OFP Prolocus

Maturiteitsanalyse gegevensbescherming

1. OVERZICHT

Doel van dit document

1. *In het* ***tabblad 'maturiteitsanalyse'*** *wordt nagegaan in welke mate de organistie een beleid en de nodige operationele instrumenten heeft om verschillende bepalingen in de AVG te waarborgen.*

Daarbij wordt telkens een indicatieve ' ***maturiteitsscore*** *' aangegeven, alsook een* ***reeks aanbevelingen*** *om deze maturiteitsscore te verhogen.*

2. *In het* ***tabblad 'Actieplan'*** *worden verschillende* ***voorgestelde maatregelen*** *uiteengezet, samen met een* ***prioritisering*** *en een* ***voorstel tot planning*** *om deze te implementeren.*

Informatie

Entiteit:	
Geraadpleegde bronnen :	Deze maturiteitsscan werd **uitvoerd op basis van onmiddelijk beschikbare interne alsook publiek beschikbare bronnen.** Er werden **in het kader van deze beperkte scan** (of pré-audit) **géén interviews afgenomen van stakeholders** (ICT-medewerkers, product owners, dossierbehandelaars, etc), **noch test of grondige analyses doorgevoerd** van bedrijfsprocessen, databanken, etc.
Uitgevoerd door:	Koen Hostyn, DPO OFP Prolocus (Cranium)
Uitgevoerd op:	17/10/2024 - versie 0.2
Gevalideerd door:	
Gevalideerd op:	
Vastgesteld door:	
Vastgesteld op:	

Dit is een document voor intern gebruik 

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Hoofdstuk I: Algemene Bepalingen			
Art. 5, 1, a) Rechtmatigheid, behoorlijkheid en transparantie	Persoonsgegevens worden verwerkt op een wijze die ten opzichte van de betrokkene rechtmatig, behoorlijk en transparant is. Zie hoofdstuk II: Rechtmatigheid.	2	Zie hoofdstuk II: Rechtmatigheid
Art. 5, 1, b) Doelbinding	Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. De doeleinden van de verwerking worden uiteengezet in het Privacybeleid.	3	Periodieke audits van de informatiesystemen van Prolocus uitvoeren om te controleren of de principes van 'minimale gegevensbescherming', 'opslagbeperking' en 'doelbinding' worden gewaarborgd.
Art. 5, 1, c) Minimale gegevensverwerking	Persoonsgegevens moeten toereikend, ter zake dienen en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt. In de Beleidsnota Gegevensverwerking en -Bescherming staat onder de beginselen van verwerking (hoofdstuk 4) vermeld dat Prolocus de Verwerking van Persoonsgegevens beperkt tot hetgeen noodzakelijk is in het kader van de administratie en uitvoering van de Pensioenregelingen. Er is ook een beleid voor gegevensclassificatie, dat de classificatie van persoonsgegevens en beveiligingsvereisten per classificatieniveau omvat.	3	Periodieke audits uitvoeren van de informatiesystemen van Prolocus' om te controleren of de principes van 'minimale gegevensbescherming', 'opslagbeperking' en 'doelbeperking' worden gewaarborgd.
Art. 5, 1, d) Juistheid	In de Beleidsnota Gegevensverwerking en -Bescherming wordt ook vermeld dat Prolocus alle redelijke maatregelen zal nemen om ervoor te zorgen dat Persoonsgegevens correct zijn en dat deze onverwijld worden gecorrigeerd en/of verwijderd als blijkt dat ze niet langer correct zijn.	3	Neem redelijke maatregelen om onjuistheden te voorkomen tijdens het gegevensverzamelingsproces en tijdens de lopende gegevensverwerking. Het wordt ook aanbevolen om periodieke evaluaties uit te voeren met betrekking tot de nauwkeurigheid van de verzamelde en opgeslagen persoonsgegevens en alle redelijke maatregelen te nemen om ervoor te zorgen dat persoonsgegevens die onjuist zijn, gelet op de doeleinden waarvoor Prolocus ze verwerkt, onverwijld worden gewist of gecorrigeerd.
