Notaire Olivier LEBRUN

Politique de sécurité de l'information

Version	Date	Changements	Auteur
1.0	2018-03-20	Document initial	Privanot
2.0	2022-12-08	Mises à jour diverses	Privanot

Table des matières

1. Préambule

a. Coordonnées de l'organisme

Dénomination : ETUDE DU NOTAIRE OLIVIER LEBRUN

Adresse : rue du 28 juin 1919, numéro 17 à 6180 Courcelles.

b. Coordonnées du délégué à la protection des données

Dénomination : Privanot asbl.

Adresse : Rue de la Montagne 32, 1000 Bruxelles.

Email : info@privanot.be.

c. Objectifs de la politique

La présente politique garantit, conformément aux obligations prévues par le Règlement Général à la protection des données (UE) 2016/679 et les autres lois en vigueur que les mesures techniques et organisationnelles appropriées ont été mises en place de façon à être opérationnelles, de manière à assurer un niveau de protection adéquat des données à caractère personnel traitées tout en tenant compte :

- de la nature des données à caractère personnel traitées et de leur traitement ainsi que des exigences en matière de confidentialité, intégrité et disponibilité ;
- des exigences légales ou réglementaires d'application ;
- de la taille de l'organisme ;
- de l'importance et de la complexité des systèmes d'information, systèmes informatiques et applications concernés ;
- de l'ouverture de l'organisme vers l'extérieur ainsi que des accès depuis l'extérieur ;
- des risques encourus tant pour l'organisme lui-même que pour les personnes dont les données à caractère personnel sont traitées ;
- de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures.

Spécifiquement, la présente politique garantit la protection des données récoltées auprès des diverses sources officielles auxquelles l'organisme à accès.

De manière plus générale, la présente politique permet également de garantir la protection des autres données à caractère personnel et de l'information traitées par l'organisme.

2. Evaluation des risques

Une évaluation des risques encourus a été réalisée et les mesures de protection des données ont été définies en conséquence dans un plan d'actions.

Les traitements de données à caractère personnel sont documentés et repris dans un registre spécifique : le « registre des traitements ».

3. Classification de l'information

Information confidentielle

L'information dont la diffusion libre et sans restriction, la modification, l'utilisation abusive ou la mauvaise utilisation entraineraient un impact négatif significatif sur l'organisme est considérée comme confidentielle. La majorité des données à caractère personnel sont par nature considérées comme confidentielles.

Information interne

L'information dont la diffusion libre et sans restriction, la modification, l'utilisation abusive ou la mauvaise utilisation entraineraient un impact négatif sur l'organisme est considérée comme interne.

Information publique

L'information dont la diffusion libre et sans restriction n'entraineraient pas d'impact négatif sur l'organisme est considérée comme publique.

4. Information du personnel

Le personnel interne et externe impliqué par la présente politique a été informé de ses devoirs de confidentialité et de sécurité vis-à-vis des informations traitées découlant aussi bien des différentes exigences légales que de la politique de sécurité de l'information.

Le personnel interne et externe directement concerné par les traitements d'informations est suffisamment informé des obligations en matière de sécurité et de protection des données.

Des instructions découlant de la politique de sécurité de l'information et du règlement de travail précisent les règles spécifiques à suivre pour la protection de l'information et les règles d'utilisation du matériel informatique ainsi que la procédure de contrôle mise en place par l'employeur, notamment dans le cadre de l'utilisation des emails et de l'internet.

5. Identification des supports d'information

Les supports d'information sont placés dans des locaux identifiés et protégés dont l'accès est limité aux seules personnes autorisées.

Les supports et systèmes d'informations impliquant les stockage d'informations sont les suivants :

- Serveurs installés au sein de l'organisme ;

Aucune information confidentielle ou interne n'est conservée sur le disque dur local d'un poste de travail ou sur un support mobile (clé USB, portable, tablette etc.) sauf si cela s'avère strictement nécessaire à l'accomplissement de la mission professionnelle de l'utilisateur qui a obtenu une autorisation formelle en ce sens de son supérieur hiérarchique, et si les données stockées sur ce support sont chiffrées. Les données sont détruites dès que leur utilisation n'est plus nécessaire à l'accomplissement de la mission poursuivie.

