AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Minister van Buitenlandse Zaken
De heer mr. W.B. Hoekstra MBA
Rijnstraat 8
2515 XP Den Haag

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een boete en een last onder dwangsom

Geachte heer Hoekstra,

De Autoriteit Persoonsgegevens (AP) heeft besloten om aan de minister van Buitenlandse Zaken (hierna: de Minister) een **bestuurlijke boete** van **€ 565.000** op te leggen. De AP is tot de conclusie gekomen dat de Minister, als verwerkingsverantwoordelijke bij het proces van het verlenen van zogeheten Schengenvisa, betrokkenen ontoereikend informeert en de beveiliging van de verwerking van persoonsgegevens onvoldoende waarborgt. Voor wat betreft de beveiliging van persoonsgegevens heeft de AP met betrekking tot het Nieuw Visum Informatie Systeem (NVIS) kortgezegd vastgesteld dat:

- er een beveiligingsplan ontbreekt;
- er onvoldoende maatregelen (genomen) zijn om persoonsgegevens fysiek te beschermen;
- onvolledige procedures bestaan over (de controle op) toegangsrechten tot NVIS;
- er tekortkomingen zijn in de logbestanden en de regelmatige controle hierop; en
- de procedure voor het melden van beveiligingsincidenten onvolledig was.

De Minister handelt hierdoor in strijd met artikel 13, lid 1 onder e, en artikel 32, lid 1, van de Algemene Verordening Gegevensbescherming (AVG). De AP heeft besloten aan u tevens een last onder dwangsom op te leggen, die ziet op het ongedaan maken van deze overtredingen – die bij het vaststellen van dit besluit nog immer niet zijn beëindigd.

De AP licht het besluit hierna nader toe. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 bevat de bevindingen. In hoofdstuk 3 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en in hoofdstuk 4 staat de last onder dwangsom beschreven. Hoofdstuk 5 bevat tot slot het dictum en de rechtsmiddelenclausule.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

Inhoud

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

1.Inleiding

1.1 Achtergrond

1. De AP is verantwoordelijk voor het houden van toezicht op het nationale deel van een aantal Europese informatiesystemen, waaronder het Visum Information System (hierna: VIS) en het Schengen Information System (hierna: SIS II). Op grond van het EU-rechtskader van deze systemen, dient de AP onafhankelijk toezicht te houden op de rechtmatigheid van de verwerking van persoonsgegevens door de betrokken lidstaat, met inbegrip van de verzending van en naar de centrale Europese voorziening van VIS en SIS. Voor visumaanvragen vindt de toegang tot het Europese VIS plaats via een nationaal systeem, te weten: N.VIS. De specifieke applicatie die onder N.VIS valt en door het ministerie van Buitenlandse Zaken (hierna: BZ) ten behoeve van Schengenvisa wordt gebruikt, is het Nieuw Visum Informatie Systeem (hierna: NVIS).

2. Het NVIS bevat de aanvraaggegevens, inclusief biometrische data, van alle aanvragers die via een Nederlandse consulaire post in het buitenland Schengenvisa willen verkrijgen ten behoeve van hun verblijf in Nederland en/of in andere Schengenlanden. Aanvragen voor Schengenvisa worden gedaan in landen buiten het Schengengebied en waar tevens geen sprake is van een speciale visumvrijstelling. Bij de behandeling van de visumaanvragen wordt ook altijd gecontroleerd of de aanvrager in SIS II voorkomt. SIS II omvat ingevoerde alerts door lidstaten op onder andere het gebied van Europese arrestatiebevelen en ongewenst verklaarden. De SIS II-controle vindt automatisch plaats, op de achtergrond van een visumaanvraag via NVIS.

3. In 2015 vond de Schengenevaluatie plaats, waarin de door de AP uitgevoerde toezicht op het nationale gedeelte van het SIS II en VIS werd beoordeeld. In het Schengen evaluatierapport 2015 is expliciet opgenomen dat de AP regelmatige controles bij de Nederlandse consulaire posten moet uitvoeren. Deze AP-controles maken tevens deel uit van het politie en justitie meerjarenplan dat de AP volgt in het kader van haar toezicht op onder andere de genoemde SIS II en VIS (systemen).