Art. 5, 1, e) Opslagbeperking	Persoonsgegevens moeten worden bewaard in een vorm die het niet mogelijk maakt de betrokkenen langer te identificeren dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens worden verwerkt. In de Beleidsnota Gegevensverwerking en -Bescherming staat vermeld dat Prolocus persoonsgegevens niet langer zal verwerken en bewaren dan dan noodzakelijk is voor de in het betreffende document genoemde doeleinden. Verder geven zij in de Privacybeleid de exacte bewaartermijn in sommige gevallen van verwerking.	3	Een jaarlijkse 'data opruimdag' organiseren. Periodieke audits van de informatiesystemen van Prolocus uitvoeren om te controleren of de principes van 'minimale gegevensbescherming', 'opslagbeperking' en 'doelbinding' worden gewaarborgd. Ervoor zorgen dat er dataretentieperiodes worden bepaald voor elk van de verwerkingsactiviteiten en de doeleinden ervan. Er wordt een procedure voor het vaststellen en handhaven van passende bewaarperioden opgesteld en geïmplementeerd.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 5, 1, f) Integriteit en vertrouwelijkheid	Persoonsgegevens moeten worden verwerkt door passende technische of organisatorische maatregelen te nemen om een passende beveiliging ervan te waarborgen, met inbegrip van bescherming tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Prolocus vermeldt in de Beleidsnota gegevensverwerking en -bescherming dat dergelijke maatregelen worden genomen, maar ook dat ze regelmatig zullen worden geëvalueerd en indien nodig bijgewerkt. Bovendien zal Prolocus in het geval van een inbreuk ook passende maatregelen nemen om de omvang en de gevolgen ervan vast te stellen, deze zo snel mogelijk ongedaan te maken en indien nodig de gevolgen ervan voor de betrokken aangeslotenen en/of begunstigden te beperken.	3	Zie hoofdstuk IV, afdeling 2: Persoonsgegevensbeveiliging
Hoofdstuk II. Rechtmatigheid			
Art. 6, 1, a) Toestemming Art. 9, 2, a) Specifieke toestemming	Wanneer de verwerking is gebaseerd op toestemming, moet de verantwoordelijke hiervoor kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn of haar persoonsgegevens. In het cookiebeleid van Prolocus wordt vermeld dat er geen analytische cookies worden gebruikt, maar alleen strikt noodzakelijke en functionele cookies. Wat het verzamelen van gevoelige persoonsgegevens betreft, wordt in de Beleidsnota Gegevensverwerking en -bescherming vermeld dat Prolocus, indien nodig, in het kader van het beheer en de uitvoering van de pensioenplannen dergelijke gegevens kan verwerken. Prolocus maakt echter niet duidelijk of die verwerking plaatsvindt op basis van uitdrukkelijke toestemming. Prolocus baseert zich ook op toestemming als rechtsgrondslag voor PR-doeleinden (aanspreekpunt voor vragen).	1	Ervoor zorgen dat geldige toestemming kan worden aangetoond wanneer nieuwe gegevens worden verwerkt (bijv. voor direct marketing). Ervoor zorgen dat wanneer analytische/tracking cookies worden geïmplementeerd, de toestemming van de gebruiker op de juiste manier wordt verkregen. Privacybeleid bijwerken waarin wordt uitgelegd of toestemming vereist is/wordt verkregen voor de verwerking van gevoelige gegevens.
Art. 6, 1, b) Uitvoering van een overeenkomst	Prolocus gebruikt de rechtsgrondslag van noodzaak voor de uitvoering van een overeenkomst (dienstverband) als een van de rechtsgronden voor rechtmatige verwerking. Op basis daarvan verwerkt Prolocus volgens de privacyverklaring persoonsgegevens ten behoeve van de uitvoering van de arbeidsovereenkomst. Daarnaast verwerkt Prolocus ook persoonsgegevens voor de volgende doeleinden; Administratie van personeel en tussenpersonen; Leveranciersbeheer; Registratie en administratie van aandeelhouders of partners; en PR	2	Gegevens verifiëren die worden verwerkt in het kader van de uitvoering van een contract is noodzakelijk in verband met de doeleinden waarvoor ze worden verwerkt.
Art. 6, 1, c) Wettelijke verplichting	Prolocus verwerkt persoonsgegevens voor de registratie en administratie van aandeelhouders of vennoten in het kader van het Corporate Governance Charter. Prolocus verwerkt ook persoonsgegevens voor fraudebestrijding en inbreuken op de cliëntenwetgeving. De FSMA oefent haar toezicht uit op basis van wettelijke bepalingen, die worden opgesomd in de Privacyverklaring.	3	Het wordt aanbevolen om de wettelijke verplichtingen waaraan de verwerkingsverantwoordelijke is onderworpen, zorgvuldig te documenteren.
Art. 6, 1, e) Taken van algemeen belang	Prolocus verwerkt geen persoonsgegevens op grond van de rechtsgrondslag van algemeen belang.	nvt	