6. Sécurisation physique des accès

Des mesures de sécurité adéquates ont été mises en place afin de prévenir les accès physiques non autorisés aux supports et systèmes d'informations impliquant le traitement d'information.

Site – Rue du 28 juin 1919 à 6180 COURCELLES

i. Accès à l'organisme

L'organisme est ouvert du lundi ou vendredi, sauf les jours fériés :

- Ouverture des portes extérieures du lundi au vendredi de 8h00 à12h00
- Bureaux fermés : toutes les après-midis.
- Préciser les règles d'accès pour les visiteurs (en sonnant, en s'annonçant au préalable dans un interphone, etc.).
- Système d'alarme opérationnel en dehors des heures de fonctionnement de l'étude

ii. Caméras

Préciser si une ou plusieurs caméra(s) ont été placées à l'entrée de l'organisme

- Une à l'extérieur
- Quatre à l'intérieur

7. Sécurité physique et environnementale

a. Mesures générales

Les mesures de sécurité nécessaires ont été mises en place afin de prévenir les dommages physiques pouvant compromettre l'information.

Une alarme incendie, des détecteurs de fumée et extincteurs sont placés dans l'organisme.

Préciser les mesures de sécurité générales adoptées pour protéger les documents papiers (pièces fermées à clé, non accessibles aux visiteurs, armoires sécurisées etc.).

b. Mesures particulières dans les salles des serveurs de l'organisme

La température est constante grâce à un système de climatisation. Un système de détection et de protection contre les incendies a été installé. Une alimentation alternative a été mise en place afin de garantir la continuité du service pendant une courte durée.

8. Sécurisation du réseau

L'organisme vérifie que le réseau, son contenu et son utilisation sont gérés et contrôlés de façon adéquate afin de le protéger contre les menaces et de garantir de façon efficace la protection des systèmes et des applications qui utilisent le réseau.

Un système de pare-feu a été installé et correctement configuré au niveau du périmètre extérieur du réseau. Seul les ports strictement nécessaire aux bonnes opérations de l'organisme sont ouverts vers le monde extérieur.

Un accès sécurisé au réseau est mis en place pour le personnel qui doit y accéder ; la connexion à distance au réseau (par exemple afin d'effectuer du télétravail ou pour permettre à un fournisseur d'effectuer une opération de maintenance) passe par une authentification à facteurs multiples.

La connexion à distance au réseau se fait uniquement à l'aide de systèmes dont la protection et les mesures de sécurité sont contrôlées par l'organisme et qui répondent au minimum aux exigences décrites dans cette politique.

9. Sécurisation des serveurs, postes de travail et systèmes

Une solution anti-malware a été installé sur chaque serveur et poste de travail. La base de données des définitions des malware de chaque solution anti-malware est régulièrement mise à jour.

Chaque système d'exploitation, logiciel et composant installé sur les systèmes d'information tels que les serveurs, les postes de travail, les pares-feux et autres systèmes font régulièrement l'objet de mises à jour de sécurité et sont encore supportés par le constructeur.

Les sessions des utilisateurs se verrouillent ou arrivent à péremption suite à un délai raisonnable.

10. Gestion des copies de sécurité (backups)

Un système de backups réguliers est mis en place et couvre toutes les données nécessaires au bon fonctionnement de l'organisme.

Les backups font l'objet des mesures suivantes :

- au moins un des backups est conservé sur un site distinct de la salle serveur ;
- les données faisant l'objet de backups sont chiffrées ;
- la clé de déchiffrement de backups est sécurisée, dans un système d'information distinct du lieu de stockage de backups ;
- les backups sont soit déconnectés de tout réseau, soit immutables (impossibilité de supprimer les backups depuis le réseau d'où les données de backups sont envoyées) ;
- les backups font l'objet de tests de restauration réguliers, à une fréquence de maximum 1x par an.

11. Destruction des données

Les documents papiers contenant de l'information confidentielle ou interne sont détruits de manière sécurisée. Plus particulièrement, les documents papiers contenant des données à caractère personnel sont détruits lorsque la période de rétention de ces données, telle que définie dans le « registre des traitements », est atteinte.

Mesures adoptées pour leur destruction : recours à un sous-traitant spécialisé.

