| | |
|---|---|
| Datum | **2023** |
| Onderwerp | **Data Protection Impact Assessment** |
| Project / Verwerking | **Registration Authority** |

# 1. INHOUD

# 2. ALGEMENE CONTEXT EN DOELBEPALING

## 2.1. CONTEXT VERWERKINGSACTIVITEITEN

Binnen het JustSign project kwam de nood om de gebruikers binnen justitie te voorzien van een gekwalificeerde handtekening zoals bepaald in de eIDAS-verordening. Om deze gekwalificeerde handtekening te genereren dient ze gebaseerd te zijn op een gekwalificeerd certificaat voor elektronische handtekeningen. [1] Dit certificaat kan enkel aangeleverd worden door een vertrouwensdient, waarbij FOD Justitie gekozen heeft om samen te werken met de certificaatautoriteit Be-Ys[2] (verder CA).

Om ervoor te zorgen dat de juiste gebruiker het certificaat toegewezen wordt, is er nood aan de oprichting van een Registration Authority (verder RA). De RA staat specifiek in voor de controle van de identiteit van de gebruiker alvorens de aanvraag naar de CA door te sturen. De CA zal er op zijn beurt voor zorgen dat de aanmaak en revocatie van de digitale certificaten gegenereerd worden, zodat de documenten voorzien kunnen worden van een digitale handtekening door middel van het gebruik van de JustSign applicatie. Daarnaast kan via de JustSign applicatie de gebruiker de ondertekende documenten raadplegen om de elektronische handtekening of zegel te verifiëren.

Deze gegevensbeschermingseffectenbeoordeling (of DPIA) beperkt zich tot de taken van de Registration authority.

[1] Art. 3§12 eIDAS verordening

[2] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/LU/3/1

## 2.2. DEFINITIES

| | |
|---|---|
| elektronische identificatie | het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden |
| elektronisch identificatiemiddel | een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst |
| persoonsidentificatiegegevens | een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld |
| authenticatie | een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt |
| ondertekenaar | een natuurlijke persoon die een elektronische handtekening aanmaakt |
| elektronische handtekening | gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen |
| geavanceerde elektronische handtekening | een elektronische handtekening die voldoet aan de wettelijk voorgeschreven eisen |
| gekwalificeerde elektronische handtekening | een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen |
| gegevens voor het aanmaken van elektronische handtekeningen | unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken |
| certificaat voor elektronische handtekeningen | een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt |

| | |
|---|---|
| gekwalificeerd certificaat voor elektronische handtekeningen | een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de wettelijk voorgeschreven eisen |
| vertrouwensdienst | een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:<br>a) het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of<br>b) het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of<br>c) het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben; |
| gekwalificeerde vertrouwensdienst | een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in verordening nr. 910/2014 |
| conformiteitsbeoordelingsinstantie | een instantie die in overeenstemming met verordening nr. 765/2008 art. 2 geaccrediteerd is om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten |
| gekwalificeerde verlener van vertrouwensdiensten | een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen |
| product | software of hardware, of relevante componenten van hardware of software, die bedoeld zijn om te worden gebruikt voor de verlening van vertrouwensdiensten |
| middel voor het aanmaken van elektronische handtekeningen | geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken |
| elektronische tijdstempel | gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden |
| elektronisch document | elke inhoud die is opgeslagen in elektronische vorm, in het bijzonder tekst of geluid, beeld of audiovisuele opname |

| | |
|---|---|
| dienst voor elektronisch aangetekende bezorging | een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen |
| certificaat voor websiteauthenticatie | attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven |
| valideringsgegevens | gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren |
| validering | proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of een elektronisch zegel geldig is |
| elektronisch zegel | gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen |
| DPIA | Data Protection Impact Assessment |
| RA | Registration authority |
| IAM | Identity and Access Management |

## 2.3. NOODZAAK DPIA?

De AVG vereist dat verwerkingsverantwoordelijken passende maatregelen treffen om de naleving van de AVG te waarborgen en te kunnen aantonen, onder meer rekening houdend met "de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen" (artikel 24, lid 1).

De verplichting voor de verwerkingsverantwoordelijken om in bepaalde omstandigheden een DPIA uit te voeren, moet worden begrepen tegen de achtergrond van hun algemene verplichting om risico's die verbonden zijn aan de verwerking van persoonsgegevens op passende wijze te beheren.

| | |
|---|---|
| x | De verwerking betreft innovatief gebruik van een nieuw technologische of organisatorische oplossing[3] |
| x | Het betreft persoonsgegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade, met name waar de verwerking kan leiden tot [4]:<br>- identiteitsdiefstal of –fraude<br>- reputatieschade<br>- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens<br>- enig ander aanzienlijk economisch of maatschappelijk nadeel |

[3] ARTICLE 29 DATA PROTECTION WORKING PARTY, WP 248: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 3.B.a.8.

[4] Ibid, 3.B.a.4 & 3.B.a.7

# 3. LEGALITEIT EN RECHTMATIGHEID VAN DE VERWERKING

## 3.1. VERWERKINGSDOELEINDEN

Het doel is om de nodige processen op te zetten om de leden van FOD Justitie en de Rechterlijke Orde als subscribers in de RA te kunnen registreren. De registration authority heeft de taak om de identificatiegegevens van de aanvrager te verzamelen, te controleren, te registreren en door te sturen ten behoeve van de certificaatuitgifte.

De certificaatautoriteit verleent het gekwalificeerde certificaat, om vervolgens documenten op een gekwalificeerde wijze in de JustSign applicatie te kunnen ondertekenen, al dan niet in bulk.

## 3.1. WETGEVEND KADER

### WETGEVING

Verordening (EU) nr. 679/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Richtlijn (EU) nr. 680/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

Wet 18 juli 2017 inzake elektronische identificatie, *B.S. 9 augustus 2017*

Wet 9 juli 2001 houdende de vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, *B.S.* 29 september 2001[5]

Wetboek 13 april 2019, Burgerlijk wetboek

## ADVIEZEN TOEZICHTHOUDENDE AUTORITEIT

Aanbeveling 01/2008 met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector

Advies 29/2011 betreft de adviesaanvraag van een wetsvoorstel tot wijziging van het gerechtelijk wetboek met het oog op de invoering van telecommunicatiemiddelen en de elektronische handtekening in de gerechtelijke procedure.

Advies 30/2011 betreft de adviesaanvraag van een wetsvoorstel tot wijziging van de wet van 10 juli 2006 betreffende de elektronische procesvoering wat betreft de inwerkingtreding van artikel 863 van het Gerechtelijk Wetboek

Advies 10/2016 uit eigen beweging over de gebruikmaking van cloudcomputing door de verantwoordelijke voor de verwerking.

Advies 47/2018 betreft de adviesaanvraag van het voorontwerp van wet inzake de elektronische uitwisseling van berichten met overheidsinstanties

Advies 65/2021 m.b.t. een ontwerp van koninklijk besluit tot veralgemeend gebruik van elektronische identificatiemiddelen die deel uitmaken van een aangemeld stelsel voor elektronische identificatie

## MACHTIGINGEN GEBRUIK RIJKSREGISTERNUMMER

Aanbeveling nr. 01/2008 met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector

Beraadslaging RR nr 21/2015 met betrekking tot algemene machtiging om het rijksregisternummer te gebruiken bij aanwending van het “Federal Authentication Service” –systeem van FEDICT voor het

[5] Opgeheven door Wet 21 juli 2016 tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhavingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht, *B.S.* 28 september 2016

toegangs- en gebruikersbeheer tot van de informatietoepassingen die ontwikkeld zijn voor opdrachten van algemeen belang

## 3.2. RECHTMATIGHEID VAN DE VERWERKING

De handtekening van een rechtssubject is van essentieel belang, daar de handtekening de ondertekenaar het toelaat de inhoud te verifiëren en vervolgens in te stemmen met de inhoud van het te ondertekenen document. De handtekening is het element dat in alle akten bepalend is om de oprechtheid en de herkomst van de akte te waarborgen. Het is het teken waarmee de onderschrijver zijn akkoord definitief bevestigt.

De rechtmatigheid van deze verwerkingsactiviteit stoelt enerzijds op een wettelijke verplichting die rust op de rechterlijke orde vanuit hun mandaat, waarbij het belangrijk is om de documenten met een rechtsgeldig karakter te voorzien van een rechtsgeldige handtekening[6]. Anderzijds zijn de opmaak en het gebruik van deze documenten een noodzakelijkheid bij de uitvoering van hun taken van algemeen belang.

Daar het belangrijk is om de scope van deze DPIA voor ogen te houden, en het niet gaat om een analyse van de JustSend of JustSign applicatie in zijn geheel, echter slechts een onderdeel hiervan, **namelijk de toewijzing van het certificaat die ervoor zal zorgen dat de handtekening de juiste kwalificatie krijgt door de RA om te voorzien in een rechtsgeldig karakter**. Deze rechtmatigheid vloeit voort vanuit een taak van algemeen belang. Voor deze taken is de RA onderworpen aan de Wet 9 juli 2001 houdende de vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten.

[6] Ger. W.

