Description générale des mesures de sécurité techniques et organisationnelles

Responsable du traitement des données

Dénomination	Assurance en Direct Entreprise individuelle
Adresse	41 rue de la découverte 31670 LABEGE
Numéro d'entreprise	45386718600034
Téléphone	0582952159
Adresse e-mail	contact@assuranceendirect.com
Site web	https://www.assuranceendirect.com/

Coordonnées du représentant du responsables du traitement des données

Nom	RICOUARD SAMUEL
Adresse	41 rue de la découverte 31670 LABEGE
Téléphone	0582952159
Adresse e-mail	contact@assuranceendirect.com

Ce document vise à présenter de façon synthétique l'ensemble des mesures de sécurité techniques et organisationnelles mises en place au sein de l'entreprise pour garantir la protection des données et assurer en permanence la confidentialité, l'intégrité et la disponibilité des produits et services de l'entreprise.

Cette description répond aux obligations découlant de l'article 32 du règlement européen sur la protection des données (RGPD).

Merci de cocher les affirmations qui correspondent aux mesures de sécurité et d'organisation mises en place au sein de votre entreprise.

Authentification et habilitation

- ❑ Politique interne permettant de garantir que seules les personnes habilitées peuvent accéder aux données personnelles
- ❑ Utilisation d'un login unique par utilisateur
- ❑ Revue annuelle des habilitations
- ❑ Utilisation de mots de passe et d'identifiant pour authentifier les connexions
- ❑ Règles visant des mots de passe minimum
- ❑ Changement régulier des mots de passe
- ❑ Utilisation d'un historique de mots de passe de façon à interdire la réutilisation des mots de passe
- ❑ Base de données des mots de passe hashée ou cryptée
- ❑ Limitation de nombre de tentatives d'accès à un compte
- ❑ Utilisation de questions secondaires, codes, tokens, PIN pour renforcer la sécurité d'une partie de son réseau ou de son système
- ❑ Mise en place d'un processus pour l'attribution, la gestion et la révocation des accès aux données
- ❑ Conservation d'une liste des utilisateurs des données
- ❑ Suppression des utilisateurs inactifs et des permissions d'accès obsolètes
- ❑ Le responsable du traitement utilise une double authentification
- ❑ Allocation de privilèges administratifs seulement sur demande

Organisation interne

- ❑ Le responsable de la sécurité fait partie de l'équipe de direction
- ❑ Si autre, précisez :

Politiques internes et procédures

- ❑ Politique interne en relation avec la sécurité des données
- ❑ Politique de rétention et de suppression des données à caractère personnel
- ❑ Existence de processus définis pour répondre aux incidents de sécurité
- ❑ Existence de processus définis pour apporter les modifications à ses réseaux et systèmes informatiques
- ❑ Utilisation de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
- ❑ Utilisation des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
- ❑ Utilisation des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement
- ❑ Le responsable du traitement a mis en place une politique de destruction sécurisée des données confidentielles, notamment électroniques, sur papier et sur médias amovibles
- ❑ Si autre, précisez :

Connexion

- ❑ Verrouillage automatique des sessions
- ❑ Message d'avertissement avant toute connexion indiquant que les systèmes sont réservés au personnel autorisé
- ❑ Conservation d'une journalisation des accès à ses applications, aux opérations et aux connexions à ses applications et exploitation ces journaux
- ❑ Si autre, précisez :

Sécurité et anti-virus

- ❑ Réalisation de la pseudonymisation des données à caractère personnel
- ❑ Utilisation de méthode de cryptage pour protéger la transmission des données
- ❑ L'accès aux données n'est fourni que sur la base des stricts besoins
- ❑ Les serveurs et les PC internes du responsable du traitement sont séparés du web et des autres réseaux externes par des pare-feu et/ou d'autres moyens
- ❑ Révision régulière des règles sécurité et des alertes
- ❑ Tous les systèmes sont protégés par des anti-virus
- ❑ Les signatures des antivirus utilisés par le responsable du traitement sont mises à jour
- ❑ Mises à jour de sécurité des systèmes d'exploitation et des applications pour tous les systèmes
- ❑ Les mises à jour sont appliquées au moins mensuellement
- ❑ Les données informatiques sont protégées contre la perte ou la corruption par des sauvegardes régulières conservées séparément
- ❑ Si autre, précisez :

Information et sensibilisation

- ❑ Les utilisateurs ayant accès aux données sont informées et sensibilisés à la valeur des données dans un objectif de sécurité
- ❑ Les utilisateurs sont informés et sensibilisés quant aux procédures internes en matière de sécurisation des données
- ❑ Les utilisateurs sont formés à la protection des données à caractère personnel
- ❑ Si autre, précisez :

Connexion externe et Wi-fi

- ❑ Sécurisation des appareils informatiques nomades via des systèmes appropriés (ouverture d'accès interne, VPN, etc.)
- ❑ Les réseaux sans fil du responsable du traitement utilisent des protocoles de cryptage et d'accès
- ❑ Mise en place de protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
- ❑ Si autre, précisez :

Continuité des services

- ❑ Des plans de reprise ont été prévus
- ❑ Les plans de reprise sont testés régulièrement
- ❑ Le responsable du traitement a mis en place des accords afin de garantir la continuité des services
- ❑ Si autre, précisez :

Équipement mobile

- ❑ Mot de passe pour les équipements mobiles
- ❑ Chiffrement des équipements mobiles
- ❑ Si autre, précisez :

Protection physique matériel informatique

- ❑ Le matériel informatique est protégé grâce à un accès physique sécurisé
- ❑ Les accès physiques du matériel informatique sont répertoriés
- ❑ Le matériel informatique est protégé en cas de panne de courant
- ❑ Si autre, précisez :

Site Web

- ❑ Le site web du responsable du traitement est protégé par un pare-feu
- ❑ Le *front end* du site web du responsable du traitement est séparé des bases de données et des réseaux locaux
- ❑ Réalisation de scans de vulnérabilité du site web au moins chaque trimestre
- ❑ Réalisation des tests de pénétration au moins chaque année
- ❑ Les données du responsable du traitement sont accessibles via le site web
- ❑ Les parties sensibles du site web du responsable du traitement sont protégées par un cryptage renforcé
- ❑ Si autre, précisez :

Procédure de violation des données à caractère personnel

- ❑ Procédure de notification en cas de violation des données à caractère personnel
- ❑ Si autre, précisez :