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 6, 1, f) Gerechtvaardigde belangen van de verwerkingsverantwoordelijke	Prolocus verwerkt geen persoonsgegevens op grond van de rechtsgrondslag van gerechtvaardigd belang.	nvt	
Hoofdstuk III. Rechten van de betrokkene			
Art. 13 Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	Al de vereiste gegevens zijngedefinieerd en beschikbaar gemaakt voor de betrokkene in de Privacyverklaring en daarmee voldoet Prolocus aan artikel 13 van de AVG. De privacyverklaring is echter niet vlot toegankelijk vanop de homepagina. Prolocus heeft de 'Richtlijnen Verzoeken Betrokkenen' en de 'VERZOEKEN RECHTEN BETROKKENEN - Algemene antwoorden' gedocumenteerd.	2	Publicatie privacyverklaring op homepagine. Privacyverklaring moet regelmatig worden herzien en bijgewerkt.
Art. 14 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen	Aangezien Prolocus als verantwoordelijke voor de verwerking persoonsgegevens verwerkt die rechtstreeks van de betrokkenen zijn verzameld, wordt Prolocus geacht te voldoen aan artikel 14 van de AVG.	3	/
Art. 15 Recht van inzake van de betrokkene	Betrokkenen hebben het recht om van Prolocus een bevestiging te krijgen of hun persoonsgegevens al dan niet worden verwerkt en, als dat het geval is, om toegang te krijgen tot die persoonsgegevens en aanvullende informatie over de verwerking van de persoonsgegevens. Prolocus verstrekt de betrokkene in dat geval een kopie van zijn persoonsgegevens. Als de betrokkene zijn recht op toegang wil uitoefenen, raadt Prolocus hem aan het webformulier te bezoeken voor informatie over de procedure en de voorwaarden. Dergelijke informatie lijkt echter niet (gemakkelijk) toegankelijk op de website. Er worden geen kosten in rekening gebracht voor het invullen van het verzoek. Als aan de voorwaarden is voldaan, zal het OFP PROLOCUS het verzoek van de betrokkene inwilligen en hem zo snel mogelijk op de hoogte brengen. Prolocus kan eerst om aanvullende informatie vragen om de identiteit van de betrokkene te bevestigen. Er zijn ook sjablonen en procedures voor verzoeken beschikbaar.	3	Zorg ervoor dat we een volledig overzicht hebben van de verwerkte gegevens, zodat we op een dergelijk verzoek kunnen reageren. Zet een register om alle verzoeken van betrokkenen bij te houden.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 16 Recht op rectificatie	De betrokkene heeft het recht op rectificatie van onnauwkeurige of onvolledige persoonsgegevens. Indien mogelijk kan de betrokkene aanvullende persoonsgegevens verstrekken om de verzameling van persoonsgegevens te vervolledigen. Als de betrokkene zijn recht op rectificatie wil uitoefenen, raadt Prolocus hem aan het webformulier te bezoeken voor informatie over de procedure en de voorwaarden. Deze informatie lijkt echter niet (gemakkelijk) toegankelijk op de website. Er worden geen kosten in rekening gebracht voor het invullen van de aanvraag. Als aan de voorwaarden is voldaan, zal Prolocus het verzoek van de betrokkene inwilligen en zo spoedig mogelijk in kennis stellen. Prolocus kan eerst aanvullende informatie vragen om de identiteit van de betrokkene te bevestigen.	3	Zet een register op om alle verzoeken van betrokkenen bij te houden. Zorg ervoor dat het webformulier voor het uitoefenen van de rechten van de betrokkene gemakkelijk toegankelijk is.
Art. 17 Recht op gegevenswissing ("recht op vergetelheid")	Onder bepaalde omstandigheden hebben betrokkenen het recht om een verzoek in te dienen om hun persoonsgegevens te verwijderen. Prolocus zal de persoonsgegevens van de betrokkene verwijderen, bijvoorbeeld als de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld, als de betrokkene de toestemming waarop de verwerking is gebaseerd intrekt en er geen andere rechtsgrondslag is voor de verwerking, als de betrokkene bezwaar maakt tegen de verwerking en zijn belangen zwaarder wegen, of als Prolocus wettelijk verplicht is de persoonsgegevens van de betrokkene te verwijderen. Als de betrokkene zijn recht op gegevenswissing wil uitoefenen, raadt Prolocus de betrokkene aan het webformulier te bezoeken voor informatie over de procedure en de voorwaarden. Er worden geen kosten in rekening gebracht voor het invullen van het verzoek. Als aan de voorwaarden wordt voldaan, zal Prolocus het verzoek van de betrokkene inwilligen en hem zo snel mogelijk op de hoogte stellen. Prolocus kan eerst om aanvullende informatie vragen om de identiteit van de betrokkene te bevestigen. Prolocus heeft echter het recht om gegevens van de betrokkene te bewaren wanneer dat nodig is voor onder andere: - het voldoen aan een wettelijke verplichting; - het instellen, uitoefenen of onderbouwen van een rechtsvordering.	3	Zet een register op om alle verzoeken van betrokkenen bij te houden.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 18 Recht op beperking van de verwerking	In sommige gevallen heeft de betrokkene het recht om de verwerking van zijn persoonsgegevens te beperken. Dit betekent dat Prolocus de verwerking van de persoonsgegevens van de betrokkene tijdelijk onderbreekt, bijvoorbeeld als de betrokkene de juistheid van zijn persoonsgegevens heeft betwist of bezwaar heeft gemaakt tegen de verwerking van zijn persoonsgegevens. Als het verzoek wordt ingewilligd, zal Prolocus de persoonsgegevens in kwestie niet verder verwerken voor de duur van de beperking, tenzij dit is toegestaan onder de AVG. Als de betrokkene zijn recht op beperking van de verwerking wil uitoefenen, raadt Prolocus de betrokkenen aan om het webformulier te bezoeken voor informatie over de procedure en de voorwaarden. Er worden geen kosten in rekening gebracht voor het invullen van het verzoek. Prolocus kan eerst om aanvullende informatie vragen om de identiteit van de betrokkene te bevestigen.	3	Zet een register op om alle verzoeken van betrokkenen bij te houden.
Art. 20 Recht op overdraagbaarheid van gegevens	In bepaalde gevallen kunnen betrokkenen het recht hebben om de persoonsgegevens die zij hebben verstrekt aan hen te laten overdragen of rechtstreeks door Prolocus te laten overdragen aan een andere verwerkingsverantwoordelijke, op voorwaarde dat dit technisch haalbaar is. Er worden geen kosten in rekening gebracht voor de uitvoering van dit verzoek.	3	Zet een register op om alle verzoeken van betrokkenen bij te houden.
Art. 21 Recht van bezwaar	Wanneer de verwerking door Prolocus is gebaseerd op toestemming, kunnen betrokkenen de toestemming die ze hebben gegeven op elk moment intrekken. Ze kunnen zich bijvoorbeeld op elk moment uitschrijven voor de nieuwsbrieven.	3	Zet een register op om alle verzoeken van betrokkenen bij te houden.
Art. 22 Geautomatiseerde individuele besluitvorming, waaronder profilering	Het beleid van Prolocus is om ervoor te zorgen dat betrokkenen niet worden onderworpen aan besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking, waaronder profilering, die rechtsgevolgen voor hen kunnen hebben of die voor hen wezenlijk vergelijkbare gevolgen kunnen hebben.	4	
Hoofdstuk IV: Verwerkingsverantwoordelijke en verwerker			
Art. 26 Gezamelijke verwerkingsverantwoordelijken	Prolocus treedt op als enige verantwoordelijke voor het bepalen van doeleinden en middelen voor interne verwerkingsactiviteiten van persoonsgegevens. Echter, aangezien het kantoor van Prolocus deel uitmaakt van het gebouw van de Provincie Antwerpen, is het noodzakelijk een overeenkomst van Gezamelijke verwerkingsverantwoordelijken te ondertekenen.	1	Zorg ervoor dat de overeenkomst van Gezamelijke verwerkingsverantwoordelijken met de provincie Antwerpen wordt ondertekend

