IDEUZO
at_work

Politique RGPD interne

Mise à jour le 03/12/2024

Tableau de révision de la politique interne

Version	**Date de modification**	Rédacteur	Eléments modifiés
V1	03/12/2024	Elodie F	Création du document
V2	30/01/2025	Elodie F.	Changement d'assurances Cyber

1 Objectif de notre politique de gestion des données personnelles

Afin d'être en conformité avec le RGPD et ainsi ne pas encourir de sanctions pour non-conformité Ideuzo souhaite sensibiliser ses collaborateurs sur l'intérêt :

- de restreindre la collecte des données à caractère personnel aux données strictement nécessaires à son activité ;
- d'encadrer, en interne, l'accès auxdites données collectées (le collaborateur doit avoir accès uniquement aux données nécessaires pour travailler efficacement).

L'objectif est évidemment d'éviter qu'elles ne soient perdues, volées ou compromises, de façon à ne nuire à personne : ni à nos clients, ni à nos fournisseurs, ni à nos collaborateurs et évidemment ni à la réputation d'IDEUZO.

2 Champ d'application de notre politique

2-1 Dans le champ d'application

La politique interne RGPD IDEUZO s'applique à l'ensemble des données personnelles collectées et ce qu'elle que soit le canal de collecte et le « lieu » de stockage : serveurs, bases de données et systèmes informatiques qui traitent ces données, y compris tout appareil régulièrement utilisé pour le courrier électronique, l'accès au Web ou d'autres tâches professionnelles.

2-2 Hors du champ d'application

Les données qui ne présentent pas un caractère personnel ou les informations classées comme publiques ne sont pas soumises à la politique interne RGPD IDEUZO.

3 Notre politique RGPD

3-1 Généralités

a. Chaque collaborateur est identifié par un ID utilisateur unique, afin que tous puissent être tenus pour responsables de leurs actions.

b. Chaque utilisateur doit lire la présente politique de sécurité des données, ainsi que les directives de connexion et de déconnexion, et signer une déclaration stipulant qu'il en a pris connaissance et qu'il les a comprises.

c. Les accès doivent être accordés selon le principe du moindre privilège, ce qui signifie que chaque programme et chaque utilisateur obtiendra seulement les droits d'accès qui lui sont nécessaires pour effectuer son travail.

3-2 Autorisation de contrôles d'accès

L'accès aux ressources et aux services informatiques de l'entreprise sera accordé par le biais d'un compte d'utilisateur unique et d'un mot de passe complexe. Le service informatique fournis les comptes d'après les documents d'activité du service RH.
Les mots de passe sont gérés par le centre d'assistance informatique. Les exigences relatives à la longueur, à la complexité et à l'expiration des mots de passe seront pilotées par notre prestataire informatique. Les consignes de ce-dernier devront être appliquées sans délai.

3-3 Accès aux réseaux

Un accès aux réseaux est accordé à tous les collaborateurs selon les procédures de contrôle d'accès de l'entreprise et le principe du moindre privilège.

3-4 Responsabilités des utilisateurs

a. Tous les utilisateurs doivent verrouiller leur écran chaque fois qu'ils quittent leur bureau, pour réduire le risque d'accès non autorisé.

b. Tous les utilisateurs doivent veiller à ne laisser aucune information sensible ou confidentielle autour de leur poste de travail.

c. Tous les utilisateurs doivent tenir leurs mots de passe confidentiels et ne pas les partager.

d. Application de la politique: tout utilisateur qui enfreint cette politique est passible de sanctions disciplinaires.

3-5 Accès aux informations confidentielles et restreintes

L'accès aux données classées comme « confidentielles » ou « d'accès restreint » doit être limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, tel que déterminé par la direction.

3-6 Assurance Cyber Sécurité

IDEUZO a souscrit une assurance CYBER SECURITE garantissant les conséquences financières des risques immatériels pouvant affecter les systèmes informatiques, et les données personnelles des clients et des collaborateurs de l'entreprise assurée.

Couvertures et engagements

L'assurance cyber Stoïk nous permet de renforcer notre stratégie de gestion des risques informatiques grâce aux garanties suivantes :

- Plafond global : Une couverture jusqu'à 1 000 000 € par période d'assurance.
- Franchise : 5 000 € par sinistre, avec une réduction de 25 % si l'ensemble des outils de prévention Stoïk Protect sont en place.

Garanties principales

Notre assurance cyber offre des garanties essentielles pour protéger les données personnelles et assurer la continuité de nos activités :

- Gestion de crise et remise en état du système en cas d'incident de cybersécurité.
- Frais de notification et surveillance suite à une fuite de données, conformément aux obligations du RGPD.
- Indemnisation des pertes d'exploitation jusqu'à 6 mois (délai de carence de 12h).
- Protection contre la cyber-extorsion et la cyber-fraude (limitée à 10 % du montant des garanties, avec un maximum de 50 000 €).
- Responsabilité civile en cas d'atteinte aux données personnelles ou de transmission de virus.
- Couverture des sanctions administratives éventuellement imposées par la CNIL.

En plus des garanties financières, notre assurance cyber inclut un accompagnement technique préventif et réactif :

- Assistance 24/7 avec une hotline dédiée et une équipe spécialisée en gestion des incidents.
- Accès à la plateforme Stoïk Protect, comprenant :
  - Un scan hebdomadaire des vulnérabilités externes.
  - Une analyse des configurations Cloud et Active Directory.
  - Des simulations de phishing pour sensibiliser les employés.
  - Des modules de formation à la cybersécurité

.