4. De AP heeft naar aanleiding hiervan een controlerend onderzoek uitgevoerd bij BZ en een aantal partijen die een rol hebben bij het proces van het verlenen van Schengenvisa. Het onderzoek omvatte de volgende organisaties:
   - de Nederlandse ambassade te Londen, Verenigd Koninkrijk (hierna: consulaire post Londen);
   - de Nederlandse ambassade te Dublin, Ierland (hierna: consulaire post Dublin);
   - de Consulaire Service Organisatie te Den Haag, dat fungeert als de backoffice van de visumverlening (hierna: de CSO);
   - [VERTROUWELIJK] (hierna: Verwerker 1) te Londen, Verenigd Koninkrijk, dat fungeert als externe dienstverlener (hierna: EDV) in het visumproces van de consulaire post Londen;
   - [VERTROUWELIJK] (hierna: Verwerker 2) te Utrecht, de uitvoerder van diverse IT-taken in relatie tot het nationale visuminformatiesysteem; en
   - [VERTROUWELIJK] (hierna: Verwerker 3) te Amsterdam, de dienstverlener ten behoeve van de NVIS-servers.

1.2 Doel onderzoek

5. Het onderzoek van de AP richtte zich op de (geselecteerde) fysieke, organisatorische en technische beveiligingsaspecten van NVIS in de context van het Schengen visumproces en behelsde onder meer het beveiligingsplan, de fysieke beveiliging, het toekennen van toegangsrechten tot NVIS en de logging van het NVIS-gebruik. Daarnaast werd de naleving van de wettelijke voorschriften gecontroleerd m.b.t. de informatievoorziening aan visumaanvragers en de opleiding van medewerkers betrokken bij het visumproces.

1.3 Visumproces voor Schengenvisum kort verblijf

6. In deze paragraaf geeft de AP een toelichting op het Schengen visumproces in het algemeen, en specifiek met betrekking tot de consulaire posten Londen en Dublin.

> *Schengenvisum kort verblijf*
> Een visum kort verblijf wordt een 'Schengenvisum' genoemd. Met dit visum mogen personen binnen een periode van 180 dagen, 90 dagen in het Schengengebied verblijven.[1] Met een Schengenvisum is het – kort samengevat – voor een persoon zonder EU-nationaliteit toegestaan vrij te reizen binnen de 26 Schengenlanden. Het land waar iemand het visum moet aanvragen wordt bepaald door het hoofddoel van de reis of de voornaamste bestemming van de aanvrager.

7. Het visumproces bij de onderzochte consulaire posten bestaat uit de volgende stappen[1]:
    1. [VERTROUWELIJK]
    2. [VERTROUWELIJK]
    3. [VERTROUWELIJK]
    4. [VERTROUWELIJK][2]
    5. [VERTROUWELIJK]
    6. [VERTROUWELIJK][3]
    7. [VERTROUWELIJK]
    8. [VERTROUWELIJK]
    9. [VERTROUWELIJK]

8. Nadat de registraties voltooid zijn en de inhoudelijke stappen zijn doorlopen kan een beslissing op de visumaanvraag worden genomen. Deze beslissing wordt geregistreerd in NVIS.[4] Bij een positief besluit wordt de visumsticker geprint en in het paspoort van de aanvrager geplakt, bij een negatief besluit wordt een weigeringsbeschikking aangemaakt. In beide gevallen wordt het besluit geregistreerd in VIS.[5]

[1] Dossierstuk 3, bijlage 1: NVIS Handleiding Visumaanvraagverwerking februari 2018, p. 19.
[2] Bij de behandeling van de visumaanvragen wordt ook altijd gecontroleerd of de aanvrager in het SIS II-systeem voorkomt. SIS II omvat ingevoerde alerts door lidstaten op, onder andere, het gebied van Europese arrestatiebevelen, en ongewenste vreemdelingen. De SIS II- controle vindt automatisch plaats, in de achtergrond van een visumaanvraag via NVIS.
[3] Dossierstuk 3, bijlage 3: Visio-Schengen Flowchart, p. 6 en 7.
[4] Dossierstuk 3, bijlage 3: Visio-Schengen Flowchart, p. 7.
[5] Dossierstuk 3, bijlage 3: Visio-Schengen Flowchart, p. 9.