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 28, 3 Verwerkersovereenkomst	Onder het overzicht van verwerkingsactiviteiten staan de verwerkers van Prolocus als volgt vermeld; -Nexyan voor verschillende doeleinden, zoals het beheer van zetelmunten en de registratie en administratie van bestuursleden en (vertegenwoordigers van) leden van de algemene vergadering; -Nexyan en Pensioenarchitect voor de uitbetaling van pensioenen aan het personeel en het intermediair; -VGD voor het financieel beheer; -FSMA (Autoriteit voor Financiële Markten en Diensten) voor de bestrijding van fraude en overtredingen van (potentiële) bestuursleden; -Lydian voor de uitvoering van de klokkenluidersregeling.	2	In het Register van verwerkingsactiviteitene blijkt dat sommige verwerkersovereenkomsten nog niet zijn ondertekend (het FSMA-vak is leeg, terwijl er voor Lydian een nieuwe overeenkomst in onderhandeling is). Zorg ervoor dat alle gegevensverwerkingsovereenkomsten (DPA's) worden ondertekend en werk het register dienovereenkomstig bij.
Art. 30 Register van de verwerkingsactiviteiten	Prolocus houdt een intern register bij van alle verwerkingsactiviteiten. De records bestaan uit de volgende informatie: - titel van de verwerkingsactiviteit - doeleinden/categorieën van verwerkingsactiviteiten - contactpersoon van de verwerking - verwerker - rechtsgrondslag van de verwerkingsactiviteit - categorieën van persoonsgegevens - categorie van betrokken personen - ontvangers van de persoonsgegevens - bewaartermijn - ICT-toepassingen - indien verwerkersovereenkomsten van toepassing zijn - toegangsbeheer - gebruikersrollen - auditlogboek	3	Register van verwerkingsactiviteiten moet regelmatig worden herzien na een bepaalde periode en/of na het implementeren van nieuwe verwerkingsactiviteiten. In het register blijkt dat sommige verwerkersovereenkomsten nog niet ondertekend zijn (FSMA-vakje is leeg, terwijl er voor Lydian een nieuw contract in onderhandeling is). Zorg ervoor dat beide worden ondertekend, terwijl het register wordt bijgewerkt. Het is aan te raden om het register, audits en taken te integreren met behulp van een compliance management platform.
Afdeling 2 - Persoonsgegevensbeveiliging			
Art. 25, 1 Gegevensbescherming door ontwerp	Prolocus beschrijft in haar Privacyverklaring: 'Prolocus verbindt zich ertoe passende technische en organisatorische maatregelen te nemen, rekening houdend met de risico's die gepaard gaan met gegevensverwerking, om persoonsgegevens te beschermen tegen ongeoorloofde toegang, onrechtmatige verwerking, onopzettelijk verlies of aantasting en ongeoorloofde vernietiging ervan. In geval van uitbesteding aan externe verwerkers zal zij ervoor zorgen dat deze dienstverleners passende technische en organisatorische maatregelen nemen om de Persoonsgegevens te beschermen tegen bovengenoemde incidenten. Prolocus heeft een procedure voor informatieaanvragen en een procedure voor inbreuken geïmplementeerd. Prolocus is ook bezig met het opstellen van een Software Beveiliging Checklist.	2	Stel interne procedures op voor de toepassing van de principes voor gegevensbescherming. Voltooi de checklist voor softwarebeveiliging. Wanneer er nieuwe functies worden ontwikkeld, wordt aanbevolen om een 'privacy by design'-beoordeling uit te voeren en advies te vragen aan de functionaris voor gegevensbescherming. Overweeg certificeringsmechanisme om aan te tonen dat verwerkingsactiviteiten voldoen aan de AVG conform artikel 42.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 25, 2 Gegevensbescherming door standaardinstellingen	Prolocus geeft per specifiek doel aan welke persoonsgegevens worden gebruikt en wat de juridische grondslag is om die persoonsgegevens te mogen verwerken. Prolocus beperkt zich bij de verwerking van persoonsgegevens van aangeslotenen en uitkeringsgerechtigden tot de specifieke gegevens die noodzakelijk zijn voor de administratie en uitvoering van de betreffende pensioenregeling. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de in de beleidsnota van Prolocus genoemde doeleinden, dat wil zeggen zolang zij een wettelijke verantwoordelijkheid of aansprakelijkheid kan hebben in het kader van het beheer en de uitvoering van de pensioenregelingen waarvoor het gebruik van persoonsgegevens relevant kan zijn. Dit betekent in beginsel dat de persoonsgegevens van aangeslotenen en begunstigden worden bewaard tot: - in geval van uitkering van een eenmalig pensioenkapitaal: indien het pensioenkapitaal reeds is uitgekeerd: maximaal tien (10) jaar na de wettelijke pensioenleeftijd en tien (10) jaar na de uitkering van het pensioenkapitaal aan de aangeslotene; - bij uitkering van pensioenrente: tien (10) jaar na de uitkering van de laatste pensioenrente aan de aangeslotene; bij uitkering van een eenmalige overlijdensuitkering: tien (10) jaar na de uitkering van de overlijdensuitkering aan de begunstigde; - bij betaling van nabestaandenpensioenen: tien (10) jaar na de betaling van het laatste nabestaandenpensioen aan de begunstigde; - in geval van individuele overdracht van verworven reserves: tien (10) jaar na de wettelijke pensioenleeftijd. Prolocus heeft een gegevensclassificatiebeleid geïmplementeerd, dat de classificatie van persoonlijke gegevens en beveiligingsvereisten per classificatieniveau omvat. Er is ook een ROPA (Register van verwerkingsactiviteiten) beschikbaar, dat onder andere het doel van de verwerkingsactiviteit, de categorie persoonsgegevens en de rechtsgrondslag voor elke activiteit bevat.	3	Zorg ervoor dat gegevens niet langer worden opgeslagen dan nodig is voor de aangegeven doeleinden. Zorg ervoor dat het gegevensclassificatiebeleid up-to-date wordt gehouden. Overweeg certificeringsmechanisme om aan te tonen dat de verwerkingsactiviteiten voldoen aan de AVG conform artikel 42.
Art. 32, 1, a) Pseudonymisering en versleuteling van persoonsgegevens	Er is geen informatie beschikbaar over versleuteling of pseudonimisering van persoonsgegevens.	1	Om volledige end-to-end versleuteling van gegevens te garanderen, worden aanvullende maatregelen aanbevolen: - Encryptie van gegevens 'in rust' in cloudomgevingen (bijv. Sharepoint) - Volledige schijfversleuteling van lokale harddrivers met tools zoals Veracrypt of Bitlocker Controleer gepseudonimiseerde datasets op mogelijke heridentificatie en/of onjuiste anonimisering.