# 4. BETROKKEN ACTOREN

## 4.1. FOD JUSTITIE ALS VERWERKINGSVERANTWOORDELIJKE

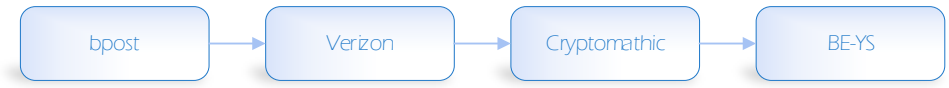
Het RA-proces wordt uitgevoerd door de leden van de “Registration Authority”. De leden van de RA office worden door FOD Justitie tewerkgesteld en werden een specifieke rol toegewezen. (zie infra “Categorieën betrokkene”)

Hun taak bestaat erin om op te volgen wie een certificaat nodig heeft of niet. Dit omvat zowel de validatie van identiteit en verantwoordelijkheid van de aanvrager, de toewijzing, de verlenging, de wijziging en de intrekking van het certificaat.

## 4.2. BE-YS

BE-YS is de certificaatautoriteit die erkend is om gekwalificeerde certificaten aan te leveren na validatie van de RA. De maatschappelijke zetel is gelokaliseerd in Luxemburg.

Zonder uit te diepen welke contractuele noden er van toepassing zijn binnen de structuur, wordt hier kort aangehaald hoe de contractuele relatie gevisualiseerd en gedefinieerd wordt. Dit heeft een belang om te bepalen of er al dan niet een verwerkingsovereenkomst in de zin van art. 28, Algemene Verordening Gegevensbescherming van toepassing is of een andere rechtshandeling om de afspraken met betrekking tot gegevensbescherming te waarborgen.




- BE-YS is een subprocessor van Cryptomathic, die de rol van Signer RA op zich neemt.
- Cryptomathic is een subprocessor van Verizon.
    - End User Sw License with maintenance and support provisions between Cryptomathic and FOD Justitie
- Verizon is een subprocessor van bpost
    - Contract ref 569082 – Europe Service Agreement between NV Verizon Belgium Luxemburg SA and Certipost NV
    - Professional Services Statement of work ID 02929751

## 4.3. ICT PARTNERS BINNEN FOD JUSTITIE

### PWC

PWC werkt aan het 'IAM project', het access management systeem van FOD Justitie, waar de rollen en verantwoordelijkheden van de werknemers van de FOD gedefinieerd, toegewezen en opgevolgd worden. Kortom een beheersysteem dat ervoor zorgt dat de gegevens over identiteiten en autorisaties worden beheerd en gebruikt om toegang te verlenen tot applicaties.

### MICROSOFT

Is de hostingservice die volgende componenten aanlevert:

- Azure AD
- Azure cloud center of Excellence

### PROXIMUS

Proximus is verantwoordelijk voor de SECaaS VPN.

# 5. VERWERKINGSACTIVITEITEN

## 5.1. VERWERKINGSACTIVITEITEN

De verwerkingsactiviteiten worden hieronder gegroepeerd per beoogd doel.

1. Gebruiker authentiseren en autoriseren
    a. Registreren van de identiteit van de gebruiker
    b. Valideren van de gebruiker
    c. Goedkeuren toegang gebruiker door middel van het toekennen van een certificaat
    d. Verlengen van de toegang gebruiker door aanmaak van een nieuw certificaat
    e. Wijzigen / Aanpassen gebruikersgegevens door aanmaken van een nieuw certificaat
    f. Gebruiker toegang weigeren na off-boarding door middel van intrekken certificaat

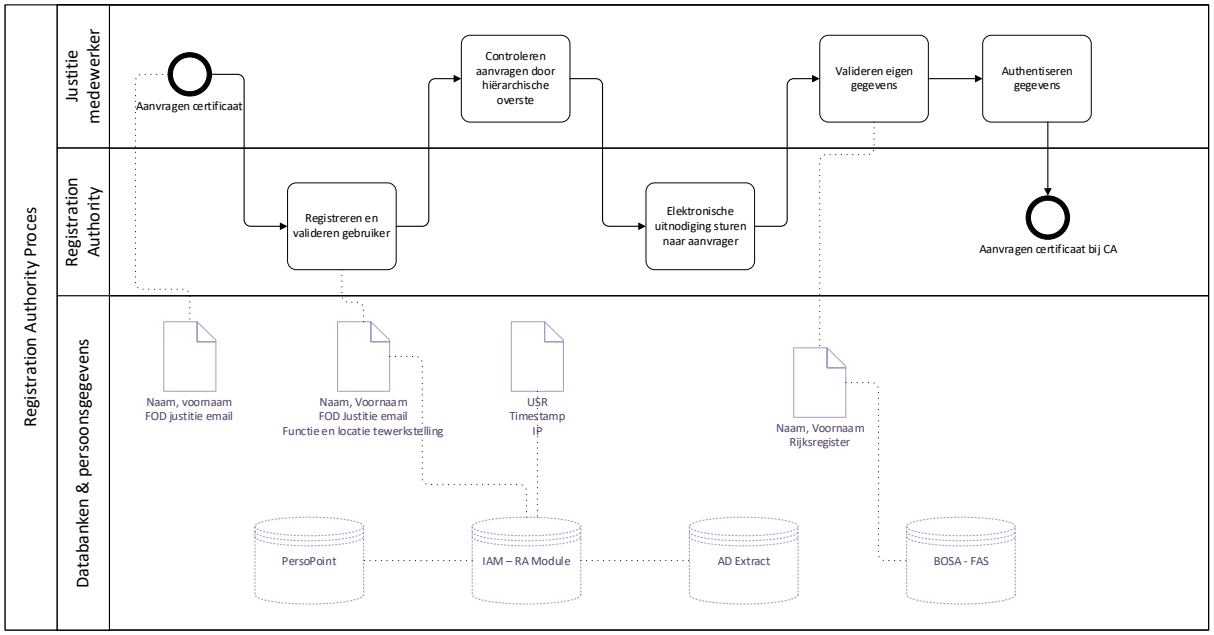
2. Audittrail van de Applicatie
    a. Auditlogging
    b. Monitoring activiteit van de applicatie

3. Documenten handtekenen. Dit is een ***JustSign*** proces, wat impliceert dat deze activiteiten buiten de scope van de DPIA RA vallen, en die louter neergeschreven worden ter vervollediging van de verwerkingsactiviteiten. Eveneens worden deze genoteerd om de gegevensstromen te kaderen die in het volgende punt worden weergegeven.
    a. Identificatie van gebruiker
    b. Importeren van de te handtekenen documenten
    c. Selectie van de te handtekenen documenten
    d. Confirmatie van het type geplaatste handtekening op het desbetreffende document
    e. Registreren van datum en tijd bij het plaatsen van de gekwalificeerde handtekening op het document (certificaat)
    f. Vermelden van de functie, plaats van uitvoering van deze functie en de datum van ondertekening in de “stamp” op het document
    g. Omzetten van document naar een ondertekend geschrift, al dan niet onder de vorm van een authentieke akte
    h. Raadplegen van de gehandtekende documenten

## 5.2. TECHNISCHE VOORSTELLING

### SCHEMATISCHE VOORSTELLING GEGEVENSSTROMEN

Voor de DPIA gaat het om volgend proces waarbij de betrokken vraagt om een certificaat, en waarbij na identity proofing van de RA door certificating authority een certificaat wordt toegekend.




### COMPONENTEN/ASSETS

| Component | Doel van de asset |
|---|---|
| Azure Cloud | Back-end van de applicatie |
| IAM, RA module | Registratie en validatie tool voor het aanvragen van certificaten gebruikt voor het tekenen van documenten binnen Justitie |
| SeCaas & VPN | Versleutelde verbinding voor de distributie van gegevens |
| Autoritatieve bron personeelsgegevens:<br>- PersoPoint<br>- AD Extract | Definieert de ICT functieprofielen binnen de Justitie |

## 5.3. CATEGORIEËN PERSOONSGEGEVENS

### CATEGORIEËN VAN PERSOONSGEGEVENS DIE VERWERKT TIJDENS DE **RA PROCEDURE**:

- Gebruikers attributen:
    - Naam en voornaam
    - Email FOD Justitie
    - Functie
    - Locatie tewerkstelling
    - Timestamp: Datum en tijdstip van handtekenen

Dit met als doel om het certificaat toe te kennen, te wijzigen, te hernieuwen of te weigeren.

### CATEGORIEËN VAN PERSOONSGEGEVENS DIE VERWERKT WORDEN DOOR DE **IT SYSTEMEN (CERTIFICAAT ZELF)**:

- Metadata
    - USR gegevens; naam en voornaam
    - Datum en tijdsregistratie van uitgifte certificaat
    - Elektronische identificatiegegevens
    - Authenticatie dmv gehashed Rijksregisternummer

### INFORMATIEF: CATEGORIEËN PERSOONSGEGEVENS DIE VERWERKT WORDT BIJ HET **TE HANDTEKENEN DOCUMENT**

- Elektronische handtekening
    - Naam en voornaam
    - Functie
    - Locatie tewerkstelling
    - Timestamp: Datum en tijdstip van handtekenen

Zoals supra omschreven, deze categorie persoonsgegevens wordt genoteerd om duiding te geven bij de schematische voorstelling van persoonsgegevens en is **niet** relevant voor deze DPIA.

## 5.4. CATEGORIEËN BETROKKENEN

- JustSign's Registration Authority verantwoordelijken
- Geregistreerde medewerkers binnen de rechterlijke orde en de FOD Justitie
- Medewerkers van de ICT helpdesk die admin rechten hebben ter ondersteuning van de werking van de applicatie

## 5.5. OPSLAGBEPERKING EN BEWAARTERMIJN

De RA office houdt initieel geen data bij. Het certificaat wordt toegekend voor een periode van 3 jaar en bewaard bij de CA. De IAM applicatie bewaart de logging gegevens van de RA module, en staat eveneens los van deze DPIA.