Aanvragen Schengenvisum bij consulaire post Londen

9. De consulaire post Londen werkt samen met Verwerker 1 die een rol van een EDV[6] vervult. De taken[7] van de EDV behelzen onder meer het:
[VERTROUWELIJK]

10. Verwerker 1 verzorgt de intake van de meeste visumaanvragen die via de consulaire post Londen verlopen. In het kader van een visumaanvraag downloadt de aanvrager het aanvraagformulier via de website van BZ of via de website van Verwerker 1. Vervolgens maakt de aanvrager een afspraak bij Verwerker 1 via het afsprakensysteem van Verwerker 1. Op de dag van de afspraak meldt de aanvrager zich bij Verwerker 1. Verwerker 1 voert achtereenvolgens de volgende taken uit:[8]
[VERTROUWELIJK]

11. De consulaire post Londen voert onder meer de volgende taken uit:
[VERTROUWELIJK]

12. De taken van de CSO bestaan onder meer uit de volgende werkzaamheden:[9]
[VERTROUWELIJK]

[6] Overweging 13 Visumcode, artikel 40 lid 3 Visumcode, artikel 43 Visumcode.
[7] Artikel 43, lid 5, Visumcode.
[8] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart.
[9] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart, p. 4-5.

13. In voorkomende gevallen is het voorleggen van een aanvraag bij de Immigratie- en Naturalisatiedienst (IND) noodzakelijk of is het noodzakelijk om lidstaten te consulteren of te informeren.[10] Daarnaast kan het noodzakelijk zijn om de aanvrager te interviewen.[11] Bij de behandeling van de visumaanvragen wordt ook altijd gecontroleerd of de aanvrager in SIS II voorkomt. De SIS II-controle vindt automatisch plaats, in de achtergrond van een visumaanvraag via NVIS. Nadat deze stappen zijn doorlopen kan een beslissing op de visumaanvraag worden genomen. Deze beslissing wordt geregistreerd in NVIS.[12] Bij een positief besluit wordt de visumsticker geprint en in het paspoort van de aanvrager geplakt, bij een negatief besluit wordt een weigeringsbeschikking aangemaakt. In beide gevallen wordt het besluit geregistreerd in VIS.[13]

Aanvragen Schengenvisum bij consulaire post Dublin

14. De consulaire post Dublin werkte tijdens het onderzoek van de AP zonder tussenkomst van een EDV en neemt zelf visumaanvragen in behandeling. Hierbij worden grotendeels dezelfde stappen van het visumaanvraagproces gevolgd als bij Verwerker 1 en de consulaire post Londen. [VERTROUWELIJK]. [VERTROUWELIJK]. In het kader van een visumaanvraag downloadt de aanvrager het aanvraagformulier via de website van de ambassade of BZ. Een afspraak voor een intake bij het consulaat kan gemaakt worden op de website van de ambassade via een link naar een systeem voor afspraken.

15. In het kader van het visumproces voert het consulaat onder meer de volgende taken uit:
[VERTROUWELIJK]

16. De CSO voert vanuit haar rol als backoffice dezelfde taken uit als die in geval van de consulaire post Londen. Daarnaast heeft de CSO een belangrijke taak bij het registreren van de visumaanvraaggegevens die de consulaire post Dublin inneemt en als papierendossiers per post naar de CSO in Den Haag verstuurt.

Zienswijze BZ

17. BZ heeft verklaard dat er sinds het onderzoek door de AP enkele wijzigingen op bovenstaand visumproces zijn doorgevoerd. Verwerker 1 neemt tegenwoordig live foto's, en de intake van de visumaanvragen verloopt niet meer per post (via de consulaire post Londen). Daarnaast maakt consulaire post Dublin inmiddels wel gebruik van een EDV.[14]

[10] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart, p. 6.
[11] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart, p. 7.
[12] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart, p. 7.
[13] Dossierstuk 3, bijlage 3: Visio-Schengen visum Flowchart, p. 9.
[14] Schriftelijke Zienswijze BZ van 15 oktober 2021, p 3.