2. AVG Maturiteitsanalyse

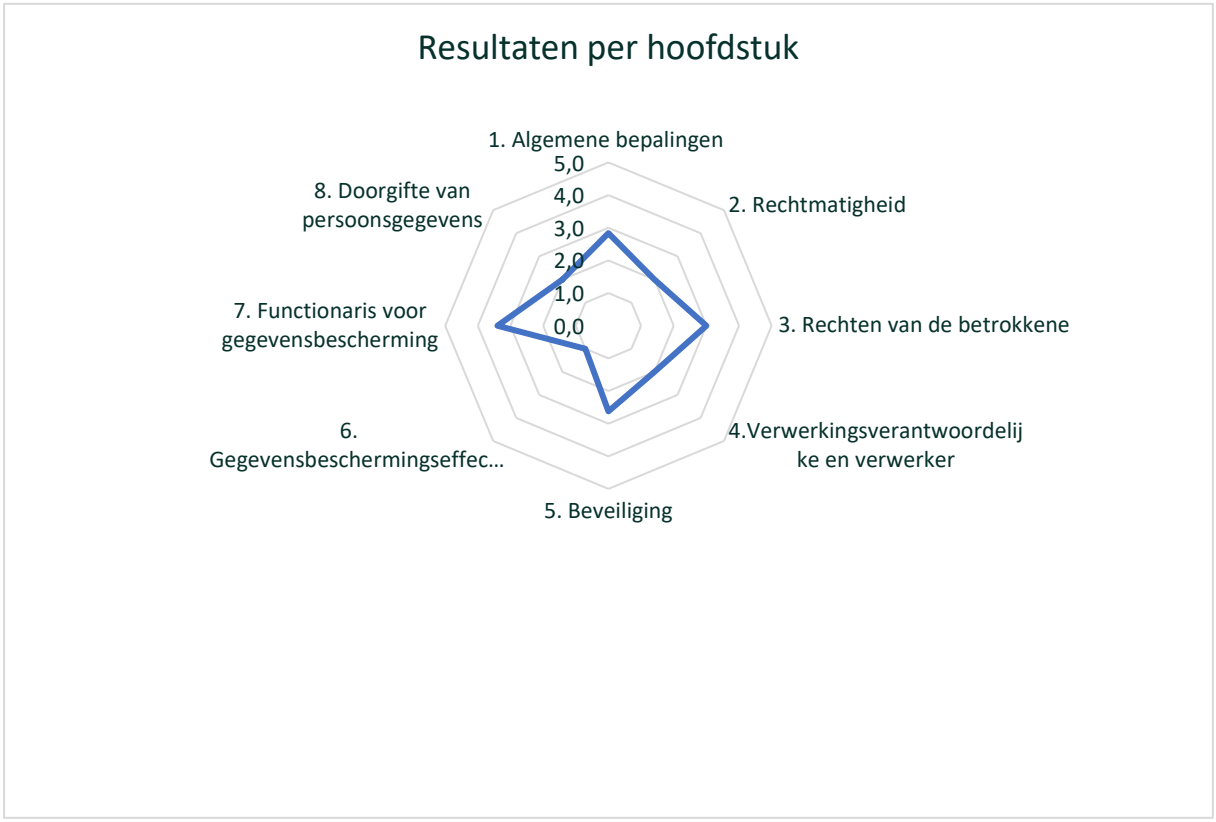
Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 32, 1, b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen	Om ongeoorloofde toegang tot persoonsgegevens door derden te voorkomen, worden alle elektronische persoonsgegevens die door Prolocus en haar verwerkers worden bewaard, opgeslagen in systemen die beschermd zijn door een veilige en up-to-date netwerkarchitectuur, uitgerust met firewalls en toegangsdetectieapparatuur. De servers bevinden zich in hoogbeveiligde faciliteiten, waar ongeoorloofde toegang wordt vermeden en branddetectie- en reactiesystemen in werking zijn. Er worden gepaste maatregelen genomen om gegevensfraude te voorkomen, om onbekende en ongeoorloofde toegang tot de computersystemen en informatie te weren en om adequate bescherming te bieden aan de persoonsgegevens die in het bezit zijn van Prolocus en de verwerkers. Alle gegevens worden vertrouwelijk bewaard in veilige en afgesloten archiefkasten of kamers. De toegang tot de geautomatiseerde databases wordt gecontroleerd door inloggegevens en vereist identificatie door middel van een wachtwoord voordat toegang wordt verleend. Geautoriseerde gebruikers hebben alleen toegang tot gegevens voor zover dit nodig is om hun functies in de administratie en uitvoering van de pensioenplannen uit te voeren.	2	Documenteer en rvalueer regelmatig de beveiligingsmaatregelen. Houd een sensibiliseringssessie voor gegevensbeveiliging. Voer een beoordeling uit of OFP Prolocus onder het toepassingegebied van van de nieuwe NIS-2 wet, en voer desgevallend een risicoanalyse uit overeenkomstig het beschreven veiligheidsniveau (basis / belangrijk / essentieel).
Art. 32, 1, c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen	Er bestaat een "back-up" van de gegevens die op de servers zijn opgeslagen, zodat de gevolgen van onopzettelijke verwijdering, vernietiging of verlies kunnen worden voorkomen.	3	Van de database moet regelmatig een back-up worden gemaakt en de herstelprocedure moet volledig worden doorgelicht voordat de database wordt ingezet. De effectiviteit van de herstelprocedures moet op gezette tijden worden geëvalueerd.
Art. 32,1,d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking	Beheerders moeten in staat zijn om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten doorlopend te garanderen. Prolocus heeft geen informatiebeveiligingsbeleid	2	Ontwerp van een informatiebeveiligingsbeleid.
Art. 33 Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit	In het geval dat de inbreuk ernstige negatieve gevolgen heeft of kan hebben voor de bescherming van de betreffende persoonsgegevens, moet deze worden gemeld aan de gegevensbeschermingsautoriteit in overeenstemming met de AVG binnen 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen. Prolocus heeft een beleid inzake inbreuken opgesteld, met inbegrip van een tool voor gegevenslekken evenals een inbreukprocedure, die door alle geautoriseerde gebruikers moet worden gevolgd bij de verwerking van persoonsgegevens in het kader van de pensioenregelingen en die alle processen bevat die moeten worden gevolgd in het geval van een (potentiële) Inbreuk.	4	Voer beoordelingen uit van de ernst van de gevolgen van (potentiële) datalekken. Zorg er voor auditdoeleinden voor dat de incidentenlijst voor datalekken accuraat is en up-to-date wordt gehouden.