De RA is afhankelijk van het on- en off-boarding proces om bij wijziging van de situatie van de betrokkene de toegang te herzien of te weigeren.

# 6. RECHTEN VAN DE BETROKKENE

Voor elke verwerking van persoonsgegevens moet er een rechtsgrond zijn (AVG, artikel 6). Voor de verwerkingen uitgevoerd door de RA, is de rechtsgrond Algemeen belang van toepassing. Afhankelijk van de rechtsgrond en in bepaalde gevallen ook de context van de verwerking van persoonsgegevens of het type van verwerking van persoonsgegevens, zijn bepaalde rechten van betrokkenen al dan niet van toepassing. Dit schema biedt een overzicht welke rechten van betrokkenen al dan niet van toepassing zijn:

| Rechtmatigheid + Rechten betrokkenen | Algemeen belang |
|---|---|
| **Informatie** | x |
| **Recht op inzage, kopie en rectificatie** | x |
| **Wissing (+ kennisgevingsplicht)** | (uitzonderingen mogelijk) |
| Beperking van de verwerking<br>**(+ kennisgevingsplicht)** | x |
| **Recht van bezwaar tegen de verwerking** | x |
| **Niet onderwerpen aan geautomatiseerde besluitvorming, profilering** | n.v.t. |

## 6.1. HOE WORDEN DE BETROKKENE GEÏNFORMEERD OVER DE VERWERKING

De nieuwe manier van werken vloeit voort vanuit de verdere digitalisering van justitie waarbij de bestaande processen op een digitale wijze kunnen worden uitgevoerd. Om tegemoet te komen aan het transparantiebeginsel, is het noodzakelijk om een transparantieverklaring op te stellen en deze mee te delen met de betrokkenen eens het nieuwe proces in voege gaat. Dit zal eerder zich toespitsen op het volledige JustSign proces dan de gegevensstromen die besproken zijn in deze DPIA.

Specifiek voor de Registration Authority officers zijn er trainingsessies voorzien waarbij de betrokken profielen leren werken met de software en hun specifiek opgelegde taak. Dit is eerder een bewustmaking rond de gegevens die verwerkt worden om tegemoet te komen aan de vraag om een certificaat toe te kennen.

De algemene transparantie verklaring met betrekking tot de JustSign applicatie wordt bij de registratie van de betrokkene voorgelegd om goed te keuren voor kennisname bij de onboarding.

## 6.2. HOE KUNNEN DE BETROKKENE HUN RECHTEN UITOEFENEN?

### RECHT OP INZAGE, RECHT OP EEN KOPIE EN RECHT OP RECTIFICATIE

Het certificaat kan enkel toegekend worden door de RA wanneer de aanvrager geregistreerd staat in de personeelsdatabase van FOD Justitie. Er is door de RA een validatie van naam, voornaam en functie en locatie tewerkstelling van de betrokkene.

De betrokkene heeft de mogelijkheid om zijn recht op inzage en kopie op te vragen via de aangestelde DPO en het toegekende e-mailadres gegevensbescherming.

Het recht op rectificatie is niet mogelijk door de RA. Hiervoor zal de betrokkene zich dienen te wenden tot de personeelsdienst om de gegevens juist te laten reflecteren. Wanneer de gegevens aangepast zijn kan de RA overgaan tot een nieuwe validatie van de gegevens en de CA de vraag stellen een nieuw certificaat te genereren en toe te kennen.

De certificaatautoriteit registreert volgende gegevens:

- Certificaat: naam, voornaam en hashed rijksregisternummer
- Zegel: omvat naam, voornaam, functie, plaats, tijdsstempel

Op basis van de eIDAS verordening mag de certificaatautoriteit het rijksregisternummer gebruiken voor authenticatie, echter niet inlezen, vandaar dat het rijksregisternummer gehashed wordt opgeslagen, waarbij FOD justitie de private key beheert.

### RECHT OP WISSEN, BEPERKING VAN DE VERWERKING

Het recht op wissen het slechts betrekking hebben op de data die gelinkt is aan het certificaat of de zegel, waardoor de juiste informatie van de betrokkene gereflecteerd wordt op de te handtekenen documenten.

Het recht op wissen kan niet uitgevoerd worden door de RA daar hun taak enkel beperkt is tot het valideren van de aanvraag, wijziging of hernieuwing van het certificaat. Wel kan de RA de vraag stellen aan de CA om tegemoet te komen aan de vraag van de betrokkene. Dit neemt opgenomen te worden in de verwerkersovereenkomst.

Wanneer de RA een trigger krijgt dat de identiteit van de betrokkene gecompromitteerd is, kan de RA wel vragen aan de CA om het certificaat van de gecompromitteerde betrokkene te wissen.

## RECHT OM NIET ONDERWORPEN TE WORDEN AAN GEAUTOMATISEERDE BESLUITVORMING

De validatie van de gegevens is niet gebaseerd op geautomatiseerde besluitvorming.  De RA valideert de gegevens van de betrokkene via de personeelsdatabase en het IAM systeem.

# 7. GENOMEN RISICOBEPERKENDE MAATREGELEN

## 7.1. GEPLANDE OF BESTAANDE ORGANISATORISCHE MAATREGELEN

### ROLLEN EN VERANTWOORDELIJKHEDEN BIJ INFORMATIEBEVEILIGING

- Aanstelling van CISO en DPO binnen de FOD Justitie
- Duidelijke omschrijving van de taken van de RA office leden, en de betrokken partijen
- De verantwoordelijkheden van de verschillende stakeholders zijn binnen het project geïdentificeerd
- Is vervat in het IAM Project

### ORGANIGRAM

- Nood aan een organigram en de respectievelijke taken zodat bij een incident vlot kan gecommuniceerd en overlegd worden om dit zo snel mogelijk op te lossen

### INFORMATIEBEVEILIGING IN PROJECT MANAGEMENT

- Voor CBE zijn richtlijnen opgesteld welke stappen doorlopen moeten worden bij het opstarten van een project. De gegevensbeschermingseffectenbeoordeling is hier een onderdeel, net als de implementatie van de technische en organisatorische maatregelen. Concreet worden volgende stappen doorlopen:
    - Validatie rechtmatigheid van de beoogde verwerkingsactiviteiten getoetst met de DPO om te voldoen aan de wettelijke vereisten
    - Contractuele afspraken met de verwerkers en (joint) controllers
    - Eventueel aanvulling op de bestaande contractuele afspraken met details rond de beoogde verwerkingsactiviteiten, eventuele subverwerkers en de genomen technische en organisatorische maatregelen
- Bij het ontwerp werd rekening gehouden met het *privacy by design and by default*-principe. De strikt noodzakelijke gegevens worden geregistreerd om te voldoen aan de voorwaarde van dataminimalisatie, zoals in deze DPIA werd uiteengezet.
- De opstelling van een DPIA
- Aanvullen van het intern register met de nieuwe verwerkersactiviteiten

## RECHTEN VAN BETROKKENE

Artikel 12 – 14 AVG legt de wettelijke verplichting op om op een duidelijke transparante manier geïnformeerd te worden welke persoonsgegevens er verwerkt worden en door wie. Daarnaast is het belangrijk dat de betrokkene weet hoe deze zijn rechten kan uitoefenen.

Belangrijk om volgende elementen beschikbaar te hebben alvorens de RA office operationeel is:

- Emailadres
- Transparantieverklaring
- Uitgeschreven proces om tegemoet te komen aan de rechten van de betrokkene
- Incidentresponsplan met duidelijke verwijzingen wie welke verantwoordelijkheid op zich neemt

## VERWERKINGSOVEREENKOMSTEN/PROTOCOLAKKOORDEN

- Er zijn contractuele afspraken tussen de verschillende partijen met een clausule rond gegevensbescherming waarbij de verplichtingen voortvloeiend uit de verordening geduid worden. Er zijn geen gehandtekende verwerkersovereenkomsten of andere rechtshandelingen die een detail geven over de beoogde verwerkingsactiviteiten.
- De mogelijkheid om een audit te initiëren
- Voorleggen van een audit rapport met betrekking tot de security of het voorleggen van een certificaat cf. ISO27000.

