Jean-Louis MERTENS et Charlotte DE VOS, notaires associés

Politique de sécurité de l'information

Table des matières

1. Préambule

a. Coordonnées de l'organisme

Préciser la dénomination sociale et l'adresse du siège social.

Jean-Louis MERTENS et Charlotte DE VOS, notaires associés

Rue de Tournai, 24

7900 Leuze-en-Hainaut

Préciser les coordonnées du data protection officer de l'Etude.

Privanot asbl

Aurélie Van Der Perre

Rue de la Montagne, 30

1000 Bruxelles

b. 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 accessibles par l'organisme auprès des sources officielles suivantes :

- le registre national ;
- la banque-Carrefour de la sécurité sociale ;
- le cadastre.

En outre, la présente politique garantit la protection des données accessibles par l'organisme auprès des sources officielles du notariat suivantes :

- Les registres centraux des testaments et des contrats de mariage ;
- Le registre central des contrats de mandat en vue d'organiser une protection extrajudiciaire ;
- Le registre central des déclarations relatives à la désignation d'un administrateur ou d'une personne de confiance ;

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 des données à caractère personnel

Données confidentielles

Les données à caractère personnel qui concernent les citoyens et les données salariales et d'évaluation des collaborateurs sont par nature confidentielles. Elles ne peuvent être traitées que par les personnes habilitées à gérer les dossiers des personnes concernées, nonobstant tout autre usage encadré légalement.

Données à usage interne

Les données à caractère personnel qui ne concerne pas les citoyens ou les données confidentielles des collaborateurs peuvent être utilisées en interne, nonobstant tout autre usage encadré légalement.

Données libres d'usage

Les données à caractère personnel traitées par l'organisme préalablement anonymisées perdent leur caractère confidentiel et sont libres d'usage.

4. Identification des supports

Les supports de données à caractère personnel 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 données à caractère personnel sont les suivants :

- Serveurs installés en l'étude ;
- Serveurs extérieures : Préciser le site extérieur sur lequel les données sont conservées.
- Préciser si des données sont conservées d'une autre manière, par exemple dans un Cloud.

Le principe est qu'aucune donnée n'est conservée en local 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. Les données sont détruites dès que leur utilisation n'est plus nécessaire à l'accomplissement de la mission poursuivie.

Le principe est qu'aucune donnée ne peut être enregistrée sur un support mobile (clé USB, PC 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. Les données sont détruites dès que leur utilisation n'est plus nécessaire à l'accomplissement de la mission poursuivie.

5. 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 données à caractère personnel traitées découlant aussi bien des différentes exigences légales que de la politique de sécurité.

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

Le code de conduite applicable au personnel interne et externe et/ou le règlement de travail précise(nt) les règles spécifiques à suivre pour la protection des données à caractère personnel 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.

6. La sécurisation physique des accès

Des mesures de sécurité adéquates ont été mises en place afin de prévenir les accès physiques inutiles ou non autorisés aux supports et systèmes d'informations impliquant les données à caractère personnel traitées.

a. Etude

i. Accès à l'étude

L'étude est ouverte du lundi ou vendredi, sauf les jours fériés :

- Ouverture des portes extérieures de 9h00 à 12h30 et 13h30 à 17h30 (porte non ouverte, le client doit sonner) ;
- Bureaux fermés : pas de travail à bureaux fermés.
- Préciser les règles d'accès pour les collaborateurs et pour les visiteurs (avec badge, avec clé, etc.)

  - les collaborateurs ont chacun leur clé

  - les visiteurs doivent sonner, on les voit à la caméra et on ouvre

- Préciser les règles d'accès pour les visiteurs (en sonnant, en s'annonçant au préalable dans un interphone, etc.).

  - cfr ci-dessus

- Alarme active : pas d'alarme

ii. Caméras

Pas de caméra

b. Site externe

Absence de site externe.

7. La 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 les données à caractère personnel traitées.

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

Les testaments sont au coffre à la banque.

