AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Onderwerp

Samenvatting onderzoek naar de bescherming van persoonsgegevens in Visum Informatiesysteem (VIS)

De Autoriteit Persoonsgegevens (hierna: AP) is aangewezen als nationale toezichthouder op de verwerking van persoonsgegevens in het nationale deel van het Visum Informatiesysteem (hierna: VIS). Vanuit de VIS-verordening dient de nationale toezichthoudende autoriteit (AP voor Nederland) ervoor zorg te dragen dat tenminste om de vier jaar een onderzoek op het nationale systeem wordt verricht.

Vanuit deze verplichting heeft de AP in 2020 door een externe partij een onderzoek laten uitvoeren naar de bescherming van persoonsgegevens in VIS Dit onderzoek is begin 2021 afgerond. Met deze brief informeert de AP u over de achtergrond van het systeem, het onderzoeksproces en de belangrijkste bevindingen van het onderzoek.

Achtergrond

VIS is een databank van visumaanvragen voor Schengenlanden. In het VIS worden alle persoonsgegevens opgeslagen die nodig zijn voor een visum. De lidstaten van de Europese Unie (EU) kunnen deze gegevens via het VIS uitwisselen.

In het VIS worden onder meer de volgende gegevens opgeslagen van degene die een visum aanvraagt:

- identiteitsgegevens;
- reisgegevens;
- foto;
- vingerafdrukken.

In Nederland zijn er verschillende bevoegde autoriteiten in Nederland die gebruik mogen maken van het VIS. De volgende organisaties (hierna: ketenpartners) maken gebruik van het VIS:

- Ministerie van Buitenlandse Zaken;
- Ministerie van Justitie en Veiligheid;
- Immigratie- en Naturalisatiedienst;
- Nationale Politie;
- Koninklijke Marechaussee.

Het nationale deel van het VIS bestaat uit een groot aantal samenhangende systemen, met elk hun eigen technische privacy- en beveiligingsmaatregelen. De systemen zijn eigendom van de hiervoor genoemde vijf ketenpartners, met elk hun eigen maatregelen en procedures. De persoonsgegevens worden (per ketenpartner) verspreid over meerdere systemen verwerkt en uitgewisseld tussen de verschillende systemen.

Proces van het onderzoek

Binnen het uitgevoerde onderzoek zijn systemen en de noodzakelijke of verplichte procedures omtrent deze systemen (zoals bijvoorbeeld toegangsbeheer, incidentmanagement of specifieke procedure ter borging van de rechten van betrokkenen) onderzocht die de ketenpartners hebben getroffen voor de verwerking van de (biometrische) persoonsgegevens in het VIS. Het onderzoek is door een externe partij uitgevoerd, onder verantwoordelijkheid en toezicht van de AP, bij de hiervoor opgesomde ketenpartners die gebruik maken van het VIS.

Voor het onderzoek is een normering opgesteld. Voor deze normering is gebruik gemaakt van vereisten uit de VIS-verordening en het VIS-besluit, aangevuld met vereisten uit de AVG. Daarbij is onderzoek gedaan naar de aspecten informatiebeveiliging en privacy voor de in scope zijn systemen en processen. Deze aspecten zijn vertaald naar te verwachten maatregelen (normen). De normering bestaat uit de volgende onderwerpen:

- Risico en beveiligingsbeleid;
- Beveiligingsplan;
- Informatiebeveiligingsprocessen / -procedures / -maatregelen);
- Service Level Agreements en Rapportage (SLA/SLR);
- Register van verwerkingsactiviteiten;
- Quickscan privacy / DPIA;
- Privacy-processen / -procedures / -maatregelen;
- Verwerkersovereenkomsten;
- Compliance en control.

Per ketenpartner is een onderzoek aan de hand van deze normen uitgevoerd. Per ketenpartner is de normering afgestemd op de in scope zijnde systemen en processen van de organisatie. Een aantal normen heeft betrekking op meerdere van bovenstaande onderwerpen.