## POLICIES EN PROCEDURES

| | |
|---|---|
| Niveau FOD Justitie<br><br>Draft versies | Policy – Risk Management<br>• Dit document beschrijft de richtlijnen over hoe de Federale Overheidsdienst Justitie [FOD] de risico's van vertrouwensdienst, informatiebeveiliging en privacy zal beheren door ze te identificeren, te analyseren en te evalueren of het risico moet worden aangepast door risicobehandeling om te voldoen aan de risicocriteria en rekening houdend met zakelijke en technische kwesties (REQ-5-01[1]).<br>• Om risico's op een systematische manier te beheersen, volgt [FPS] best practices zoals beschreven in de ISO/IEC 27001[2], 27701[3], 27005[4] en 31000[5] standaarden<br>Policy – Information Security<br>Policy – Organisation Reliability<br>• Het doel van dit beleid is om de nodige beveiligingscontroles vast te stellen om te voldoen aan de eIDAS-verordening (EU) nr. 910/2014[1], ETSI EN 319 401[2] en ISO/IEC 27002[3] voor de exploitatie- en beheerpraktijken van de RA.<br>Policy – Business Continuity<br>• Dit BCP is specifiek gericht aan de FOD Justitie, die instaat voor de registratie en validatie van gebruikers, de uitgifte van digitale certificaten en de algehele administratie van JustSign. Als zodanig strekt het zich niet uit tot de externe IT-infrastructuur, netwerken of andere applicaties en systemen die de algehele TSP-werking van JustSign ondersteunen.<br>Policy – Human Resources<br>Policy – Asset management<br>• Dit document is van toepassing op al het personeel (statutair, contractueel of gedetacheerd personeel, studenten en stagiaires, externe medewerkers – zijnde adviseurs, onderhoudspersoneel, leveranciers, enz.) bij [FOD] in het kader van de werking en het beheer van de RA.<br>Process – Endpoint Management<br>Process – Asset management<br>Policy – Access control<br>• Dit document is van toepassing op al het personeel (statutair, contractueel of gedetacheerd personeel, studenten en stagiaires, |

| | |
|---|---|
| | extern personeel – zijnde consultants, onderhoudspersoneel, leveranciers, enz.) bij [FOD] in het kader van de JustSign-applicatie en -infrastructuur. Dit bevat:<br>○ De toegangsrechten verleend aan de RA-functionaris en het RA-personeel voor het beheer van de RA.<br>○ De toegang tot de Azure-cloudinfrastructuur die de RA-activiteiten ondersteunt.<br>○ De toegang tot de JustSign applicatie zelf door de ondertekenaar.<br><br>Process – Access control<br><br>Policy – Cryptography<br><br>• Dit document specificeert algemene beleidsvereisten met betrekking tot een RA. Het definieert beleidsvereisten voor de werking en beheerpraktijken voor activabeheer op de technische omgeving die de RA-toepassing ondersteunt.<br><br>Het gebruik van cryptografie binnen de RA valt onder het Informatiebeveiligingsbeleid.<br><br>Policy – Physical and environmental Security<br><br>• Dit document is van toepassing op al het personeel (statutair, contractueel of gedetacheerd personeel, studenten en stagiaires, externe medewerkers – zijnde adviseurs, onderhoudspersoneel, leveranciers, enz.) bij [FOD] in het kader van de werking en het beheer van de RA.<br><br>Policy – Operation Security<br><br>• Dit document is van toepassing op al het personeel (statutair, contractueel of gedetacheerd personeel, studenten en stagiaires, externe medewerkers – zijnde adviseurs, onderhoudspersoneel, leveranciers, enz.) bij [FOD] in het kader van de werking en het beheer van de RA.<br><br>Process – Operation Security<br><br>Policy – Network security<br><br>• Dit document is van toepassing op al het personeel (statutair, contractueel of gedetacheerd personeel, studenten en stagiaires, externe medewerkers – zijnde adviseurs, onderhoudspersoneel, leveranciers, enz.) bij [FOD] in het kader van de werking en het beheer van de RA. .<br><br>Process – Network security |

| | |
|---|---|
| | Policy – Incident management<br>• Het doel van dit beleid is om de nodige beveiligingscontroles vast te stellen om te voldoen aan de eIDAS-verordening (EU) nr. 910/2014[1], ETSI EN 319 401[2] en ISO/IEC 27002[3] voor de exploitatie- en beheerpraktijken van de RA.<br>Policy – Secure application development<br>Policy – Cloud security |
| | |
| CBE<br>Bestaande documenten | Procedure – Onboarding<br>Procedure – Incident management<br>Procedure – Operational Security<br>Procedure – Access management<br><br>Policy - Telewerk<br>Gebruikersovereenkomst Laptop FOD Justitie<br>Gedragscode email, sociale media en internet<br>Risk exemption questionary (Mac OS/Win OS)<br>Handleiding projectmanagement |

## 7.2. GEPLANDE OF BESTAANDE MENSGERICHTE MAATREGELEN

### SCREENING

- Het personeel dient de kwalificaties voor te leggen voor de open vacature alvorens in aanmerking te komen als kandidaat
- Geplande maatregel: Het personeel binnen de FOD Justitie, personeel aangeleverd door consultancy bedrijven die een overheidsopdracht uitvoeren dienen een uittreksel strafregister voor te leggen bij aanwerving.

### RECHTEN EN PLICHTEN VAN DE WERKNEMER/CONSULTANT

- Nood aan een functieomschrijving die eveneens gereflecteerd wordt in de arbeidsovereenkomst die de kandidaat dient te handtekenen
- Disciplinaire procedure die voorziet dat personeel en andere belanghebbende die zich schuldig hebben maken aan een schending van de arbeidsovereenkomst teruggeroepen kunnen worden
- Het arbeidscontract is voorzien van een vertrouwelijkheids- of een geheimhoudingsovereenkomst
- Richtlijnen die gerespecteerd dienen te worden wanneer gewerkt wordt van op afstand (zie supra – Policy telewerk)
- Bij het vaststellen van een incident of inbreuk persoonsgegevens door de werknemer dient dit gemeld te worden aan de dienst SD ICT en/of DPO. (zie supra – Policy incident respons)

## SENSIBILISERING EN AWARENESS ROND GEGEVENSBESCHERMING EN INFORMATIEBEVEILIGING

- Vandaag wordt er sporadisch een mail met betrekking tot cyberawareness uitgestuurd. Het gaat meestal over de gevaren met betrekking tot phishing. Momenteel is er geen pro-actief cybersecurity awareness programma voor de werknemers
- Sensibilisering rond het gebruik van MFA en de O365 applicaties
- Richtlijnen opgesteld die teruggevonden kunnen worden op het intranet over hoe om te gaan met verdachte emails

## 7.3. GEPLANDE OF BESTAANDE MAATREGELEN FYSIEKE VEILIGHEIDSMAATREGELEN

### WERKSTATIONS BEHEREN

De FOD Justitie werkstations worden beheerd door de interne IT dienst (SD ICT) van de FOD Justitie.

- De werkstations beheerd door SD ICT dienen te voldoen aan de huidige stand van techniek, en zijn allemaal voorzien van een Windows 11 licentie
- De werkstations beheerd door SD ICT zijn voorzien van bitlocker
- Consultant met eigen PC binnen CBE dient een risk exemption questionnaire voor te leggen alvorens te connecteren met het interne netwerk. Deze exemption questionnaire geeft een momentopname weer of het werkstation beheerd door de externe wel voldoet aan dezelfde normen als deze beheerd door FOD Justitie.
- De voedingskabels en kabels voor de werkstations zijn afgeschermd en geplaatst in kabelgoten om schade of compromittering te voorkomen.

### BACKUP

Niet van toepassing, enkel de logging van de aanvragen worden geregistreerd en opgeslagen in de IAM, RA module.

### ONDERHOUD

Regelmatige software updates worden doorgepushed naar de interne medewerkers die gebruik maken van een FOD Justitie-werkstation.

- De CA is verantwoordelijk voor de software updates van de webapplicatie.
- SD ICT is verantwoordelijk voor de software updates van de beheerde werkstations
- Consultant met eigen PC binnen CBE dient een risk exemption questionary voor te leggen alvorens te connecteren op het interne netwerk

### NETWERK VEILIGHEID

Het netwerk wordt beheerd door de verschillende ICT partners waar er SLA’s zijn mee afgesproken.

### FYSIEKE TOEGANGSCONTROLE

Alle gebouwen zijn voorzien van toegangscontrole.

- Badge op naam voor iedere medewerker

- Bezoekersregistratie met voorlegging van identiteitskaart en vermelding van contactpersoon die de bezoeker dient op te halen alvorens deze de gebouwen kan betreden.
- CCTV voorzien aan de verschillende gebouwen en geplaatst volgens de voorschriften van de camerawetgeving.

### NETWERKACTIVITEIT CONTROLEREN

- Monitoring en logging van de netwerkactiviteit is een standaardpraktijk, die centraal beheerd wordt door de dienst SD ICT.

## 7.4. GEPLANDE OF BESTAANDE MAATREGELEN TECHNISCHE VEILIGHEIDSMAATREGELEN

### ENCRYPTIE EN PSEUDONIMISERING

Voor de Security as a service wordt er gerekend op Proximus die via een VPN verbinding ervoor zorgt dat de gegevens versleuteld worden tijdens de verzending.

Alle gegevensstromen tussen de verschillende applicaties zijn versleuteld.

### AUTHENTICATIE EN TRACEERBAARHEID

Er is logging en monitoring voorzien door de verschillende ICT Partners.

- Be-Ys is een vertrouwensdienst die erkend is om een certificaat uit te geven en voldoet aan de wettelijke voorschriften van de eIDAS verordening. Logging en monitoring van de diensten zijn een vereiste om gecertificeerd te worden.
- Proximus en Microsoft zijn beide ISO27000-gecertificeerd, waarbij monitoring en logging eveneens een vereiste is.
- Iedere gebruiker van de toepassing dient gebruik te maken van zijn FOD Justitie emailadres om een aanvraag tot het verkrijgen van een certificaat te lanceren. Tijdens het proces dient de kandidaat-subscriber zich te authenticeren (identity proofing) via het FAS (CSAM platform) waarbij de kandidaat zowel zijn eigen gegevens die zullen gebruikt worden in het certificaat als via het FAS met zijn rijksregisternummer valideert en bevestigd.

### WERKSTATIONS BEHEREN

De FOD Justitie-werkstations worden beheerd door de interne IT dienst van de FOD Justitie.

- Het werkstation is slechts toegankelijk na login op naam en met eigen paswoord
- Iedere betrokkene werkt met multi-factor authenticatie alvorens ze toegang kunnen verschaffen tot het Justitie netwerk
- Automatische screen lock na periode van inactiviteit

## WACHTWOORDEN

Alle wachtwoorden maken gebruik van MFA. De wachtwoorden hebben voorwaarden opgelegd zoals een minimum lengte, gebruik van hoofd- en kleine letters en speciale tekens. Maandelijks wordt de medewerker gedwongen zijn wachtwoord te bevestigen door middel van het gebruik van MFA.

