Catalogue des Exigences en Matière de Confidentialité

Introduction

Ce catalogue définit un ensemble d'exigences essentielles pour garantir la protection des données personnelles et la confidentialité des utilisateurs. Il est aligné sur le Règlement Général sur la Protection des Données (RGPD), la Loi Organique Espagnole sur la Protection des Données Personnelles et la Garantie des Droits Numériques (LOPDGDD), le Schéma National de Sécurité (ENS), ISO/IEC 27001 et IEEE 29148. L'objectif est de fournir des directives concrètes permettant aux équipes techniques, juridiques et d'audit d'intégrer la protection des données dès la conception des systèmes et de garantir leur conformité aux réglementations en vigueur.

Catégories des Exigences en Matière de Confidentialité

1. Gestion du Consentement de l'Utilisateur

PRIV-001 : Obtention du Consentement Explicite

Description : Le consentement explicite des utilisateurs doit être obtenu avant tout traitement des données personnelles, conformément à l'article 6 du RGPD. Ce consentement doit être donné librement, de manière informée, spécifique et sans ambiguïté.
Critères d'Acceptation :

- La demande de consentement comprend une case à cocher explicite (non pré-cochée).
- Un journal des consentements avec horodatage est conservé.
  Priorité : Élevée
  Source : RGPD Article 6, LOPDGDD Article 6

PRIV-002 : Retrait du Consentement

Description : Les utilisateurs doivent pouvoir retirer leur consentement à tout moment, et ce retrait doit être aussi simple que son octroi.
Critères d'Acceptation :

- Un mécanisme clair et accessible pour le retrait du consentement.
- Effet immédiat sur le traitement des données après le retrait.
  Priorité : Élevée
  Source : RGPD Article 7

2. Droits des Utilisateurs

PRIV-003 : Droit d'Accès

Description : Les utilisateurs doivent avoir le droit d'accéder à leurs données personnelles et d'en obtenir une copie sur demande. Le système doit fournir une interface permettant cet accès.
Critères d'Acceptation :

- Interface utilisateur pour les demandes d'accès.
- Données fournies dans un délai de 30 jours.
  Priorité : Élevée
  Source : RGPD Article 15, LOPDGDD Article 13

PRIV-004 : Droit à l'Effacement (Droit à l'Oubli)

Description : Les utilisateurs doivent pouvoir demander la suppression de leurs données personnelles lorsqu'elles ne sont plus nécessaires ou s'ils retirent leur consentement.
Critères d'Acceptation :

- Vérification de l'éligibilité à la suppression.
- Suppression sécurisée des données.
  Priorité : Élevée
  Source : RGPD Article 17, LOPDGDD Article 15

3. Minimisation et Conservation des Données

PRIV-005 : Minimisation des Données

Description : Le système ne doit collecter que les données personnelles strictement nécessaires à l'objectif visé.
Critères d'Acceptation :

- Vérification des champs obligatoires avant la collecte.
- Justification pour chaque champ de données collectées.
  Priorité : Moyenne
  Source : RGPD Article 5(1)(c)

PRIV-006 : Politique de Conservation des Données

Description : Les données personnelles ne doivent être conservées que pendant la durée strictement nécessaire. Une politique de conservation des données doit être en place.
Critères d'Acceptation :

- Périodes de conservation définies pour chaque type de données.
- Mécanismes d'effacement automatique des données.
  Priorité : Élevée
  Source : RGPD Article 5(1)(e), LOPDGDD Article 32

4. Mesures de Sécurité

PRIV-007 : Stockage Sécurisé des Données

Description : Les données personnelles doivent être stockées de manière sécurisée à l'aide de techniques de chiffrement et de contrôles d'accès.
Critères d'Acceptation :

- Chiffrement des données selon des normes approuvées.
- Mise en œuvre d'un contrôle d'accès basé sur les rôles.
  Priorité : Élevée
  Source : RGPD Article 32, ISO/IEC 27001

PRIV-008 : Notification des Violations de Données

Description : Les organisations doivent notifier l'autorité de protection des données et les utilisateurs concernés en cas de violation de données.
Critères d'Acceptation :

- Mise en place d'un plan de réponse aux incidents.
- Notification envoyée dans un délai de 72 heures après détection.
  Priorité : Élevée
  Source : RGPD Article 33, ENS Article 25

PRIV-09 : Gestion des Accès des Utilisateurs

Description : Les accès aux données personnelles doivent être limités aux seules personnes autorisées et doivent être régulièrement révisés.
Critères d'Acceptation :

- Attribution des droits d'accès basée sur le principe du moindre privilège.
- Journalisation et audit des accès aux données personnelles.
  Priorité : Élevée
  Source : ISO/IEC 27001

5. Transferts Internationaux de Données

PRIV-010 : Conformité aux Transferts Internationaux

Description : Les données personnelles ne peuvent être transférées hors de l'UE que si le pays destinataire garantit un niveau de protection adéquat ou si des garanties appropriées sont mises en place.
Critères d'Acceptation :

- Vérification de la décision d'adéquation ou clauses contractuelles types.
- Documentation des accords de transfert.
  Priorité : Élevée
  Source : RGPD Article 44

6. Protection de la Vie Privée dès la Conception et par Défaut

PRIV-011 : Mise en Œuvre de la Protection de la Vie Privée dès la Conception

Description : Les considérations en matière de confidentialité doivent être intégrées dès la phase de développement des produits et services.
Critères d'Acceptation :

- Réalisation d'une analyse d'impact sur la vie privée pour les nouveaux systèmes.
- Intégration de techniques de protection de la vie privée dans le développement.
  Priorité : Élevée
  Source : RGPD Article 25, IEEE 29148