement repose sur le consentement (envoi de courriels, publication), le logiciel en garde la preuve : date, moyen de recueil, et date du retrait éventuel.

Domaine	Règle
Conservation	Une donnée personnelle a une durée de conservation ; une fonction d'archivage ou de suppression est prévue dès la création du champ, en cohérence avec les obligations comptables.
Exports et sauvegardes	Un fichier d'export ou de sauvegarde contenant des données personnelles est chiffré, ou à défaut conservé pour une durée limitée et annoncée à l'utilisateur.
Journaux et erreurs	Les journaux techniques, les messages d'erreur et les traces de débogage (`console.log`) ne contiennent pas de données personnelles ; les traces de débogage sont retirées avant livraison.
Données de test	Les tests et les démonstrations utilisent des bases fictives ou anonymisées. Une base réelle de client n'est copiée sur un poste que pour une intervention demandée, puis supprimée.
Sécurité	Les droits sont contrôlés côté serveur et pas seulement à l'écran ; aucun mot de passe, clé ou secret n'est écrit dans le code ni dans un dépôt Git ; les dépendances sont tenues à jour et leurs vulnérabilités connues corrigées.

Contrôle

- À la création d'un ticket d'évolution touchant des données personnelles, le demandeur précise la finalité.
- Avant fusion, le développeur vérifie les règles ci-dessus ; un écart est signalé dans le ticket.
- Les écarts constatés lors des audits NF 552 sont suivis dans la page de synthèse annuelle des audits.

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
https://wiki-logeas.fr/certif/doku.php?id=certif:procedure:develop:protectiondonnees&rev=1790917856

Last update: **2026/10/02 07:10**