# 8. RISICOBEHEERSING

## 8.1. METHODOLOGIE VAN DE RISICOANALYSE

*Benoem op welke manier men tot risico's komt: gebruikt men een bepaalde norm (ISO27001), heeft men een brainstorm sessie gedaan, is er een bepaalde lijst met risico's, ...*

*Risico's zullen vervolgens ook een score moeten krijgen, benoem de wijze waarop men tot een score komt. De score moet objectief vast te stellen zijn zodat resultaten reproduceerbaar zijn.*

De lijst met risico's kwam tot stand na een brainstorm met de betrokken partijen en met ondersteuning van de PIA-tool.

*Risico = Impact x Likelihood*

***Impact:*** *hoeveel schade kan er plaatsvinden?*

***Likelihood****: kans op fouten*

| | ***Impact*** | ***Likelihood*** | ***Score*** |
|---|---|---|---|
| *Verwaarloosbaar* | *Geen of verwaarloosbare gevolgen*[7] | *Zelden, weinig waarschijnlijk*[8] | *1* |
| *Beperkt* | *Hinder kan overwonnen worden zonder ernstige moeilijkheden*[9] | *Occasioneel, moeilijk te materialiseren*[10] | *2* |
| *Belangrijk* | *Hinder kan overwonnen worden mits ernstige moeilijkheden*[11] | *Mogelijk: is eerder gebeurd en kan nog voorkomen*[12] | *3* |
| *Maximaal* | *Significante of onomkeerbare gevolgen*[13] | *Reëel en waarschijnlijk, regelmatig*[14] | *4* |

[7] Verwaarloosbaar = Laag: Betrokkenen kunnen enkele kleine ongemakken tegenkomen, die ze zonder problemen zullen overwinnen (tijd besteed aan het opnieuw invoeren van informatie, ergernissen, irritaties, etc.).

[8] Verwaarloosbaar = Onwaarschijnlijk: De bedreiging komt alleen in bepaalde omstandigheden voor (vb. afhankelijk van willekeur)

[9] Beperkt = Medium: Betrokkenen kunnen aanzienlijke ongemakken ondervinden, die ze ondanks enkele moeilijkheden kunnen overwinnen (extra kosten, weigering van toegang tot zakelijke diensten, angst, onbegrip, stress, kleine lichamelijke aandoeningen, enz.).

[10] Beperkt = Waarschijnlijk: De bedreiging kan op een bepaald moment gebeuren (vb. afhankelijk van de intentie van de individuele begunstigde)

[11] Belangrijk = Hoog: Betrokkenen kunnen aanzienlijke gevolgen ondervinden, die zij zouden moeten kunnen overwinnen, hoewel met ernstige moeilijkheden (verduistering van fondsen, zwarte lijst door financiële instellingen, materiële schade, verlies van werk, dagvaarding, verslechtering van de gezondheid, enz.).

[12] Belangrijk = Zeer waarschijnlijk: De bedreiging zal ooit op een bepaald moment gebeuren (vb. instanties zoals overheid, commerciële organisatie, criminele organisatie kunnen dit overwegen uit eigenbelang)

[13] Maximaal = Zeer hoog: Betrokkenen die aanzienlijke of zelfs onomkeerbare gevolgen kunnen ondervinden, die ze mogelijk niet verhelpen (arbeidsongeschiktheid, langdurige psychische of lichamelijke aandoeningen, overlijden, enz.).

[14] Maximaal = Onvermijdbaar: De bedreiging is onafwendbaar

## 8.2. RISICO-IDENTIFICATIE: NATUURLIJKE BEDREIGINGEN

Natuurlijke bedreigingen: overstroming, brand, aardbeving, extreme koude, waardoor de RA module niet beschikbaar is voor de RA office en aanvragen/wijzigingen niet kunnen worden gevalideerd.

### IMPACT EN LIKELIHOOD

Natuurlijke bedreigingen hebben een impact op de **beschikbaarheid** van de gegevens.

De impact is maximaal (4), de kans is echter verwaarloosbaar (1) dat de applicatie geïmpacteerd wordt door een natuurlijke bedreiging.

### MITIGATIE VAN HET RISICO

De RA applicatie is een cloud applicatie, die enerzijds gegevens valideert uit andere FOD applicaties, en daarna doorstuurt naar de Registration authorithy die op zijn beurt de goedkeuringsgegevens registreert alvorens het certificaat te generen en bij te houden. De samenwerking met de andere actoren zoals supra besproken, werden contractueel afgedekt, waarbij SLA's afgesproken zijn.

### BESTAANDE TOM

- SLA-contracten zijn opgesteld tussen de verschillende partijen om continuïteit te garanderen.
- Draft policy om business continuïteit te garanderen

## 8.3. RISICO-IDENTIFICATIE: TECHNISCH FALEN

Het falen van de hardware of software waardoor de RA module niet beschikbaar is voor de RA office en aanvragen/wijzigingen niet kunnen worden gevalideerd.

### IMPACT EN LIKELIHOOD

Technisch falen hebben een impact op de **beschikbaarheid** van de gegevens.

De impact is groot (4), de kans is echter klein (1) dat de applicatie geïmpacteerd wordt door een technisch falen.

### MITIGATIE VAN HET RISICO

Bij technisch falen van hardware is het steeds mogelijk om via een andere computer in te loggen met de eigen credentials in de RA module.

Het technisch falen met betrekking tot eigen hardware kan voorkomen worden door het gebruik van asset management. Dit zorgt ervoor dat hardware na een bepaalde levenscyclus wordt vervangen.

De gebruikte hardware door de RA office is voorzien van de laatste OS updates, een goede virusscanner en heeft bitlocker geactiveerd.

Software aangeleverd door andere partijen hebben contractuele afspraken opgenomen in de service agreements.

### BESTAANDE TOM

Organisatorisch is er vooral nood aan een beleid dat ook uitgeschreven staat in overkoepelende policies :

- Draft policy rond fysiek asset beheer binnen SD ICT
- Risk exemption questionary invullen als externe partij

## 8.4. RISICO-IDENTIFICATIE: SERVICES VOORZIEN DOOR DERDE PARTIJEN

- Onvolledig of incorrect gebruik van de wettelijke bepalingen die noodzakelijk zijn om te spreken van een contract, vb. de toepasbare wetgeving, de bevoegde jurisdictie, …
- Geen vertrouwelijkheidsclausule of andere confidentialiteitsbepaling in de contracten met het personeel, freelancers en/of consultants.
- Voorleggen van een certificaat die aantoont dat men voldoet aan de beveiliging zoals noodzakelijk voor de huidige stand van de techniek.
- Door een verwerkingsactiviteit uit te besteden aan andere partijen zijn er verschillende risico's die in acht moeten genomen worden met betrekking tot gegevensbescherming. De elementen dienen opgenomen te worden in een rechtshandeling (addendum bestaand contract of verwerkersovereenkomst) De kans bestaat erin dat er niet langer:
    - Controle is over het beheer van de eigen data binnen de applicaties.
    - Gegevensbeschermingsrisico's omdat de verwerker niet voldoet aan de wettelijke voorschriften dat deze verordening met zich meebrengt
    - Onveilige verwijdering van de data
    - Subverwerkers die gekozen worden door de verwerker die zich buiten de EU bevinden, en waar geen adequaatheidsbesluit voor bestaat
    - Gebruik van de verzamelde data voor andere doeleinden dan contractueel afgesproken
    - Geen tot weinig ondersteuning bij incidenten
    - Geen tot weinig ondersteuning wanneer betrokkene zijn rechten uitoefent.

### IMPACT EN LIKELIHOOD

Risico's verbonden aan de samenwerking met andere partijen hebben een impact op **betrouwbaarheid**, **integriteit** en de **beschikbaarheid** van de data.

De impact is hoog, en de kans is hoog.

### MITIGATIE VAN HET RISICO

- Het opstellen van een gegevensbeschermingseffectenbeoordeling om ervoor te zorgen dat de verwerkingsverantwoordelijke bewust is van de risico's die de samenwerking met verschillende partijen met zich meebrengt is belangrijk om de juiste contractuele afspraken te maken.
- Contractuele afspraken met betrekking tot aansprakelijkheid, gegevensbescherming en SLA's zijn noodzakelijk om bovenstaande risico's te reduceren.

- Tenslotte kan bij de keuze van de samenwerkende actoren geëist worden dat ze een certificaten/normen behaald hebben waarbij gegarandeerd wordt dat de huidige beveiligingsnorm behaald is. Voorbeelden van ISO normen die garanderen dat de beveiliging van de Cloudapplicaties gegarandeerd zijn ISO27000, ISO27701 en een ISO27018 .

## BESTAANDE TOM

- Richtlijnen bij de opstart van ieder project waarbij gevraagd wordt om na te gaan of de samenwerkende actoren beschikken over contractuele afspraken en/of (aanvullende) verwerkersovereenkomst. Indien niet, dan wordt de template van Justitie aangeboden om deze in te vullen.
- Aanstellen van een functionaris gegevensbescherming (DPO)
- Contractuele afspraken tussen de verschillende partijen inclusief de details van de vooropgestelde verwerkingsactiviteiten
- Voorleggen van een audit rapport met betrekking tot de security of het voorleggen van een certificaat cf. ISO27000.
- Audit initiëren bij de verwerkers

## 8.5. RISICO-IDENTIFICATIE: SYSTEM ERRORS

Risico's gelinkt aan system errors die een impact hebben op de betrouwbaarheid, de integriteit en de beschikbaarheid van de gegevens.

