PRIVACYBELEID COMMUNICATIEPLATFORM

1) Protocol tussen de NKGB en het OCMW

Het protocol wordt afgesloten tussen de NKGB en het OCMW dat wenst deel te nemen aan dit project. Het protocol regelt de contractuele verhouding (de krachtlijnen en de rechten en plichten van de samenwerking) tussen de NKGB en het OCMW dat zich aansluit.

De NKGB, die het communicatieplatform heeft ontwikkeld en aanbiedt aan het OCMW en zijn leden, alsook aan de gerechtsdeurwaarders, is bijgevolg de verwerkingsverantwoordelijke.

De gerechtsdeurwaarders die wensen aan te sluiten bij het CPC doen dat via de gekende CIA en ondertekenen een toetredingsovereenkomst met de NKGB. Voor de consultaties van het CBB en andere databanken (DIV, RR, KSZ, CROS) gebruiken zij nu ook al de CIA en in dat kader hebben zij een gebruikersprotocol met de NKGB afgesloten waarin hun verplichtingen zeer streng zijn geregeld, waardoor zij GDPR-conform zijn. Het respecteren van dat gebruikersprotocol wordt ook door de DPO van de NKGB permanent gemonitord door *internal audits*.

Een uitgebreide (bijkomende) verwerkersovereenkomst tussen de NKGB en de individuele deelnemende gerechtsdeurwaarders is onnodig in deze context en zal geen meerwaarde bieden op vlak van GDPR-compliancy.

Een verwerkersovereenkomst tussen de deelnemende gerechtsdeurwaarders en de OCMW's kan een optie zijn, maar de vraag is of dit een echte meerwaarde gaat bieden. Daarenboven zijn gerechtsdeurwaarders in hun beroepsactiviteiten sowieso al verwerkingsverantwoordelijken en dienen zij GDPR-compliant te werken. Bovendien is er een Gedragscode voor gerechtsdeurwaarders (Code of Conduct - in de maak) die de GDPR-compliante werking van het beroep uitgebreid gaat vastleggen.

2) DPIA

De DPO van de beheerder van het platform heeft de informatiestroom via het communicatieplatform van de NKGB nagekeken en heeft een DPIA opgesteld (risicodetectie), op vraag en voor de beheerder/verwerkinsgverantwoordelijke, waardoor deze de nodige maatregelen kon nemen om de risico's in te perken.

3) Technische en organisatorische maatregelen

Gerechtsdeurwaarders zijn, aangezien zij toegang hebben tot het CPC via de gekende CIA, reeds onderworpen aan het *Informatieveiligheidsbeleid van de NKGB* dat zeer uitgebreide Technische & Organisatorische maatregelen oplegt. De NKGB gaat hierin dan ook zeer ver om GDPRcompliancy van haar beroepsleden af te dwingen.

Daarnaast heeft het CPC ook verscheidene technische en organisatorische maatregelen genomen om tot een veilige verwerking van persoonsgegevens te komen. Een systeem van *passende rechten en rollen* wordt toegepast. In de eerste plaats kan enkel het OCMW een dossier aanmaken op het CPC. Ten tweede kan enkel toegang tot het CPC worden verkregen wanneer er een akkoord werd gesloten en na registratie. Voor de betrokkene gebeurt dit door zich te laten registreren op het platform en aldus uitdrukkelijke toestemming te geven voor het verwerken van zijn persoonsgegevens voor een bepaald doel. Hij/zij kan deze toestemming op elk moment intrekken, waarna zijn/haar gegevens worden gewist op het CPC. Ten derde kan een gerechtsdeurwaarder geen personen registreren of een dossier aanmaken op het CPC. Hij kan, na door het OCMW uitgenodigd te zijn, enkel aangeven dat hij voor het betrokken dossier wenst mee te werken en vervolgens kan hij zijn vorderingen opladen. De geregistreerde gerechtsdeurwaarder kan enkel zijn eigen dossiers raadplegen. Het OCMW heeft als enige een overzicht van alle dossiers van de betrokkene.

Iedere toegang tot het CPC is beschermd: de toegang wordt pas verleend nadat de identiteit van de betrokkene werd vastgesteld door gebruik te maken van diens e-ID met het bijhorende wachtwoord. Aldus kan worden vastgesteld wie toegang tot het CPC vraagt en of deze persoon over de nodige rechten beschikt. Er wordt ook een systeem van logging en tracing gehanteerd

waardoor steeds kan worden gecontroleerd wie wanneer toegang heeft gekregen tot de databank.

Het CPC voorziet in passende bewaartermijnen zodat persoonsgegevens niet langer dan noodzakelijk worden verwerkt. Wanneer een dossier wordt afgesloten, blijven de gegevens nog gedurende één jaar raadpleegbaar volgens de rechten en rollen die werden toegekend. Daarna gaan deze gegevens in rust en kunnen zij enkel nog geraadpleegd worden door de gerechtsdeurwaarder die in het kader van zijn beroepsaansprakelijkheid wordt aangesproken. Deze termijn bedraagt 10 jaar. Nadat deze termijn is verstreken worden de gegevens in rust definitief verwijderd.

De gegevens die zich in het CPC bevinden zijn allemaal geëncrypteerd. Dit betekent dat ze slechts gedecrypteerd kunnen worden door en dus leesbaar worden voor personen die toegangsrechten hebben tot het CPC. Bovendien zorgt de encryptie ervoor dat ze bij een eventuele diefstal van de gegevens of de harde schijf, dan wel server waarop ze werden opgeslagen, onleesbaar zijn.