Art. 34 Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene	In bepaalde gevallen zal Prolocus ook de betrokken partijen die getroffen zijn door deze inbreuk zonder redelijke vertraging op de hoogte stellen.	4	Zorg er voor auditdoeleinden voor dat het register voor datalekken accuraat is en up-to-date wordt gehouden.
Afdeling 3 - Gegevensbeschermingseffectenbeoordeling en voorafgaande raadpleging			
Art. 35 Gegevensbeschermingseffectenbeoordeling	Er is geen informatie over de gegevensbeschermingseffectbeoordeling (DPIA) die is uitgevoerd door het OFP Prolocus.	1	Zorg ervoor dat bij verwerkingsactiviteiten met een hoog risico een DPIA wordt uitgevoerd.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 36 Voorafgaande raadpleging	Wanneer uit een DPIA blijkt dat de verwerking een hoog risico inhoudt, indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke de toezichthoudende autoriteit voorafgaand aan de verwerking.	1	
Afdeling 4 - Functionaris voor gegevensbescherming			
Art. 37 Aanwijzing van de functionaris voor gegevensbescherming ('DPO')	De functionaris voor gegevensbescherming werd in overeenstemming met de voorschriften benoemd op basis van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van gegevensbeschermingswetgeving en -praktijk.	4	Kondig de nieuwe functionaris voor gegevensbescherming aan bij de gegevensbeschermingsautoriteit.
Art. 38 Positie van de functionaris voor gegevensbescherming	De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitoefening van deze taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitoefening van zijn taken. De functionaris voor gegevensbescherming rapporteert rechtstreeks aan de hoogste manager van de verwerkingsverantwoordelijke of de verwerker. Het privacybeleid zorgt er ook voor dat betrokkenen contact kunnen opnemen met de functionaris voor gegevensbescherming over alle kwesties met betrekking tot de verwerking van hun persoonsgegevens en hun rechten onder de AVG kunnen uitoefenen.	3	Het wordt aanbevolen om regelmatig verslag uit te brengen aan het hoogste management over zaken met betrekking tot de bescherming van persoonsgegevens. Evalueer op geregelde tijdstippen de inzet aan mandagen voor de functionaris.
Art. 39, 1, a) De verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen	De functionaris voor gegevensbescherming is verantwoordelijk voor het informeren en adviseren van de verwerkingsverantwoordelijke en de werknemers/consultants die de verwerking uitvoeren over hun verplichtingen volgens de wet- en regelgeving inzake gegevensbescherming. Bovendien is de functionaris voor gegevensbescherming verantwoordelijk voor het geven van advies waar dat gevraagd wordt met betrekking tot de gegevensbeschermingseffectbeoordeling en het toezicht op de uitvoering ervan.	3	De functionaris voor gegevensbescherming is verantwoordelijk voor het informeren en adviseren van de verwerkingsverantwoordelijke en voor het adviseren van de werknemers over nieuwe verwerkingsactiviteiten. Registreer voor nalevingsdoeleinden het advies dat de functionaris voor gegevensbescherming heeft gevraagd en gegeven. Werknemers/consultants die de verwerking uitvoeren worden ingelicht over hun verplichtingen volgens de wet- en regelgeving inzake gegevensbescherming.

