POLITIQUE DE SÉCURITÉ DE L'INFORMATION

1) **Protocole entre la CNHB et le CPAS**

Un protocole est conclu entre la CNHB et le CPAS qui souhaite participer à ce projet. Le protocole régit la relation contractuelle (lignes directrices, droits et obligations des parties), entre la CNHB et le CPAS qui ont rejoint le projet.

La CNHB a développé la plateforme de communication et en propose maintenant l'usage aux CPAS, à ses membres et aux huissiers de justice. La CNHB a donc la qualité de responsable du traitement.

Les huissiers de justice qui souhaitent se connecter à la CPC le font via le CIA et doivent signer un accord d'adhésion avec la CNHB. Pour l'utilisation du FCA et d'autres bases de données (DIV, RN, BCSS, RCCI), les huissiers ont déjà eu l'occasion de conclure un protocole d'utilisation avec la CNHB, dans lequel leurs obligations sont très strictement réglementées, en toute conformité avec le RGPD. Le respect de ce protocole d'adhésion est surveillé de manière permanente par le DPO de la CNHB au moyen d'audits internes.

Un accord de traitement étendu (supplémentaire) entre la CNHB et chaque huissier de justice participant individuel est inutile dans ce contexte et n'apportera aucune valeur ajoutée en termes de respect du RGPD.

Un accord de traitement entre les huissiers de justice participants et les CPAS peut constituer une option, la question étant de savoir si cela apporte une réelle plus-value. En outre, dans le cadre de leurs activités professionnelles, les huissiers de justice ont la qualité de responsable du traitement des données et doivent travailler conformément au RGPD. Enfin, un code de conduite est en cours d'élaboration, permettant de définir de manière exhaustive le fonctionnement de la profession dans le respect du RGPD.

2) **DPIA**

La DPO du gestionnaire de la plateforme a examiné le flux d'informations transitant par la plateforme de communication établie par la CNHB et a effectué une analyse d'impact (DPIA – analyse des risques). Cette DPIA est faite à la demande et l'attention du gestionnaire/responsable du traitement, qui a pu prendre les mesures nécessaires pour limiter les risques.

3) **Mesures techniques et organisationnelles**

Les huissiers de justice, puisqu'ils ont accès à la CPC via le CIA, sont déjà soumis à la *politique de sécurité de l'information établie par la CNHB*, imposant des mesures Techniques & d'Organisationnelles très larges. La CNHB fait donc tout son possible pour faire respecter le RGPD par ses membres.

En outre, des mesures techniques et organisationnelles spécifiques ont été prises pour la CPC, afin de garantir un traitement sécurisé des données à caractère personnel. Un système de *droits et de rôles* adapté a été mis en place. Premièrement, seul le CPAS peut introduire un dossier sur la CPC. Deuxièmement, l'accès à la CPC n'est autorisé que si un engagement intervient et après enregistrement. Pour la personne concernée, cela se fait en s'inscrivant sur la plateforme et en donnant son consentement de manière explicite pour le traitement de ses données et pour une finalité très précise. Il peut retirer son consentement à tout moment, ses données à caractère personnel seront alors supprimées de la CPC. Troisièmement, un huissier de justice ne peut pas enregistrer une personne ou introduire un nouveau dossier sur la CPC. Il peut, après invitation du CPAS, uniquement manifester sa volonté d'intervenir dans un dossier précis et télécharger ensuite les demandes liées au dossier. L'huissier de justice enregistré peut uniquement consulter ses dossiers. Le CPAS est le seul à avoir une vue d'ensemble.

Tout accès à la CPC est protégé grâce à un accès autorisé uniquement après vérification de l'identité de la personne concernée via eID et le mot de passe associé. Cela permet de déterminer qui demande l'accès à la plateforme et si cette personne a les droits nécessaires. Il existe également un système d'enregistrement et de traçage permettant de vérifier qui a eu accès à la plateforme et à quel moment.

La CPC prévoit des délais de conservation appropriés afin que les données ne soient pas traitées plus longtemps que nécessaire. Lorsque le dossier est clôturé, les données restent consultables durant un an conformément aux droits et rôles qui ont été attribués. Ensuite, les données sont archivées et ne peuvent être consultées que par l'huissier de justice pouvant être tenu responsable dans le cadre de sa responsabilité professionnelle. Ce délai de conservation est fixé à 10 ans. Une fois cette période écoulée, les données archivées sont définitivement supprimées.

Les données figurant dans la CPC sont toujours cryptées. Cela signifie qu'elles peuvent être uniquement décryptées (donc lisibles) par les personnes ayant un droit d'accès à la plateforme. En outre, le cryptage garantit que les données seront illisibles en cas de vol du support sur lequel elles sont stockées.

Un stockage sécurisé est prévu pour stocker les données. Les données sont conservées sur deux serveurs back-up indépendants, de sorte qu'en cas de problème, il est possible de passer très rapidement au serveur de sauvegarde.