Daarbij is onderzoek gedaan naar het ontwerp en de implementatie van beleid, plannen, processen, procedures en maatregelen voor de verwerking van de (biometrische) persoonsgegevens in het VIS door de ketenpartner. Het onderzoek is uitgevoerd door middel van het kennisnemen van documentatie, het houden van interviews, het evalueren van de resultaten van de door de ketenpartners uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden.

Na het evalueren van de resultaten zijn de uitkomsten van het onderzoek verwerkt in een samenvatting per ketenpartner, bestaande uit bevindingen, conclusies en aanbevelingen per norm. Deze samenvatting is afgestemd per ketenpartner waar het onderzoek is uitgevoerd. Na afstemming van de samenvatting zijn de bevindingen per ketenpartner in een rapport samengevat dat aan de AP is opgeleverd.

Uitkomsten van het onderzoek

Bij alle ketenpartners is in totaal naar 84 normen onderzoek gedaan (19 normen x 5 ketenpartners). Per ketenpartner is de normering afgestemd op de in scope zijnde systemen en processen van de organisatie en zijn enige normen niet van toepassing bij de betreffende ketenpartner. Op basis van het onderzoek zijn 30 bevindingen vastgesteld en aan de ketenpartners gerapporteerd.

Samenvattend is op 36% van de normen een aandachtspunt geconstateerd. Van de 30 aandachtspunten zijn er 6 geclassificeerd als ‘voldoet niet’, wat wil zeggen dat op geen van de onderdelen die in de norm zijn opgenomen door de ketenpartner maatregelen of procedures zijn getroffen.

De andere bevindingen (24 van de 30) zijn geclassificeerd als 'voldoet deels', waarbij op één van de onderdelen uit de norm geen procedures of maatregelen zijn getroffen (en op de overige onderdelen uit de norm wel).

De aandachtspunten zijn op de volgende onderwerpen geconstateerd:

Onderwerp	Aantal Aandachts-putnen	Percentage aandachtspunten	Aantal classificatie 'voldoet niet'
Risico- en beveiligingsbeleid	2	40%	-
Beveiligingsplan	2	40%	-
Informatiebeveiligingsprocessen / -procedures / -maatregelen)	5	33%	-
Service Level Agreements en Rapportage (SLA / SLR)	3	75%	-
Register van verwerkingsactiviteiten	2	40%	-
Quickscan privacy / DPIA	4	50%	2
Privacy--processen / -procedures / -maatregelen	8	28%	1
Verwerkersovereenkomsten	1	25%	-
Compliance en control	11	61%	3

Er is binnen deze bevindingen een aantal verschillende ketenoverkoepelende bevindingen geconstateerd, bestaande uit:

- de persoonsgegevens in het VIS (per ketenpartner) worden verspreid over meerdere systemen verwerkt en uitgewisseld tussen verschillende systemen. Er is geadviseerd door middel van een jaarlijks roulerend onderzoek (op onderdelen van) het systeem) uiteindelijk het totale systeem in beeld te brengen;
- de ketenpartners hebben het beheer in veel gevallen uitbesteed aan externe ICT-dienstverleners. Er is geadviseerd onderzoeken naar de (kwaliteit van de) dienstverlening van ICT-dienstverleners uit te voeren.

Ter afsluiting

De AP is met de ketenpartners een verbetertraject gestart waarin de ketenpartners met beleid, processen, procedures en maatregelen (nader) invulling moeten geven aan de bevindingen die tijdens het onderzoek zijn vastgesteld.

De AP heeft op regelmatige basis de status en voortgang in de opvolging bekeken die de ketenpartners aan de aanbevelingen geven. Hiertoe is regelmatig contact geweest met de ketenpartners en zijn de ketenpartners gevraagd om de AP mee te laten kijken naar de aanbevelingen waar zij opvolging aan geven. Op deze manier heeft de AP toezicht gehouden of de aanbevelingen zijn opgevolgd door de ketenpartners. Dit verbetertraject heeft ertoe geleid dat, op 3 aandachtspunten na (bij twee verschillende ketenpartners), de ketenpartners met beleid, processen, procedures en maatregelen de aandachtspunten hebben opgepakt. Voor drie ketenpartners is daarmee dit traject inmiddels afgerond, bij twee ketenpartner is dit nog onderhanden.