- Incorrecte installatie van de software bij de opzet van de systemen waardoor de applicatie niet of minder performant werkt
- Incorrecte netwerkconfiguratie waardoor de applicatie niet of beperkt beschikbaar is
- Incorrecte configuratie van de monitoring en logging waardoor er geen audit trail beschikbaar is
- Software vulnerabilities die niet opgevolgd of gefixed worden, waardoor de applicatie beschikbaar wordt voor hackers die de vulnerability willen exploiten.

Risico's gelinkt aan system errors die een impact hebben op de integriteit van de gegevens.

- Fouten in de logdata geven een incorrecte audit trail.
- Fouten in de procedurele stappen die door het systeem moet doorlopen worden alvorens het certificaat wordt toegewezen. (sequence error)

### IMPACT EN LIKELIHOOD

System errors zoals gedefinieerd hebben een impact op de **beschikbaarheid**, de **betrouwbaarheid** en de **integriteit** van de gegevens.

De impact is hoog, en de kans is midden.

### MITIGATIE VAN HET RISICO

Deze risico's kunnen gemitigeerd worden door een goede governance die neergeschreven staan in policies en procedures om dit te voorkomen.

Wanneer samengewerkt wordt met externe partijen kan het voorleggen van een certificaat of audit rapport met betrekking tot security van de systemen een voorwaarde zijn alvorens de samenwerking te starten.

Pentesting en audits opleggen, zowel intern als bij de verwerker(s).

### BESTAANDE TOM

- Aanstellen van een CISO
- Draft policies in opmaak

## 8.6. RISICO-IDENTIFICATIE: DATA KWALITEIT

- Incorrecte informatie gedocumenteerd in de andere systemen waar de RA office zij voor nodig heeft (AD extract en Persopoint)

### IMPACT EN LIKELIHOOD

Incorrecte data in de IAM RA module zorgt voor een compromittering van de **betrouwbaarheid** van de data.

De impact is hoog, en de kans is midden.

### MITIGATIE VAN HET RISICO

Bij de aanvraag zijn er verschillende controlepunten van de gegevens:

- Eerste controle door de RA officer in de database van PersoPoint en AD Extract alvorens de vraag door te sturen naar de hiërarchische overste.
- De hiërarchische overste controleert de lijst van namen die de aanvraag lanceerden van een certificaat.
- Tenslotte zal de aanvrager zelf zijn gegevens valideren en authenticeren alvorens de RA officer de aanvraag doorgeeft aan de CA.
- Wanneer data incorrect genoteerd staat in PersoPoint of AD Extract, dan heeft de RA officer de mogelijkheid om de data aan te passen binnen de IAM, RA module opdat alle gegevens noodzakelijk om een certificaat uit te reiken correct zijn. Deze worden vervolgens door de aanvrager gevalideerd en geconfirmeerd via FAS. Het gaat specifiek over de aanpassing van de locatie en de afdeling/functie van de kandidaat.

### BESTAANDE TOM

- Policy met betrekking tot rollenbeheer in ontwerpface

## 8.7. RISICO-IDENTIFICATIE: USR ERRORS

- Ingeven van incorrecte informatie in de RA module van IAM
- Verwijderen van gegevens in de RA module van IAM
- Wijzigen van de gegevens in de RA module van IAM
- Lijst van namen voor toegang niet voldoende controleren door de verantwoordelijke van de aanvrager, waardoor een persoon toegang al dan niet wordt toegewezen

### IMPACT EN LIKELIHOOD

Incorrecte data door user errors in de IAM RA module zorgt voor een compromittering van de **betrouwbaarheid** van de data.

De impact is hoog, en de kans is midden.

### MITIGATIE VAN HET RISICO

- Lijst wordt aangeleverd door de vragende partij
- Validatie bestaan van de kandidaat in de systemen PersoPoint en AD Extract
- Bij akkoord
    - Controle van de toegewezen profielen door hiërarchische overste
    - Controle door de kandidaat zelf van de gegevens
    - Derde bevestiging van de RA om het proces te valideren om de aanmaak door te sturen
- Training van de RA officers

### BESTAANDE TOM

- Training met betrekking tot de opzet is gestart, certificaat van deelname wordt uitgereikt na het volgen van de sessies.

## 8.8. RISICO-IDENTIFICATIE: INFORMATICACRIMINALITEIT IN STRIKTE ZIN

- Manipulatie van de logging om eigen sporen uit te wissen
- Tampering met de software waardoor de applicatie niet meer toegankelijk is
- Denial of service waardoor de beschikbaarheid van de applicatie weg is
- Ransomware die het systeem versleuteld
- …

### IMPACT EN LIKELIHOOD

Vormen van informaticacriminaliteit in strikte zin zoals hacking, informaticasabotage, informaticabedrog en valsheid in informatica hebben een impact op **betrouwbaarheid**, **integriteit** en de **beschikbaarheid** van de data.

De impact is hoog, en de kans is klein.

### MITIGATIE VAN HET RISICO

- Awareness en sensibilisering
- Policies en procedures
- Uitvoeren van software updates
- Firewall
- Antivirus
- Functie en rollenbeheer van de RA officers

### BESTAANDE TOM

- Samenwerking met ISO27000-gecertificeerde instellingen
- Samenwerking met een trusted provider
- Samenwerking met een datacenter
- Contractuele afspraken en SLA’s om de business continuïteit te garanderen
- Asset management policy & procedures (fysiek & technisch)
- Maatregelen rond netwerkveiligheid
- Encryptie en pseudonymisering
- Authenticatie, logging & monitoring
  Multifactorauthenticatie

## 8.9. RISICO-IDENTIFICATIE: INFORMATICACRIMINALITEIT IN RUIME ZIN SOCIAL ENGINEERING

Misbruik maken van de goede intenties van de RA officer om er voor te zorgen dat een certificaat toegewezen wordt aan iemand die hier niet toe gerechtigd is.

- Phishing/smishing attack
- Spoofing attack

### IMPACT EN LIKELIHOOD

Informaticacriminaliteit in ruime zin zorgen voor een impact op **betrouwbaarheid**, **integriteit** en de **beschikbaarheid** van de data.

De impact is hoog, en de kans is klein.

### MITIGATIE VAN HET RISICO

De verschillende controle stappen zowel van de hiërarchische overste als van de kandidaat zorgen ervoor dat de kans is dat iemand een certificaat toegewezen krijgt die hier niet toe gemachtigd is.

### BESTAANDE TOM

- Goedkeuringsproces van de kandidaat
- Versleutelde verbinding
- Maatregelen rond netwerkveiligheid
- Authenticatie, logging & monitoring
- Multifactorauthenticatie

## 8.10. RISICO-IDENTIFICATIE: UNAUTHORISED ACCESS

- Ongeoorloofde toegang tot de applicatie verschaffen
- Identity theft

### IMPACT EN LIKELIHOOD

Informaticacriminaliteit in ruime zin zorgen voor een impact op **betrouwbaarheid**, **integriteit** en de **beschikbaarheid** van de data.

De impact is hoog, en de kans is klein.

### MITIGATIE VAN HET RISICO

De verschillende controle stappen zowel van de hiërarchische overste als van de kandidaat zorgen ervoor dat de kans is dat iemand een certificaat toegewezen krijgt die hier niet toe gemachtigd is.

### BESTAANDE TOM

- Goedkeuringsproces van de kandidaat
- Disciplinaire procedure
- Functieomschrijving personeel (in draft)
- Arbeidscontract
- Sensibilisering & awareness
- Maatregelen rond netwerkveiligheid
- Encryptie en pseudonymisering
- Authenticatie, logging & monitoring
- Multifactorauthenticatie

## 8.11. RISICO-IDENTIFICATIE: PERSONEEL/MEDEWERKERS

- Incorrecte of onvoldoende screening van het personeel
- Geen duidelijke functieomschrijvingen en afbakening van de taken binnen het team
- Geen organogram
- Tekort aan personeel of veel verschuivingen binnen het team

### IMPACT EN LIKELIHOOD

Het aanwerven van de verkeerde persoon voor een taak heeft een impact op **betrouwbaarheid**, **integriteit** en de **beschikbaarheid** van de data.

De impact is midden, en de kans is midden.

### MITIGATIE VAN HET RISICO

- Duidelijke missie en visie van FOD Justitie kaderen bij de aanwerving zodat de verwachtingen bij de kandidaat duidelijk zijn
- Duidelijke functie omschrijvingen van de verschillende actoren binnen het team
- Draaiboek van de verwachtte werkwijze
- Organogram voorzien zodat de organisatiestructuur voor iedereen duidelijk is bij escalatie

### BESTAANDE TOM

- Screeningsprocedure
- Bepalingen in het arbeidscontract
- Disciplinaire procedure
- Functieomschrijving personeel (in draft)
- Sensibilisering & awareness
- Maatregelen rond netwerkveiligheid
- Encryptie en pseudonymisering
- Authenticatie, logging & monitoring
- Multifactorauthenticatie

## 8.12. RISICO-IDENTIFICATIE: SCHENDING RECHTEN VAN DE BETROKKENE

- De verzamelde persoonsgegevens worden verwerkt voor een andere doel dan vermeld in de privacy statement
- De verzamelde persoonsgegevens worden langer bewaard dan nodig voor het beoogde doel
- De verzamelde persoonsgegevens worden verwerkt zonder een rechtmatige rechtsgrond
- FOD justitie kan niet tegemoet komen aan de vraag van de betrokkene die zijn rechten wenst uit te oefenen
- Het niet bestaan van een verwerkingsregister
- Geen incident response plan wanneer een inbreuk persoonsgegevens zou plaatsvinden
- Geen gegevensbeschermingseffectenbeoordeling opgesteld om de risico's in kaart te brengen
- Geen verwerkersovereenkomsten of een rechtshandeling die alle essentiële elementen bevat noodzakelijk om te voldoen aan de wettelijke voorschriften in de AVG.