Préciser les mesures de sécurité adoptées pour protéger les actes

Salle d'archive + armoire bureau collaboratrice pour les actes récents → aucun accès aux clients car un client ne sera jamais seul dans ces pièces.

Les dossiers en cours sont dans les bureaux des collaborateurs et les dossiers clôturés dans les salles d'archives. Pas de dossier visible dans les pièces accessibles aux clients.

b. Mesures particulières dans la salle des serveurs de l'Etude

La température est constante grâce au système de climatisation. Un système de détection et de protection contre les incendies a été installé.

c. Mesures particulières concernant la destruction des données

En ce qui concerne la destruction des données et des documents papiers :

- les dossiers ne sont plus conservés après 30 ans ;
- les données comptables sont détruites après 10 ans ;
- les actes sont transmis aux Archives du royaume après 75 ans ;

Les données et documents papiers sont détruits de manière sécurisées (déchiqueteuse).

d. Mesures particulières dans les salles des serveurs du site externe (le cas échéant)

Des mesures au moins identiques, ou supérieures, sont adoptées par le gestionnaire du site extérieur. Les règles prévues en matière de sécurité leur sont contractuellement imposées.

e. Mesures particulières du système de Cloud (le cas échéant)

Des mesures particulières de protection des données sont adoptées par le fournisseur du système de Cloud. Ces mesures lui ont été contractuellement imposées, soit directement par l'étude, soit par le fournisseur informatique de l'étude qui sous-traite le système de Cloud (le cas échéant).

En tout état de cause, tous les fournisseurs d'un système de Cloud sont clairement identifiés par l'étude.

8. La sécurisation des réseaux

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

Afin de prévenir et de découvrir les logiciels nuisibles, des systèmes de pare-feu et d'anti-virus ont été installés, les mises à jour de sécurité sont gérées et appliquées sur les postes, serveurs et équipements.

Un accès sécurisé au réseau est mis en place pour le personnel qui doit y accéder en dehors des deux sites précités (le cas échéant).

9. Sous-traitance

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

10.La liste des personnes habilitées

Une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel des sources officielles peut être établie sur demande.

Cette liste est tenue à la disposition de l'Autorité de protection des données, sur demande.

11.La sécurisation logique des accès

Les données à caractère personnel des sources officielles ne sont accessibles que par le biais du portail sécurisé de l'e-Notariat. Les accès aux données à caractère personnel se font par le biais d'une carte à puce permettant un système d'identification, d'authentification et d'autorisation de l'utilisateur.

Les règles d'utilisation de la carte à puce sont précisées dans les conditions d'utilisation du portail de l'e-Notariat.

L'organisme responsable des accès à l'e-Notariat — la Fédération Royale du Notariat belge – est immédiatement averti du départ d'un collaborateur de manière à ce que l'accès puisse être bloqué dans les plus brefs délais.

12.La journalisation des accès

Le système d'information a été conçu de façon à permettre une journalisation, un traçage et une analyse des accès des personnes et entités logiques aux sources officielles. Le système est mis en place et assuré par la Fédération Royale du Notariat belge.

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).

13.La surveillance, la révision et la 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.

14.La gestion d'urgence des incidents de sécurité

Lorsqu'un incident de sécurité impliquant les données à caractère personnel traitées survient, le notaire 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 constitue une atteinte grave aux données à caractère personnel, la procédure spécifique de notification des atteintes aux données à caractère personnel est suivie.

Un système de copies de sécurité (backups) est mis en place et est régulièrement contrôlé afin d'éviter la perte irréparable de données en cas de catastrophe totale ou partielle.

Une alimentation alternative a été mise en place afin de garantir la continuité du service pendant une courte durée (juste batterie sur le serveur, les PC des collaborateurs s'éteignent en cas de panne)

Signature du notaire :

Jean-Louis MERTENS	Charlotte DE VOS
8/06/2021	8/06/2021
Signature	Signature