Protection des données

Bref aperçu

DÉFINITION

Ensemble de principes et de pratiques visant à garantir que les données à caractère personnel soient collectées, utilisées et protégées, d'une manière qui tienne compte la vie privée des personnes et des risques qu'elles peuvent encourir, si leurs données ne sont pas protégées de manière adéquate.

CONCEPTS

Traitement : operations de gestion des données concernant les données personnelles, y compris la collecte, le stockage, l'accès, l'analyse, la suppression, etc.

Données personnelles : informations qui se rapportent à une personne physique vivante identifiée ou identifiable : nom, adresse, sexe, âge, numéro d'un document d'identité, photographie, empreinte digitale, etc. Également des informations plus sensibles : état de santé, appartenances religieuses ou politiques, ou orientation sexuelle. Il est important de signaler que cette liste n'est pas exhaustive, ce qui est considéré comme personnel, voire comme sensible, peut changer selon le contexte politique, social ou économique.

Partage : fournir un accès à l'information en l'envoyant par courrier électronique, en fournissant un lien vers des données numériques, en faisant une copie et en la fournissant à quelqu'un, en fournissant un accès direct ou indirect à une base de données.

BONNES PRATIQUES GÉNÉRALES

CORRECT

- Identifier quelles sont les données personnelles qu'il est absolument nécessaire de collecter avant de mettre en œuvre un projet.
- Tenir compte des coutumes locales et du contexte politique pour déterminer quelles données personnelles collecter et comment expliquer le(s) but(s) de la collecte.
- Tenir compte du fait que les données de localisation et les données démographiques, même si elles ne sont pas nécessairement personnelles, peuvent être très sensibles et faire courir des risques aux individus et/ou à des groupes de personnes.
- Déterminer quelles informations seront fournies aux personnes concernées. Par exemple : le but du projet, pourquoi les données doivent être collectées, de quelle façon elles seront utilisées et avec qui elles seront partagées, où s'adresser si il ou elle a des questions sur ses propres données personnelles.
- Lors de la fourniture d'informations, ou l'obtention d'un consentement, consigner les interactions, notamment: quelles informations ont été fournies, qui les a données, la date et le lieu, le public, si des objections ont été soulevées.
- Déterminer qui sera chargé de répondre aux questions concernant l'utilisation, le stockage, la correction, etc. des données personnelles.
- Crypter et/ou protéger par mot de passe les appareils et les fichiers numériques (word, excel, etc.) contenant des données personnelles (ou autres données sensibles).
- Planifier ce qu'il adviendra des données personnelles lorsqu'elles ne seront plus nécessaires. Par exemple, seront-elles archivées, peuvent-elles être supprimées/détruites en toute sécurité ?
- Donner uniquement accès aux fichiers numériques ou papier contenant des données personnelles aux membres du personnel (ou aux bénévoles, consultants ou autres agents autorisés) qui en ont besoin pour accomplir leurs taches.
- Maintenir des mots de passe, des verrous physiques, une protection antivirus, des pare-feux et toute autre forme raisonnable de sécurité pour les ordinateurs, les téléphones portables, les classeurs ou tout autre endroit où des données personnelles seront stockées.
- Prévoir l'établissement d'un accord écrit avant de partager toute donnée personnelle (ou autre donnée sensible) en dehors de votre organisation.

À NE PAS FAIRE

- Utiliser les dossiers publics Dropbox ou Google Drive/Docs accessibles au public ou d'autres plateformes Internet pour partager ou collaborer sur des documents contenant des données personnelles (ou d'autres données sensibles), en particulier lorsque ces documents en ligne ne sont pas protégés par un mot de passe.
- Partager ou donner accès à des fichiers contenant des données à caractère personnel à des gouvernements, ou à tout autre partenaire, sans en avoir préalablement étudié les conséquences et sans avoir formalisé les conditions de ce partage.
- Publier des données personnelles (y compris des photographies) de personnes concernées sur des comptes de médias sociaux, que ce soit à titre personnel ou professionnel, sans accord préalable avec les équipes de communication et juridiques de votre organisation.
- Laisser les fichiers contenant des données personnelles (ou d'autres données sensibles) sans protection. Les stocker dans des armoires, des tiroirs, des bureaux lorsqu'ils ne sont pas utilisés.
- Utiliser des dispositifs de stockage USB pour les données personnelles (ou autres données sensibles), à moins que leur contenu ne soit protégé par un mot de passe et/ou crypté.
- Partir du principe que le simple fait de demander à une personne son consentement, ou de lui demander son accord pour une action impliquant l'utilisation de ses données personnelles, est juridiquement ou moralement suffisant pour agir. Le consentement ne peut pas être donné librement lorsque la fourniture de l'aide nécessaire est conditionnée par celui-ci.

Il convient de noter que la présente note d'information ne prétend pas être exhaustive et qu'il existe de nombreux domaines de la protection des données qui ne sont pas couverts par le présent document. Il faut toujours demander l'avis d'un conseiller juridique en cas de doute sur l'interprétation et/ou la mise en œuvre des pratiques de protection des données

IFRC

Préparé par le bureau de la PD de la FICR.

Coordonnées :

Gestion de l'information
FICR HQ, Genève
im@ifrc.org