### IMPACT EN LIKELIHOOD

De schending van de rechten van de betrokkene heeft een impact op **betrouwbaarheid** en de **beschikbaarheid** van de data.

De impact is groot, en de kans is klein.

### MITIGATIE VAN HET RISICO

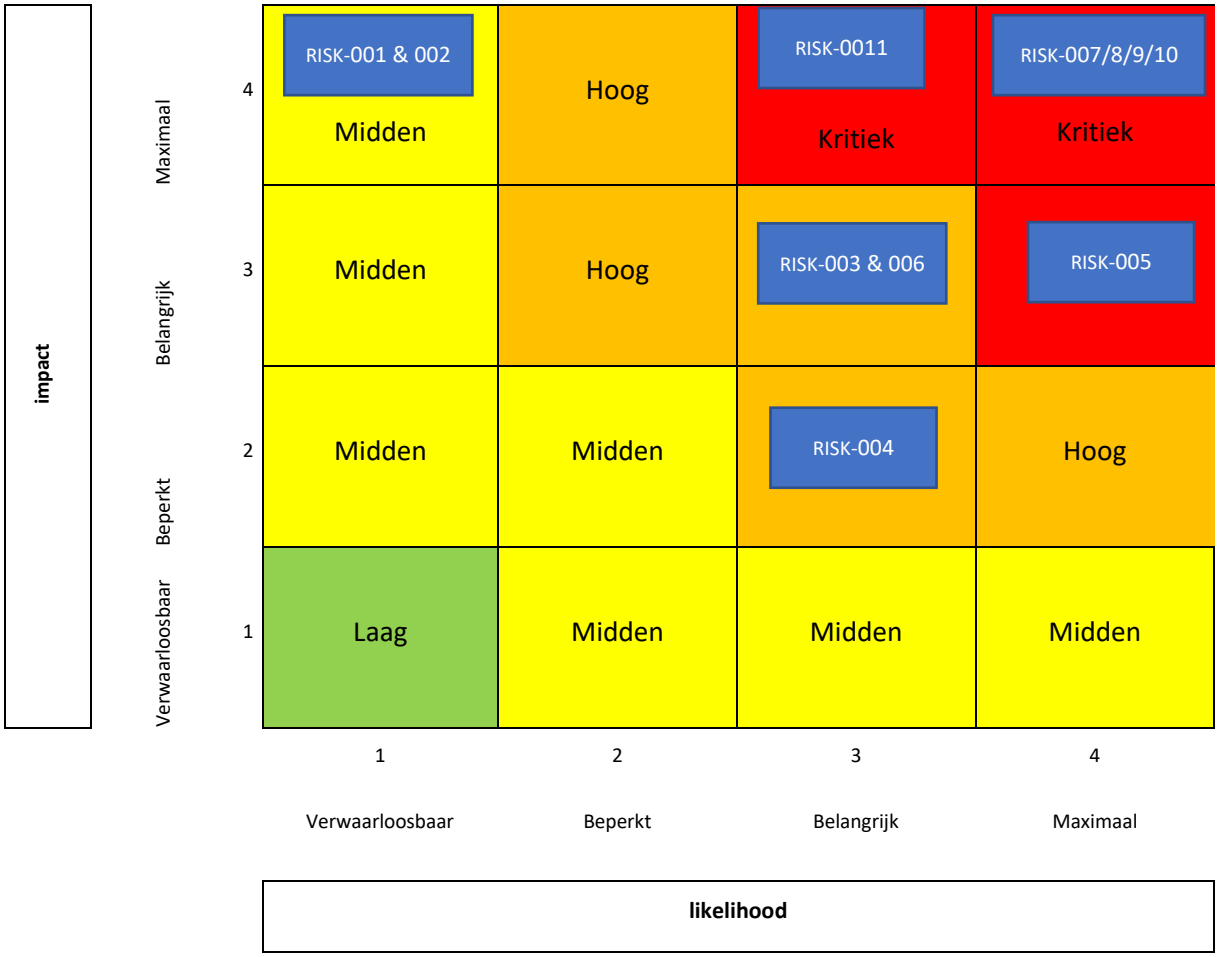
- Aanstellen van een functionaris gegevensbescherming (DPO)
- Awareness en sensibilisering van het personeel met betrekking tot gegevensbescherming
- Opstellen van een transparantieverklaring
- Mogelijkheid tot uitoefening van de rechten van betrokkene
- Mogelijkheid tot het indienen van een bezwaar bij de toezichthoudende autoriteit
- Opstellen van een gegevenseffectenbeschermingsbeoordeling (DPIA)
- Opstellen van een verwerkersovereenkomst met de verwerkers binnen dit proces
- Opstellen van een procedure inbreuk persoonsgegevens
- Uitwerken proces om tegemoet te komen aan de rechten van betrokken binnen de termijn van 1m

### BESTAANDE TOM

- Aanstellen van een functionaris gegevensbescherming (DPO)
- Opstellen van een DPIA

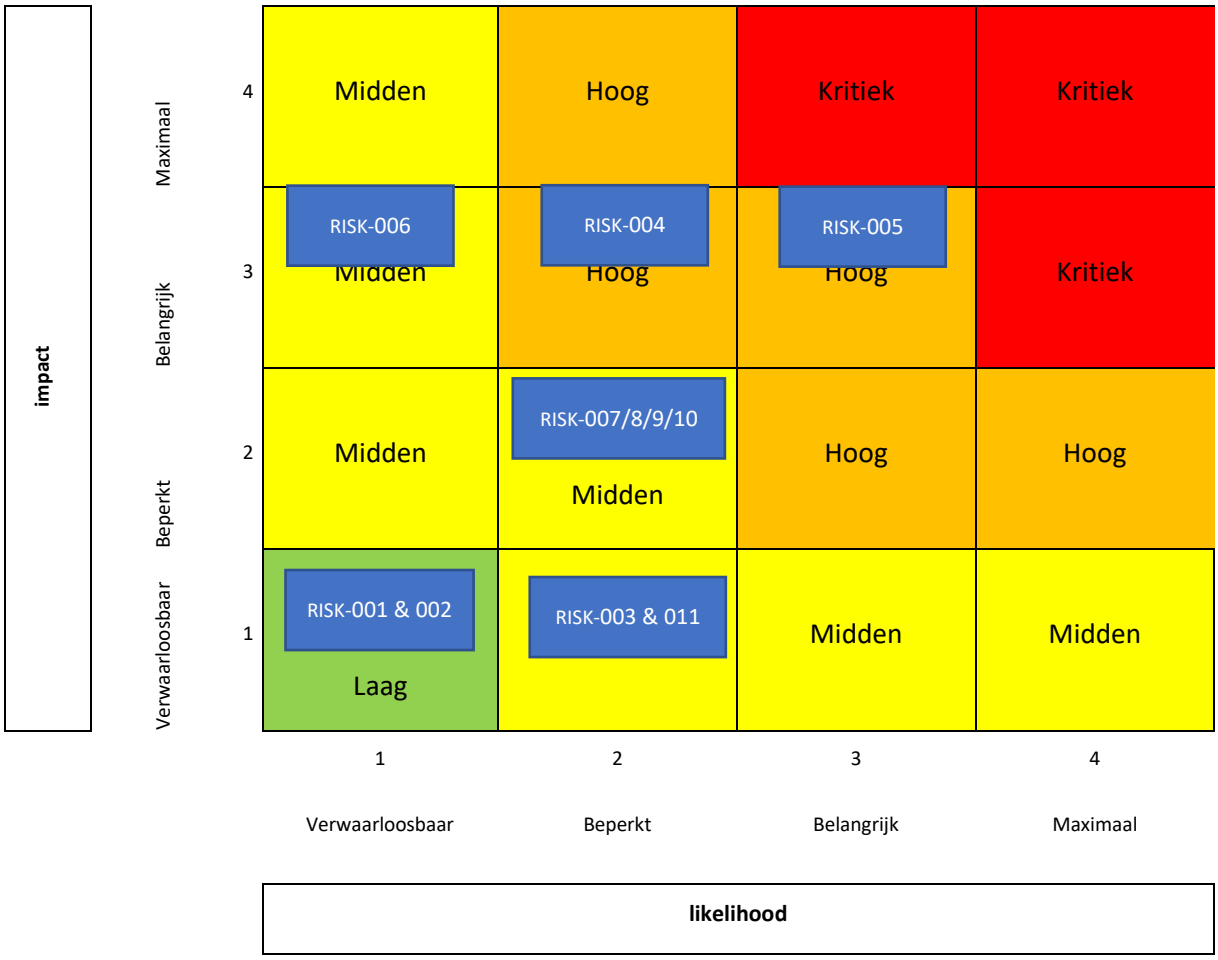
## 8.13. EVALUATIE VAN DE RISICO'S

| *NR* | *OMSCHRIJVING* | *RISICO (IxL)* | *ERNST* |
|---|---|---|---|
| *RISK-001* | *Natuurlijke bedreiging* | *4x1 = 4* | *Midden* |
| *RISK-002* | *Technisch Falen* | *4x1 = 4* | *Midden* |
| *RISK-003* | *Services voorzien door derde partijen* | *3x3 = 9* | *Hoog* |
| *RISK-004* | *System errors* | *3x2 = 6* | *Hoog* |
| *RISK-005* | *Data kwaliteit* | *3x4 = 12* | *Kritiek* |
| *RISK-006* | *User errors* | *3x3 = 9* | *Hoog* |
| *RISK-007* | *Hacking en informaticasabotage* | *4x4 = 16* | *Kritiek* |
| *RISK-008* | *Social engineering* | *4x4 = 16* | *Kritiek* |
| *RISK-009* | *Unauthorised access* | *4x4 = 16* | *Kritiek* |
| *RISK-010* | *Personeel* | *4x4 = 16* | *Kritiek* |
| *RISK-011* | *Schending rechten van betrokkene* | *4x3 = 12* | *Kritiek* |