- Les serveurs Web sont situés dans la zone DMZ (zone démilitarisée) et n'ont donc aucune connexion directe avec le réseau interne ;
- Des pare-feu NETASQ capables de détecter et de signaler les intrusions, ainsi qu'un logiciel anti-virus mis à jour en permanence sont également mis en place ;
- Les postes de travail des utilisateurs finaux ne peuvent se connecter au serveur de la base de données que via des serveurs de transaction ;
- En ce qui concerne la sécurité physique, la plateforme est répartie sur deux datacenters. Les serveurs se trouvent dans un environnement hautement sécurisé qui répond à toutes les exigences techniques pour assurer la sécurité et la continuité des serveurs, telles qu'un système de détection d'incendie couplé à un système d'extinction automatique à base de gaz, un double circuit d'alimentation, un contrôle d'accès électronique, une surveillance 24h/24 par caméra, une salle climatisée, et une alimentation électrique de secours, une duplication complète de la connexion internet, etc.

Vis-à-vis de l'extérieur, la plateforme est protégée contre tout accès non autorisé : les serveurs web et FTP se trouvent en dehors des bureaux, dans une zone DMZ, l'accès aux serveurs

nécessite des certificats, la connexion n'est possible que par des identifiants et mots de passe personnalisés ou une eID.

En ce qui concerne la sauvegarde des données, nous utilisons les outils standards (VEAAM/Solarwinds) qui permettent une restauration complète des VM/File/Database. Ces outils sont intégrés aux services de copie Volume Shadow de Microsoft. Cela permet d'effectuer des sauvegardes cohérentes de l'environnement dans l'application. En outre, nous effectuons des sauvegardes quotidiennes sur un serveur de sauvegarde externe, localisé dans un centre de données distinct et où les bandes sont conservées dans un coffre-fort sécurisé.

Afin de garantir que les données transmises par une autre étude ne puissent être utilisées que pour la finalité pour laquelle elles ont été recueillies, un certain nombre de mesures ont été prises :

- ✓ Les données sont conservées sur un serveur indépendant, géré uniquement par la CNHB ;
- ✓ Des droits d'accès distincts sont accordés pour accéder à ce serveur, avec une surveillance distincte ;
- ✓ Il n'y pas de lien entre ce serveur et d'autres serveurs de la CNHB, de sorte que les données ne peuvent être mêlées à d'autres données ;
- ✓ Il y a un contrôle permanent effectué par le DPO de la CNHB, portant sur l'utilisation correcte de ces données ;
- ✓ Toute activité sur le serveur fait l'objet d'un *log* et d'un *tracing*, de sorte qu'une utilisation abusive est détectable et peut être sanctionnée (faute déontologique et exclusion temporaire ou permanente de la plateforme) ;
- ✓ Le droit de consultation est limité à un an pour chaque étude, après quoi les données sont archivées et seront rendues accessibles uniquement si la responsabilité professionnelle d'un huissier de justice est mise en cause.

4) **DPO**

La CNHB dispose de son propre délégué à la protection des données (DPO) dont la tâche consiste à détecter les problèmes potentiels en matière de protection de la vie privée, en collaboration avec le service IT, en vue d'y remédier. En outre, le DPO a pour mission de

contrôler l'utilisation correcte de la plateforme et le respect du RGPD par les utilisateurs. Le cas échéant, le DPO proposera des mesures pour réduire ou remédier aux risques potentiels détectés. Par conséquent, il y a une évaluation permanente de l'application correcte du RGPD sur la plateforme et par les utilisateurs.

Pour plus d'informations sur la politique de sécurité de l'information ou pour déposer une plainte concernant le traitement de vos données à caractère personnel, vous pouvez contacter le Data Protection Officier via info-dpo@nkgb-cnhb.be.

5) Autorité de surveillance

L'autorité de surveillance est l'Autorité de protection des données (APD). Pour des informations supplémentaires, vous pouvez consulter le site internet de cette autorité : https://www.autoriteprotectiondonnees.be/citoyen. Vous pouvez également contacter l'APD via les coordonnées suivantes :

Autorité de Protection des données
Rue de la Presse 35, 1000 Bruxelles
Téléphone : +32 (0)2 274 48 00
Fax : +32 (0)2 274 48 35
Mail : contact@apd-gba.be

Si vous souhaitez introduire une plainte concernant la protection des données à caractère personnel, vous pouvez remplir le formulaire de plainte standard disponible ici : Introduire une plainte | Autorité de protection des données (autoriteprotectiondonnees.be)

6) L'information sur la dette ne se limite pas à une information financière

Outre les données financières, il est possible que des données concernant la santé d'une personne concernée (dettes hospitalières, frais médicaux, etc.) ou concernant des infractions pénales (adresse d'incarcération, etc.) soient reprises dans le dossier. Afin de garantir le respect du RGPD, la CNHB et ses membres accorderont toute l'attention nécessaire à la proportionnalité et à la limitation de la finalité du traitement lors du téléchargement de ces

données personnelles particulières, pour lesquelles le consentement particulier et explicite de la personne concernée est toujours requis.