Université Saint-Joseph de Beyrouth
جامعة القدّيس يوسف في بيروت

Politique de protection des données dès la conception et par défaut

Texte approuvé par le Conseil de l'Université lors de sa 216e réunion en date du 18 octobre 2022

Objet (objectif, avantages, cadre)

L'objectif de cette politique est de définir les principes adoptés par l'Université Saint-Joseph de Beyrouth (ci-après : l'Université) pour la protection des données dès la conception et tout au long de leur durée de conservation. Elle vise de même la protection des données par défaut.

La présente politique permet à l'Université d'envisager la protection des données pour assurer la protection de la vie privée et garantir à cet effet le respect des lois et règlements en vigueur, notamment le règlement général sur la protection des données (RGPD).

Cette politique s'applique à tous les membres du PSG et les enseignants de l'Université.

Directeur/Gérant

Responsable de la sécurité des systèmes d'information (Chief information security officer-CISO, ci-après le RSSI).

Utilisateurs

Membres du PSG et enseignants

Rôles et devoirs

RSSI
Le RSSI a pour rôle de veiller au respect de la présente politique par les différentes parties prenantes.

Utilisateurs
Les utilisateurs doivent se conformer aux recommandations et exigences de la politique définie ci-après.

Description

Principes généraux

Les principes généraux de la protection des données à caractère personnel à l'Université se résument comme suit :

1. Être vigilant, proactif et non réactif, afin de détecter les incidents liés à l'atteinte à la vie privée avant leur survenance.
2. Considérer la protection des données comme un paramètre par défaut, en spécifiant la finalité du traitement, limitant la collecte des données, minimisant les données partagées et détruisant les données lorsqu'elles ne servent plus leur objectif initial.
3. Intégrer la protection des données dès la conception dans l'architecture des systèmes informatiques et dans toutes les opérations quotidiennes.
4. Garantir la protection de la vie privée et la sécurité des données sans aucun compromis pour assurer d'autres fonctionnalités.
5. Assurer la sécurité des données de bout en bout pendant toute la période de conservation, depuis leur collecte jusqu'au moment de leur destruction.
6. Assurer une transparence totale à l'égard des personnes concernées en leur communiquant le traitement de leurs données à caractère personnel de manière claire et cohérente.
7. Respecter la vie privée et préserver le meilleur intérêt des personnes concernées en leur proposant des mesures appropriées telles que des paramètres par défaut stricts en matière de confidentialité, des avis appropriés et des options d'activation conviviales.

Protection des données dès la conception

L'Université adopte le principe de protection des données dès la conception pour garantir la confidentialité et la protection des données tout au long du cycle de vie, depuis la conception de tout système, service, produit ou processus, jusqu'à la destruction des données.
Les utilisateurs doivent assurer en permanence la sécurité des systèmes et des données au sein de l'Université pour éviter les risques de violation des données, surtout lors de l'utilisation des appareils mobiles et des connexions à distance.

Protection des données par défaut

L'Université garantit que, par défaut, seules les données à caractère personnel nécessaires à chaque finalité spécifique du traitement sont traitées, y compris la quantité de données collectées, l'étendue de leur traitement, leur durée de conservation et leur accessibilité. Lors de la collecte des données, les paramètres par défaut doivent être clairs, conviviaux et stricts en matière de confidentialité.

Partage de données

Tout traitement et transfert de données à caractère personnel doit être effectué en toute sécurité. En outre, et en vue d'être conforme au RGPD, les demandes d'informations doivent être approuvées par le Data Protection Officer (DPO) avant leur transmission aux propriétaires des données concernés. Ainsi, toute demande de données sollicitée par un service ou une institution nécessite l'envoi du Formulaire de demande de données en précisant les informations demandées et la finalité du traitement. Une fois l'accord du DPO obtenu, le propriétaire des données demandées peut les envoyer au demandeur. Il faudra toujours veiller à ne partager que le nombre minimal de données requis pour effectuer le traitement en question. Il est également recommandé d'appliquer l'anonymisation ou la pseudonymisation (anonymisation réversible) aux données à caractère personnel, afin de réduire les risques de fuite de données.

Solutions tierces

Avant l'achat de systèmes ou de plateformes impliquant des données à caractère personnel, y compris l'utilisation du cloud, la confidentialité et la sécurité des données doivent être évaluées, pour éviter que des données ne soient exposées à un risque de violation. Les données à caractère personnel ne doivent être placées sur ces systèmes sans l'accord du DPO conformément aux politiques et règlements de l'Université, notamment la politique de sécurité de l'information. La durée de conservation de ces données doit être réduite au minimum.

Bonnes pratiques pour réduire les risques de fuite de données

- Obtention du consentement des personnes concernées avant tout traitement de données.
- Utilisation des avis de confidentialité pour assurer une transparence à l'égard des personnes concernées.
- Limitation de l'accès aux données à caractère personnel à ceux qui en ont besoin.
- Vérification des destinataires avant tout envoi de courriels.
- Suppression régulière des données à caractère personnel après l'achèvement de la finalité du traitement ou de la période de conservation.
- Minimisation de la collecte, du stockage, de l'utilisation et de la transmission des données à caractère personnel autant que possible.
- Anonymisation totale et irréversible des données à caractère personnel lorsque chaque fois que pareille mesure serait possible.
- Pseudonymisation des données à caractère personnel et conservation de la clé dans un lieu sécurisé.
- Chiffrement des documents (Excel, Word, etc.) contenant des données à caractère personnel.
- Stockage des documents sur support papier contenant des données à caractère personnel dans des espaces sécurisés (coffres-forts, armoires fermées à clé, tiroirs verrouillés ou autre).

Norme, conseil, références

Règlement général sur la protection des données (RGPD)

Formulaires relatifs à cette procédure

Données connexes	Titre de la donnée connexe
Politique	Politique de sécurité de l'information (CISO-PL-01)
Lexique	**Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable. **Anonymisation** : rendre impossible et d'une façon irréversible l'identification d'une personne. **Pseudonymisation** : remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, numéro séquentiel, etc.). En cas de besoin, l'opération de pseudonymisation pourrait être réversible, contrairement à l'anonymisation. **Chiffrement** : protéger les documents sauvegardés par un mot de passe.
Abréviations	**CISO** : Chief Information Security Officer RSSI : Responsable de la sécurité des systèmes d'information **PSG** : Personnel des Services Généraux **DPO** : Data Protection Officer **RGPD** : Règlement Général sur la Protection des Données