impact
Maximaal
Belangrijk
Beperkt
Verwaarloosbaar
4
3
2
1
RISK-001 & 002
Midden
Hoog
RISK-0011
Kritiek
RISK-007/8/9/10
Kritiek
Midden
Hoog
RISK-003 & 006
RISK-005
Midden
Midden
RISK-004
Hoog
Laag
Midden
Midden
Midden
1
2
3
4
Verwaarloosbaar
Beperkt
Belangrijk
Maximaal
likelihood

# 9. RESIDUELE RISICO'S (RR)

| NR | OMSCHRIJVING | ERNST | Risicobep erkende maatregel (en) | RR |
|---|---|---|---|---|
| *RISK-001* | *Natuurlijke bedreiging* | *Midden* | *8.2* | *Laag* |
| *RISK-002* | *Technisch Falen* | *Midden* | *8.3* | *Laag* |
| *RISK-003* | *Services voorzien door derde partijen* | *Hoog* | *8.4* | *Midden* |
| *RISK-004* | *System errors* | *Hoog* | *8.5* | *Hoog* |
| *RISK-005* | *Data kwaliteit* | *Kritiek* | *8.6* | *Hoog* |
| *RISK-006* | *User errors* | *Hoog* | *8.7* | *Midden* |
| *RISK-007* | *Hacking en informaticasabotage* | *Kritiek* | *8.8* | *Midden* |
| *RISK-008* | *Social engineering* | *Kritiek* | *8.9* | *Midden* |
| *RISK-009* | *Unauthorised access* | *Kritiek* | *8.10* | *Midden* |
| *RISK-010* | *Personeel* | *Kritiek* | *8.11* | *Midden* |


impact
Maximaal
Belangrijk
Beperkt
Verwaarloosbaar
4
3
2
1
Midden
Hoog
Kritiek
Kritiek
RISK-006
Midden
RISK-004
Hoog
RISK-005
Hoog
Kritiek
Midden
RISK-007/8/9/10
Midden
Hoog
Hoog
RISK-001 & 002
Laag
RISK-003 & 011
Midden
Midden
1
2
3
4
Verwaarloosbaar
Beperkt
Belangrijk
Maximaal
likelihood

## 9.1. AANDACHTSPUNTEN TEN AANZIEN VAN DE ORGANISATORISCHE MAATREGELEN

De organisatorische maatregelen moeten voldoen aan art. 32 AVG waarbij tegemoet gekomen wordt aan de huidige stand van de techniek, rekening houden met de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

- Verdere nood aan het uitschrijven van policies en uniforme procedures om tegemoet te komen aan de wettelijke vereisten van de AVG, en deze ook uitrollen binnen de FOD zodat iedereen ervan op de hoogte is.
- Uitschrijven van een transparantieverklaring.
- De uitrol van het IAM project met betrekking tot de 2 externe databases die de RA module voeden voor de toekenning van het certificaat zou minstens in testfase moeten zijn alvorens de RA office operationeel wordt.

## 9.2. AANDACHTSPUNTEN TEN AANZIEN VAN DE MENSGERICHTE MAATREGELEN

De mensgerichte maatregelen moeten voldoen aan art. 32 AVG waarbij tegemoet gekomen wordt aan de huidige stand van de techniek, rekening houden met de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

- Eerder nood aan een actieve aanpak om de awareness bij het personeel te verhogen rond informatiebeveiliging en de kernprincipes van gegevensbescherming.
- Het incidentresponsbeleid met betrekking tot de inbreuk persoonsgegevens is onvoldoende gekend onder het personeel. Hierdoor zijn er te weinig interne meldingen.
- Nood aan sensibilisering en awareness rond zowel gegevensbescherming als informatiebeveiliging. Momenteel wordt sporadisch een mail doorgestuurd met een boodschap rond informatiebeveiliging, echter wordt het niet afgedwongen.

## 9.3. AANDACHTSPUNTEN TEN AANZIEN VAN DE FYSIEKE MAATREGELEN

De fysieke maatregelen moeten voldoen aan art. 32 AVG waarbij tegemoet gekomen wordt aan de huidige stand van de techniek, rekening houden met de uitvoeringskosten, alsook met de aard, de

omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

- Operationele policies en procedures noodzakelijk om de opvolging van de geïmplementeerde maatregelen op te volgen.

## 9.4. AANDACHTSPUNTEN TEN AANZIEN VAN DE TECHNISCHE MAATREGELEN

De technische maatregelen moeten voldoen aan art. 32 AVG waarbij tegemoet gekomen wordt aan de huidige stand van de techniek, rekening houden met de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

- De implementatie van het *Clean and Clear Desk*-principe om te voorkomen dat er informatie wordt gecapteerd door onbevoegden
- Er is geen gestandaardiseerd proces om mensen te on- of offboarden vandaag. Hierdoor blijven accounts te lang actief of incorrect binnen de systemen.

# 10. EVALUATIE DATA PROTECTION OFFICER

## 10.1. VASTSTELLING VAN DE CONTROLES

| Controle | JA = Aanvaarbaar<br>NEEN = Te verbeteren | Corrigerende maatregelen |
|---|---|---|
| DPIA leesbaar en correct ingevuld? | *JA* | |
| Doelen: specifiek, uitdrukkelijk, te rechtvaardigen | *JA* | |
| Rechtvaardigheidsgrond | *JA* | |
| Noodzakelijkheid en evenredigheid? | *JA* | |
| Data minimalisatie | *JA* | |
| Data kwaliteit | *JA* | |
| Verantwoorde bewaartermijn | *JA* | |
| Rechten betrokkene gevrijwaard? | - | *Transparantieverklaring noodzakelijk*<br>*Emailadres is voorzien, echter is het een algemeen emailadres waardoor de wettelijke termijn om te antwoorden op de vragen van de betrokkene in het gedrang kan komen. Nood aan een privacy_RA mailadres* |
| Verwerkersovereenkomst met de verwerkers? | - | *Verwerkersovereenkomsten niet ontvangen van de ondersteunende ICT partners* |
| Gegevensbescherming voldoende bij transfer buiten EER? | *JA* | *Private key in bezit van de FOD Justitie*<br>*Adequaatheidsbesluiten voor de US partners* |
| Voldoende organisatorische beveiligingsmaatregelen? | *Aanvaardbaar* | *Nood aan de policies en procedures, echter zijn ze in de aanmaak* |
| Voldoende mensgerichte beveiligingsmaatregelen | *JA* | |

| | | |
|---|---|---|
| Voldoende fysieke beveiligingsmaatregelen? | *JA* | |
| Voldoende technische beveiligingsmaatregelen? | - | *Het IAM project blijft vaag, waardoor er geen duidelijke functie en rollenbeheer is van de verschillende actoren binnen justitie.* |

### 10.2. ADVIES DPO

Op basis van de procesbeschrijving met de verscheidene elementen uit de DPIA, de uitgevoerde risico-analyse en de vaststelling van de controles, stelt de DPO vast dat een voorafgaande raadpleging van de gegevensbeschermingsautoriteit ~~wel~~ / **niet** nodig is.

## 11. BESLISSING ROND VOORAFGAANDE RAADPLEGING DPIA

*Afhankelijk van de restrisico's uit 7, wordt hier vastgelegd of men uiteindelijk wel, of niet, zal overgaan tot een voorafgaande raadpleging. Met andere woorden, of de lokale data protection authority moet worden gecontacteerd om advies te vragen over de verwerking omdat de restrisico's (mogelijk) te hoog zijn.*

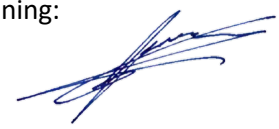
Deze beslissing komt er na advies van de DPO op 12/08/2023

### Ondertekening van de vertegenwoordiger:

Naam: Vincent Flore

Datum: 13/09/2023

Handtekening:



## 12. HEREVALUATIE

Indien zich:

- Geen wijzigingen van de verwerkingsmiddelen of technische evoluties voordoen;
- Geen ontdekkingen van nieuwe kwetsbaarheden in de beveiliging voordoen, wordt er een herevaluatie van bovenstaande DPIA voorzien d.d. *(datum + 3 jaar).*

## 13. BRONNEN

- GDPR, art. 35 inclusief grond 75, 84, 89, 90, 91, 92, 93
- WP 29, WP 248 rev. 01 d.d. 04.10.2017
- CBPL, Aanbeveling nr. 01/2018 d.d. 28.02.2018
- ISO/IEC 29134
- https://www.cnil.fr/: methodologie ontwikkeld door de CNIL (Commission Nationale Informatique et Libertés)