PROTECTION DES DONNÉES PERSONNELLES

BTS SIO Option SLAM — Épreuve E7

Le Règlement Général sur la Protection des Données (RGPD — Règlement UE 2016/679) est applicable depuis le 25 mai 2018. Il constitue le cadre juridique de référence pour tout développeur SLAM manipulant des données à caractère personnel. Sa maîtrise est évaluée dans l'épreuve E7 (Cybersécurité des services informatiques).

1. RGPD : Droits des personnes & Obligations de l'entreprise

1.1 Champ d'application

Le RGPD s'applique à tout traitement de données à caractère personnel dès lors que :

- le responsable de traitement ou le sous-traitant est établi dans l'UE, OU
- les personnes concernées sont situées dans l'UE (principe d'extra-territorialité).

Une donnée à caractère personnel désigne toute information permettant d'identifier directement ou indirectement une personne physique (Art. 4 RGPD) : nom, adresse IP, identifiant de cookie, biométrie, etc.

1.2 Droits des personnes concernées

Droit	Définition	Contrainte technique (SLAM)
Droit d'accès (Art. 15)	Obtenir confirmation du traitement + copie des données	Endpoint GET /user/data — export JSON/CSV
Droit de rectification (Art. 16)	Corriger des données inexactes ou incomplètes	Formulaire d'édition sécurisé + log de modification
Droit à l'effacement (Art. 17)	Obtenir la suppression (« droit à l'oubli »)	Suppression physique ou anonymisation + cascade BDD
Droit à la portabilité (Art. 20)	Recevoir ses données dans un format structuré et lisible par machine	Export XML/JSON/CSV structuré
Droit d'opposition (Art. 21)	S'opposer au traitement à des fins de prospection	Opt-out stocké, filtrage des traitements marketing
Droit à la limitation (Art. 18)	Geler temporairement le traitement sans effacement	Flag is_restricted en BDD, exclusion des traitements actifs
Droit à ne pas subir une décision automatisée (Art. 22)	Refus des décisions fondées uniquement sur profilage	Intervention humaine obligatoire sur décisions sensibles

> *En SLAM : tout droit doit être implémenté via une API ou interface dédiée. Le délai de réponse légal est d'1 mois, extensible à 3 mois pour les demandes complexes.*

1.3 Obligations de l'entreprise (Responsable de traitement)

▸ Principes fondamentaux (Art. 5)

- Licéité, loyauté, transparence : base légale obligatoire (consentement, contrat, obligation légale, intérêt légitime…)
- Limitation des finalités : les données ne peuvent être réutilisées pour d'autres buts
- Minimisation : ne collecter que ce qui est strictement nécessaire
- Exactitude : maintenir les données à jour
- Limitation de conservation : durée maximale définie et respectée
- Intégrité et confidentialité : sécurité technique et organisationnelle
- Responsabilité (accountability) : capacité à démontrer la conformité à tout moment

▸ Désignation d'un DPO (Art. 37)

Le Délégué à la Protection des Données (DPO) est obligatoire pour les organismes publics, les entreprises dont le cœur d'activité implique un suivi à grande échelle ou le traitement de données sensibles. Il est l'interlocuteur de la CNIL.

▸ Analyse d'Impact (DPIA — Art. 35)

Obligatoire pour tout traitement susceptible d'engendrer un risque élevé : biométrie, surveillance systématique, scoring automatique, données de mineurs. La DPIA comprend : description du traitement, évaluation de la nécessité, identification des risques, mesures d'atténuation.

▸ Notification de violation (Art. 33-34)

- Notification à la CNIL : dans les 72h après détection
- Notification aux personnes concernées : si risque élevé pour leurs droits et libertés
- Contenu obligatoire : nature de la violation, catégories de données affectées, conséquences probables, mesures prises

2. Collecte et Traitement des Données

2.1 Quelles données collecter ?

Le principe de minimisation (Art. 5.1.c) impose de ne collecter que les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités. En pratique, pour un développeur SLAM :

Type de données	Exemples	Sensibilité
Identification	Nom, prénom, email, téléphone	Standard
Techniques	IP, cookies, logs de connexion	Standard (pseudonymisation recommandée)
Catégories spéciales (Art. 9)	Santé, biométrie, opinions politiques, religion, orientation sexuelle	⚠ Traitement interdit sauf exception stricte
Données pénales (Art. 10)	Condamnations, infractions	⚠ Réservé aux autorités publiques
Mineurs (Art. 8)	Tout profil < 15 ans (France)	Consentement parental obligatoire

2.2 Base légale du traitement (Art. 6)

Tout traitement doit reposer sur une base légale explicite. L'absence de base légale rend le traitement illicite.