Les données à caractère personnel sont effacées des systèmes d'information lorsque la période de rétention de celles-ci, telle que définie dans le « registre des traitements », est atteinte.

Lors du remplacement de matériel informatique, les données des supports contenant des informations confidentielles ou internes sont effacées de manière sécurisée (effacement par le fournisseur informatique qui remet une notification ou un certificat de destruction de données sécurisée) ou leur support est détruit de manière suffisante à rendre les données inexploitable (destruction de disques durs à l'aide d'un marteau ou d'une foreuse).

12. Sous-traitance

Tout sous-traitant de données s'est engagé contractuellement à respecter les mesures adéquates de sécurité et de protection des données.

13. Sécurisation logique des accès

Les accès de toute nature aux informations confidentielles ou internes se font par le biais d'un système d'identification, d'authentification et d'autorisation de l'utilisateur. Les autorisations sont configurées de telle sorte que chaque utilisateur n'a accès qu'aux informations confidentielles dont il a besoin dans le cadre de son travail, et a accès à l'ensemble des informations internes. Les accès en écriture aux informations publiques se font par le biais d'un système similaire.

Les données à caractère personnel des sources officielles ne sont récoltées que de manière sécurisée par le biais du portail dédié.

Les accès aux sources officielles et aux systèmes d'information sont adaptés suite aux mouvements de personnel de l'organisation (entrées, changements de rôles et responsabilités, départs).

Les systèmes d'information dont l'authentification nécessite l'utilisation d'un mot de passe sont configurés de manière centralisée afin d'imposer des mots de passe d'une longueur de minimum 10 caractères et dont le contenu inclut des caractères complexes (majuscules, minuscules, symboles et chiffres), ou d'une protection équivalente ou supérieure. Les tentatives infructueuse répétées et successives d'authentification à de tels systèmes entraînent le verrouillage de l'ouverture de sessions du compte utilisateur durant un brève période.

L'accès aux systèmes d'information pouvant être atteints depuis l'extérieur de l'organisme (VPN, email etc.) est protégé par une authentification à facteurs multiples, et s'effectue via des systèmes d'information implémentant les mesures de cette politique.

Chaque utilisateur dispose d'accès nominatifs ou identifiables (les comptes génériques ou partagés sont proscrits).

Une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel des sources officielles est établie. Cette liste est tenue à la disposition de l'Autorité de protection des données, sur demande.

14. Journalisation des accès

Les systèmes d'information de l'organisme ont été conçus de manière à permettre une journalisation, un traçage et une analyse des accès des personnes à l'information et aux systèmes d'information (accès directs sur les disques réseaux de l'organisme, accès via les logiciels des sous-traitants, accès au réseau par un sous-traitant dans le cadre de la maintenance etc.).

Le système d'information des sources officielles a été conçu de façon à permettre une journalisation, un traçage et une analyse des accès des personnes et organismes logiques aux sources officielles.

Les éléments suivants sont conservés :

- Les données d'identification de l'utilisateur concerné ;
- Les données d'identification de la personne sur qui une recherche a été effectuée ;
- Le moment de la recherche ;
- La finalité de la recherche (application informatique et/ou dossier concerné).

15. Surveillance, révision et maintenance

Un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles mises en place est prévu.

Les systèmes techniques font l'objet de tests et de maintenance. Ceux-ci sont contractuellement prévus si un sous-traitant est impliqué.

La présente politique et les autres documents auxquels il est fait référence, font l'objet de révision régulière.

L'organisme met en place les crédits nécessaires à la surveillance, à la révision et à la maintenance des mesures techniques et organisationnelles mises en place.

16. Gestion des incidents de sécurité

Lorsqu'un incident de sécurité impliquant un traitement de l'information survient, le délégué à la gestion journalière en est immédiatement averti. Ce dernier prend les mesures nécessaires et assigne les tâches aux personnes compétentes afin de remédier à l'incident. Ainsi, l'incident est facilement détecté, suivi et réparé.

Lorsque l'incident concerne une fuite de données à caractère personnel, le délégué à la protection des données en est informé. Lorsqu'un tel incident crée un risque pour les droits et libertés des personnes concernées, la procédure spécifique de notification des atteintes aux données à caractère personnel est suivie.

Signature du délégué à la gestion journalière :

Le notaire Olivier LEBRUN à Courcelles
Signé