2. AVG Maturiteitsanalyse

Artikel *(relevant artikel van de AVG)*	**Beschrijving van de situatie** *(situatie "zoals die is" op het moment van beoordeling)*	**MATURITEIT** *geef een score tussen 0 (afwezig) en 5 (geoptimaliseerd)*	**Aanbevelingen** *(beschrijft maatregelen die moeten worden genomen om de maturiteit te verhogen)*
Art. 39, 1, b) Toezicht op naleving van de AVG	De functionaris voor gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de relevante wet- en regelgeving inzake gegevensbescherming en van het beleid van de verwerkingsverantwoordelijke of de verwerker inzake de bescherming, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en training van personeel dat betrokken is bij verwerkingsactiviteiten en bijbehorende audits. Bovendien is de functionaris voor gegevensbescherming verantwoordelijk voor het desgevraagd verstrekken van advies met betrekking tot de gegevensbeschermingseffectbeoordeling en het toezicht op de uitvoering ervan.	3	Voer audits van informatiesystemen uit om ervoor te zorgen dat gegevens worden verwerkt in overeenstemming met de AVG-standaardverwerkingsprincipes. Organiseer gegevensbeschermingstrainingen voor managers. Organiseer AVG-bewustmakingssessies voor werknemers. Stel een beleid op over de bescherming van persoonsgegevens voor werknemers van Prolocus.
Art. 39, 1, e) Optreden als een contactpunt voor de toezichthoudende autoriteit	De functionaris voor gegevensbescherming is verantwoordelijk voor de samenwerking met de toezichthoudende autoriteit en treedt op als contactpersoon voor de toezichthoudende autoriteit voor kwesties met betrekking tot de verwerking, met inbegrip van voorafgaande raadpleging, en om indien nodig overleg te plegen over andere kwesties. De vorige functionaris voor gegevensbescherming werd bij de gegevensbeschermingsautoriteit aangemeld. De nieuwe functionaris voor gegevensbescherming moet echter bij de autoriteiten worden aangemeld.	4	Kondig de nieuwe functionaris voor gegevensbescherming aan bij de gegevensbeschermingsautoriteit.
Hoofdstuk V. Doorgifte van persoonsgegevens aan derde landen of internationale organisaties			
Art. 45 Doorgiften op basis van adequaatheidsbesluiten	In het kader van de beschikbare informatie en documentatie is het niet duidelijk of Prolocus Persoonsgegevens buiten de EER doorgeeft.	2	Controleer of er gegevensverwerkers zijn die gegevens buiten de EU/EER verwerken en of deze onder het toepassingsgebied van een adequaatheidsbesluit (bijvoorbeeld US-EU Data Privacy Framework) vallen.
Art. 46 Doorgiften op basis van passende waarborgen	Hetzelfde als hierboven.	2	Als persoonlijke gegevens buiten de EER worden overgedragen, moet er in bepaalde gevallen een "Effectbeoordeling overdracht" ('Data Transfer Impact Assessement') worden uitgevoerd.


Resultaten per hoofdstuk
1. Algemene bepalingen
5,0
4,0
3,0
2,0
1,0
0,0
2. Rechtmatigheid
3. Rechten van de betrokkene
4.Verwerkingsverantwoordelijke en verwerker
5. Beveiliging
6. Gegevensbeschermingseffec…
7. Functionaris voor gegevensbescherming
8. Doorgifte van persoonsgegevens

3. ACTIEPLAN

ACTIEPLAN GEGEVENSBESCHERMING - voorstel aan het dagelijks bestuur			2024	2025				2026			
NR	Te ondernemen actie	Prioriteit	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Hoofdstuk I: Algemene bepalingen											
1	Uitvoeren van periodieke audits van de informatiesystemen van Prolocus om te controleren of de principes van 'minimale gegevensbescherming', 'opslagbeperking' en 'doelbinding' worden gewaarborgd.	LAAG						X			
2	Ervoor zorgen dat de periodes voor het bewaren van gegevens worden vastgesteld voor elk van de verwerkingsactiviteiten en de doeleinden ervan.	GEMIDDELD		X							
3	Vaststellen en implementeren van een procedure voor het vaststellen en handhaven van passende bewaarperioden.	GEMIDDELD			X						
4	Redelijke maatregelen nemen om onnauwkeurigheden te voorkomen tijdens het verzamelen van gegevens en tijdens het verwerken van gegevens.	LAAG									
5	Periodieke controles uitvoeren op de juistheid van de verzamelde en opgeslagen persoonsgegevens en ervoor zorgen dat onjuiste persoonsgegevens onmiddellijk worden verwijderd of gecorrigeerd.	LAAG			X						
6	Ervoor zorgen dat het beleid voor gegevensclassificatie up-to-date wordt gehouden.	LAAG				X					
7	Organiseren van een jaarlijkse 'data opruimdag'.	LAAG							X		
Hoofdstuk II: Rechtmatigheid											
8	Privacybeleid bijwerken waarin wordt uitgelegd of toestemming vereist is/wordt verkregen voor de verwerking van gevoelige gegevens.	GEMIDDELD			X						
9	Ervoor zorgen dat geldige toestemming kan worden aangetoond.	GEMIDDELD			X						
10	Gegevens verifiëren die worden verwerkt in het kader van de uitvoering van een contract zijn noodzakelijk in verband met de doeleinden waarvoor ze worden verwerkt.	GEMIDDELD			X						
11	Maken van een lijst en documenten van wetten en wettelijke verplichtingen waaraan de verwerkingsverantwoordelijke is onderworpen en waarop hij zich baseert als rechtsgrondslag voor de verwerking van persoonsgegevens.	GEMIDDELD				X	X				
Hoofdstuk III: Rechten van de betrokkene											
12	Een register opzetten om alle verzoeken van datasubjecten bij te houden.	GEMIDDELD		X							
13	Ervoor zorgen dat de privacyverklaring vlot toegankelijk is vanop de homapagina.	HOOG	X								
14	Ervoor zorgen dat het webformulier voor het uitoefenen van de rechten van de betrokkene gemakkelijk toegankelijk is.	HOOG	X								
15	Privacybeleid periodiek bijwerken	GEMIDDELD				X				X	
Hoofdstuk IV: Verwerkingsverantwoordelijke en verwerker											
16	Ervoor zorgen dat er een samenwerkingsovereenkomst met de provincie Antwerpen wordt ondertekend.	GEMIDDELD		X	X						
17	Kwalificatie van de bijdragende entiteiten uitklaren bij toegang tot het portaal	HOOG	X								
17	Ervoor zorgen dat alle verwerkersovereenkomsten worden gedocumenteerd en ondertekend.	GEMIDDELD		X	X	X					
18	Overleg met DPO Vlaams Pensioenfonds voor eventuele harmonisaties										
19	Het register van verwerkingsactiviteiten regelmatig bijwerken.	GEMIDDELD			X				X		