- Consentement : libre, éclairé, spécifique, univoque — recueilli avant traitement — révocable à tout moment
- Exécution d'un contrat : traitement nécessaire à la fourniture du service
- Obligation légale : imposée par une norme juridique (ex : conservation comptable)
- Intérêts vitaux : protection de la vie d'une personne
- Mission d'intérêt public : organismes publics
- Intérêts légitimes : équilibre à démontrer avec les droits de la personne

> *Le consentement en SLAM se matérialise par une case à cocher non pré-cochée, une double confirmation pour les données sensibles, et un mécanisme de retrait simple (bouton de désinscription accessible).*

2.3 Comment stocker les données ?

Architecture de base de données

- Séparation des données d'identification et des données métier (tables distinctes, jointure par UUID interne)
- Chiffrement des colonnes sensibles au niveau applicatif (AES-256) ou via chiffrement transparent de la BDD (TDE)
- Clés étrangères sur UUID non-prédictible (pas d'auto-incrément exposé)
- Journalisation des accès en lecture/écriture sur tables de données personnelles

Exemple de modèle de séparation

Table	Colonnes	Remarque
users_identity	uuid, email_chiffré, nom_chiffré, date_inscription	Accès restreint au module auth
users_profile	uuid_fk, préférences, historique_actions	Pseudonymisé — pas de lien direct
users_consent	uuid_fk, consentement_marketing, date, version_cgu	Audit trail obligatoire
audit_log	user_uuid, action, timestamp, ip_hash	Immuable, rétention 12 mois

2.4 Durées de conservation

La durée de conservation doit être définie avant le traitement et documentée dans le registre. Elle repose sur les phases suivantes :

Catégorie	Conservation active	Archivage intermédiaire	Sort final
Données clients actifs	Durée relation commerciale	5 ans (prescription)	Suppression / anonymisation
Données prospects	3 ans sans contact	Non applicable	Suppression
Logs de connexion	6 mois (LPM)	1 an	Suppression sécurisée
Données RH	Durée contrat + 5 ans	10 ans (retraite)	Archivage définitif anonymisé
Données pénales / fraude	Durée procédure	5 ans	Suppression ou anonymisation
Cookies analytiques	13 mois (CNIL)	Non applicable	Suppression automatique

> *Implémentation SLAM : mise en place d'un job automatique (CRON / scheduler) qui identifie les données expirées et déclenche soit la suppression physique, soit l'anonymisation selon la politique définie.*

3. Mesures de Sécurité Techniques

3.1 Chiffrement

Chiffrement en transit

- TLS 1.2 minimum (TLS 1.3 recommandé) pour toutes les communications HTTP → HTTPS obligatoire
- HSTS (HTTP Strict Transport Security) : header Strict-Transport-Security: max-age=31536000
- Certificats valides (Let's Encrypt ou autorité de certification reconnue)
- Désactivation des suites de chiffrement faibles (RC4, DES, export ciphers)

Chiffrement au repos

- AES-256 pour les données sensibles au niveau applicatif
- Chiffrement transparent de la BDD (TDE : Transparent Data Encryption) — disponible sur MySQL, PostgreSQL, SQL Server
- Chiffrement des sauvegardes : backup chiffré avant transfert vers stockage externe
- Gestion des clés : HSM (Hardware Security Module) ou KMS (AWS/Azure/GCP) — rotation périodique obligatoire

> *En SLAM, pour le chiffrement de colonnes : PHP → openssl_encrypt() / sodium_crypto_secretbox() | Python → Fernet (cryptography lib) | Java → javax.crypto.Cipher AES/GCM*

Hachage des mots de passe

Le hachage n'est PAS un chiffrement — il est irréversible. Utiliser exclusivement :

- bcrypt (facteur de coût ≥ 12) — standard en PHP (password_hash)
- Argon2id — recommandé par l'OWASP et la CNIL pour les nouveaux projets
- PBKDF2 avec SHA-256 (≥ 600 000 itérations) — conforme NIST 2023
- INTERDIT : MD5, SHA-1, SHA-256 seul (sans sel ni itérations) pour les mots de passe

3.2 Anonymisation et Pseudonymisation

Technique	Description	Impact RGPD
Anonymisation	Suppression définitive et irréversible de tout lien avec la personne	Donnée hors champ RGPD — libre d'usage
Pseudonymisation	Remplacement des identifiants par un pseudonyme — ré-identification possible avec clé séparée	Reste une donnée personnelle — allège les obligations
Masquage (masking)	Substitution partielle (ex : jean****@mail.com)	Pseudonymisation partielle — usage en logs, affichage
Généralisation	Remplacement d'une valeur précise par une plage (ex : âge → tranche 30-40)	Réduction du risque de ré-identification
Suppression (suppression d'attributs)	Retrait des colonnes non nécessaires à l'analyse	Minimisation — obligatoire pour jeux de données analytiques

3.3 Contrôle des accès

- Principe du moindre privilège : chaque rôle n'accède qu'aux données strictement nécessaires
- RBAC (Role-Based Access Control) : matrice rôle / ressource documentée
- MFA (Multi-Factor Authentication) pour les accès administrateurs et aux données sensibles
- Gestion des sessions : token JWT à durée limitée (≤ 15 min pour données sensibles), refresh token HttpOnly
- Révocation immédiate des accès en cas de départ ou compromission