Er is voor wat betreft de opgeslagen gegevens een beveiligde dataopslag. De gegevens worden op twee onafhankelijke back-upservers opgeslagen zodat bij eventuele onregelmatigheden zeer snel overgeschakeld kan worden naar de back-upomgeving.

- De Webservers zijn ondergebracht in de DMZ (Demilitarized zone) en hebben bijgevolg geen rechtstreekse verbinding met het interne netwerk.
- Er is bovendien voorzien in NETASQ firewalls die intrusie kunnen detecteren en rapporteren en een permanent geüpdatete antivirussoftware.
- De werkstations van de eindgebruikers kunnen zich enkel via de transactieservers in verbinding stellen met de databaseserver.
- Voor de fysieke beveiliging heeft het platform een redundante opstelling over twee datacenters. De servers staan in een sterk beveiligde omgeving die voldoet aan alle technische specificaties die noodzakelijk zijn om de beveiliging en de continuïteit van de servers te kunnen verzekeren, zoals: een branddetectiesysteem en automatisch brandblussysteem op basis van gas, dubbel stroomcircuit, elektronische toegangscontrole, 24 uur per dag camerabewaking, klimaatgeregelde ruimte, noodstroomvoeding (UPS) en back-up power supply, volledige ontdubbeling van de internetverbinding, ...

Het platform wordt extern beveiligd tegen ongeoorloofde toegang : de web- en ftp-server bevinden zich buiten het netwerk van de kantoren in een DMZ-zone, voor de toegang tot de servers zijn certificaten vereist, aanmelden kan enkel door gepersonaliseerde logins en wachtwoorden of door een eID.

Voor de back-up van gegevens maken we gebruik van industriestandaardtools (VEAAM/Solarwinds) die toelaten om full VM/File/Database restores uit te voeren. Deze tools zijn geïntegreerd met de door Microsoft voorziene Volume Shadow copy services. Dit laat toe om in de applicatie consistente back-ups te voorzien van de omgeving. Daarnaast maken we dagelijks een back-up op een externe back-upserver die zich in een afzonderlijk datacenter bevindt en waar de tapes in een beveiligde kluis worden bewaard.

Om ervoor te zorgen dat de gegevens die van een ander gerechtsdeurwaarderskantoor worden ontvangen uitsluitend kunnen worden gebruikt voor hetzelfde doel waarvoor deze gegevens werden verstrekt, werden een aantal maatregelen genomen:

- ✓ De gegevens worden op een aparte server bewaard die enkel de NKGB beheert;
- ✓ Er zijn aparte toegangsrechten toegekend tot deze server, die worden gecontroleerd;
- ✓ Er is geen verbinding tussen deze server en andere servers van de NKGB waardoor de data niet vermengd kan geraken met andere data;
- ✓ Er is een permanente controle door de DPO van NKGB op het juiste gebruik van deze gegevens;
- ✓ Er is permanente *logging* en *tracing* van alle activiteit op de server waardoor oneigenlijk gebruik opspoorbaar is en kan worden gesanctioneerd (deontologische fout en de tijdelijke of permanente uitsluiting van toegang tot het platform);
- ✓ Het consultatierecht is voor ieder gerechtsdeurwaarderskantoor beperkt tot één jaar, waarna de gegevens in rust worden geplaatst en pas toegankelijk zijn indien er een concrete beoordeling van beroepsaansprakelijkheid dient te gebeuren.

4) DPO

De NKGB beschikt over een eigen Data Protection Officer (DPO) die als taak heeft om in samenwerking met de IT-dienst potentiële problemen te detecteren en te laten verhelpen. Verder heeft de DPO de opdracht om controle te laten uitvoeren op het correcte gebruik van

het platform en de correcte toepassing van de GDPR door de gebruikers. In voorkomend geval zal de DPO maatregelen voorstellen om gedetecteerde potentiële risico's te verminderen of te verhelpen. Er is bijgevolg een permanente evaluatie op de juiste toepassing van de GDPR door het platform en zijn gebruikers.

Voor meer informatie over dit privacybeleid of voor klachten in verband met de verwerking van uw persoonsgegevens, kan u contact opnemen met de Data Protection Officer via info-dpo@nkgb-cnhb.be.

5) Toezichthoudende autoriteit

De toezichthoudende autoriteit is de gegevensbeschermingsautoriteit (GBA). Voor bijkomende informatie kan u terecht op de website www.gegevensbeschermingsautoriteit.be. U kan de gegevensbeschermingsautoriteit bereiken via volgende contactgegevens:

Gegevensbeschermingsautoriteit
Drukpersstraat 35, 1000 Brussel
Telefoon: +32 (0)2 274 48 00
Fax: +32 (0)2 274 48 35
Mail: contact@apd-gba.be

Indien u een klacht wenst neer te leggen die betrekking heeft op de bescherming van persoonsgegevens kan u een standaard klachtenformulier verkrijgen via www.gegevensbeschermingsautoriteit.be/verzoek-klacht-indienen.

6) Schuldinfo is méér dan louter financiële info

Naast financiële gegevens zijn er natuurlijk ook gegevens die een indicatie kunnen geven over de gezondheidstoestand van een betrokkene (ziekenhuisschulden, medische kosten, …) of over strafrechtelijke feiten (domicilieadres in gevangenis, …). Vanuit GDPR compliancy zullen de NKGB en haar leden de nodige aandacht besteden aan de proportionaliteit en de

doelbinding bij het opladen van dergelijke bijzondere persoonsgegevens, waarvoor steeds de uitdrukkelijke toestemming van de betrokkene vereist is.