3. ACTIEPLAN

ACTIEPLAN GEGEVENSBESCHERMING - voorstel aan het dagelijks bestuur			2024	2025				2026			
NR	Te ondernemen actie	Prioriteit	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
20	Periodiek bijwerken van gegevensclassificatiebeleid	LAAG					X				X
21	Nalevingsdocumenten verplaatsen naar een online platform voor nalevingsbeheer.	GEMIDDELD				X	X				
22	Een duidelijk en actueel overzicht geven van technische en organisatorische maatregelen om persoonlijke gegevens te beveiligen.	GEMIDDELD			X	X					
23	Jaarlijkse vragenlijst minimale normen KSZ	GEMIDDELD			X				X		
24	Uitvoeren van een assessment of de organisatie onder het toepassingsgebied van de NIS2 valt	HOOG	X								
25	NIS-2 risico analyse conform vetrouwelijkheidscategorie (basis / belangrijk / essentieel)	GEMIDDELD									
26	Vertrouwelijkheidsovereenkomst en -beleid voor werknemers opstellen.	GEMIDDELD						X	X		
27	Periodiek testen van back-up en herstel.	LAAG							X		
28	Jaarlijkse maturiteitsanalyse uitvoeren.	HOOG	X				X				X
29	De kwetsbaarheid van informatiesystemen testen.	GEMIDDELD					X				X
30	Opstellen van beleid voor de gecoördineerde bekendmaking van kwetsbaarheden	LAAG								X	X
31	Personeel bewust maken van gegevensinbreuken.	GEMIDDELD				X				X	
32	Regelmatig het register van inbreuken op gegevens bijwerken.	GEMIDDELD					X				X
33	Voorafgaande gegevensbeschermingseffectbeoordelingen uitvoeren voor lijst verwerkingsactiviteiten	GEMIDDELD				X	X				
34	De nieuwe functionaris voor gegevensbescherming aankondigen bij de gegevensbeschermingsautoriteit	HOOG	X								
35	Ervoor zorgen dat de functionaris voor gegevensbescherming regelmatig rapporteert aan het management over het beleid voor de bescherming van persoonsgegevens.	GEMIDDELD		X				X			
36	Regelmatige controles van informatiesystemen uitvoeren om ervoor te zorgen dat gegevens worden verwerkt in overeenstemming met de standaard AVG-verwerkingsprincipes	LAAG					X				X
37	AVG-trainingen organiseren	GEMIDDELD				X				X	
38	Finalieeren van de controlelijst voor softwarebeveiliging.	GEMIDDELD						X			
39	Volledige schijfversleuteling implementeren (Bitlocker)	GEMIDDELD						X			
40	Opstellen van een informatiebeveiligingsbeleid	GEMIDDELD				X	X				
Hoofdstuk V: Doorgifte van persoonsgegevens aan derde landen of internationale organisaties											
41	Bekijken welke verwerkers gegevens buiten de EU/EER verwerken.	GEMIDDELD						X	X		
42	Uitvoeren impactanalyses voor gegevensdoorgifte	LAAG								X	X

4. LEGENDA

Maturiteitsscore	Toelichting (*)
0	**Afwezig** - maatregelen ontbreken volledig binnen de organisatie.
1	**Ad hoc** - procedures of processen zijn over het algemeen informeel, onvolledig en worden niet consequent toegepast.
2	**Herhaalbaar** - procedures of processen bestaan; ze zijn echter niet volledig gedocumenteerd en bestrijken niet alle relevante aspecten.
3	**Gedefinieerd** - procedures en processen zijn volledig gedocumenteerd en geïmplementeerd, en dekken alle relevante aspecten
4	**Beheerd** - beoordelingen worden uitgevoerd om de effectiviteit van controles te waarborgen.
5	**Geoptimaliseerd** - regelmatige evaluatie en feedback worden gebruikt om te zorgen voor verbetering naar optimalisatie van het gegeven proces.
(*) Gebaseerd op AICPA/CICA, Privacy Maturity Model, Maart 2011.	

Prioriteiten	
LAAG	Moet worden geïmplementeerd als de tijd het toelaat, maar kan worden uitgesteld.
GEMIDDELD	Niet dringend, maar uw verantwoordelijkheid en AVG-naleving kunnen in het gedrang komen
HOOG	Moet dringend worden geïmplementeerd, naleving komt in het gedrang totdat de maatregel is geïmplementeerd.