3.4 Sauvegardes (Backup)

▸ Règle 3-2-1

- 3 copies des données (1 production + 2 sauvegardes)
- 2 supports différents (disque local + NAS ou Cloud)
- 1 copie hors site / hors ligne (protection contre ransomware)

▸ Exigences SLAM

- Chiffrement des sauvegardes avant stockage (AES-256 minimum)
- Test de restauration périodique obligatoire (documentation du PRA/PCA)
- Journalisation des opérations de backup : date, hash d'intégrité, emplacement
- Durée de rétention des sauvegardes alignée sur la politique de conservation
- Sauvegardes des données personnelles soumises au RGPD : même durée que données actives

3.5 Sécurité applicative (Privacy by Design — Art. 25)

- Validation de toutes les entrées utilisateur : protection injection SQL, XSS, CSRF
- Absence de données personnelles dans les URLs (logs de serveur accessibles)
- Headers de sécurité HTTP : X-Content-Type-Options, X-Frame-Options, CSP, Referrer-Policy
- Variables d'environnement pour les secrets (jamais en dur dans le code)
- Journaux d'audit sans données personnelles en clair (hachage des identifiants dans les logs)

4. Documents Obligatoires

4.1 Registre des Activités de Traitement (Art. 30)

Tenu par le responsable de traitement. Obligatoire pour les organisations de plus de 250 salariés ou traitant des données sensibles ou à risque élevé.

Contenu obligatoire de chaque entrée :

- Identité du responsable de traitement et du DPO
- Finalité du traitement (ex : gestion des commandes, newsletter, RH)
- Catégories de personnes concernées (clients, salariés, prospects…)
- Catégories de données traitées
- Destinataires des données (internes et sous-traitants)
- Transferts hors UE : pays de destination, garanties (clauses contractuelles types, adéquation)
- Durée de conservation
- Description des mesures de sécurité techniques et organisationnelles

Traitement	Finalité	Base légale	Données	Durée	Sécurité
Gestion clients	Suivi commandes	Contrat	Email, adresse, historique	5 ans	TLS, AES, RBAC
Newsletter	Marketing	Consentement	Email, préférences	3 ans sans clic	Opt-out, chiffrement
Logs applicatifs	Sécurité système	Intérêt légitime	IP hashée, actions	6 mois	Pseudonymisation

4.2 Politique de Confidentialité (Privacy Policy)

Document public, accessible avant toute collecte. Rédigé en langage clair et compréhensible (Art. 13-14).
Mentions obligatoires :

- Identité et coordonnées du responsable de traitement
- Coordonnées du DPO (si désigné)
- Finalités et base légale de chaque traitement
- Intérêts légitimes poursuivis (si base = intérêt légitime)
- Destinataires ou catégories de destinataires
- Transferts hors UE et garanties applicables
- Durées de conservation
- Droits des personnes et modalités d'exercice (contact DPO ou adresse dédiée)
- Droit de retirer le consentement à tout moment
- Droit d'introduire une réclamation auprès d'une autorité de contrôle (CNIL en France)
- Existence d'une prise de décision automatisée et logique sous-jacente

4.3 Autres documents clés

Document	Objectif	Acteur SLAM concerné
Contrat de sous-traitance (DPA)	Encadrer juridiquement tout sous-traitant accédant aux données (Art. 28)	Tout prestataire cloud, API tiers
Analyse d'impact (DPIA)	Évaluer les risques avant mise en production d'un traitement à risque élevé	Développeur + DPO + RSSI
Procédure de gestion des violations	Protocole de réponse en cas de fuite ou incident (Art. 33)	RSSI, DPO, équipe dev
Charte informatique interne	Encadrer l'utilisation des outils numériques par les collaborateurs	Tous les salariés
Politique de mots de passe	Définir les règles de complexité, rotation, stockage	Équipe technique
Formulaires de consentement	Preuve légale du consentement avec horodatage et version de la politique	Interface utilisateur (front SLAM)

POINTS CLÉS POUR L'ÉPREUVE E7

Ce que l'examinateur attend d'un développeur SLAM :

- Connaître et citer les articles RGPD pertinents (Art. 5, 6, 13, 17, 20, 25, 30, 32, 33, 35)
- Lier les obligations légales à des implémentations techniques concrètes (hachage, chiffrement, RBAC, API de droits…)
- Distinguer anonymisation (hors RGPD) et pseudonymisation (reste soumis au RGPD)
- Justifier les durées de conservation par rapport aux bases légales et archivages intermédiaires
- Maîtriser le contenu du registre des traitements et de la politique de confidentialité
- Connaître les sanctions CNIL : jusqu'à 20 M€ ou 4 % du CA mondial annuel (Art. 83)