1.4 Wettelijk kader

18. De AP verwijst voor het wettelijk kader naar **BIJLAGE 1**.

1.5 Procesverloop

19. In het kader van dit onderzoek heeft de AP verschillende onderzoeksmethoden ingezet. De AP verrichtte bureau-onderzoek, verzocht schriftelijk om inlichtingen en heeft op diverse locaties meerdere onderzoeken ter plaatse (hierna: OTP's) gedaan. Tijdens de OTP's hebben de inspecteurs van de AP interviews afgenomen en onderzoek gedaan naar de informatiesystemen die gebruikt worden bij het visumproces. Naar aanleiding van de uitgevoerde OTP's heeft de AP de aanvullende documentatie opgevraagd en schriftelijke vragen gesteld. Gedurende het onderzoek zijn meerdere bestanden opgevraagd die betrekking hebben op de verleende toegangsrechten tot NVIS, NVIS-logging en selecties uit de NVIS-databases (m.n. tabellen van de databases).

20. Bij brief van 13 augustus 2021 heeft de AP aan de Minister een voornemen tot handhaving verzonden. De Minister heeft op 15 oktober 2021 schriftelijk een zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde rapport met bevindingen.[15] Op 4 november 2021 heeft bij de AP een zienswijzezitting plaatsgevonden waarbij BZ ook mondeling haar zienswijze heeft toegelicht.[16] Op 10 december 2021 heeft BZ desgevraagd nadere documenten gezonden.[17]

[15] Schriftelijke Zienswijze BZ van 15 oktober 2021.
[16] Brief BZ aan AP van 19 november 2021 met bijlage 1 Gespreksverslag.
[17] E-mail BZ aan AP van 10 december 2021.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

2. Bevindingen

2.1 Het verwerken van persoonsgegevens

2.1.1 Feitelijke bevindingen

21. In de Visumcode is vastgelegd welke gegevens de lidstaten moeten verzamelen om visa te kunnen verstrekken. In de VIS-Verordening is vastgelegd dat de volgende gegevens ten behoeve van het behandelen en het nemen van beslissingen over visumaanvragen voor het Schengengebied in het VIS opgeslagen dienen te worden: alfanumerieke gegevens betreffende de aanvrager en de aangevraagde, afgegeven, geweigerde, nietig verklaarde, ingetrokken of verlengde visa, een foto van de aanvrager, vingerafdrukgegevens en koppelingen naar andere aanvragen.[18] Bij ontvangst van een aanvraag stelt de visumautoriteit onverwijld het aanvraagdossier op door verschillende gegevens in het VIS in te voeren, zoals de voor- en achternaam, geslacht, plaats en land van geboorte, nationaliteit, soort visum dat wordt aangevraagd, doel van de reis, verblijfplaats, huidig beroep, foto en vingerafdrukken van de aanvrager.[19]

22. Gemachtigde personeelsleden van de visumautoriteiten hebben toegang tot het VIS en kunnen deze gegevens invoeren, wijzigen of verwijderen.[20] Zo worden bij de afgifte van een visum, bij het afbreken van een visumaanvraag, bij een weigering van een visumaanvraag, bij een nietigverklaring/intrekking van een visum of een verlenging van een visum[21] gegevens toegevoegd aan het aanvraagdossier. Vervolgens is het mogelijk dat de gegevens gedurende het aanvraagtraject worden gewijzigd of verwijderd.[22] BZ (en diens consulaire posten) maken gebruik van het NVIS waarin persoonsgegevens ten behoeven van het Schengen-visumproces worden opgeslagen, gewijzigd en verwijderd.

2.1.2 Juridische beoordeling

23. De gegevens van visumaanvragers die zijn verwerkt in het NVIS kwalificeren als *persoonsgegevens* in de zin van artikel 4, onder 1, AVG, omdat het informatie betreft over geïdentificeerde natuurlijk personen.[23] Een gedeelte van deze gegevens zijn biometrische gegevens in de zin van artikel 4, onder 14, en artikel 9 AVG en kwalificeren daarmee als bijzondere persoonsgegevens.

24. Verder valt het invoeren, raadplegen, opslaan, inzien en wijzigen van persoonsgegevens in NVIS onder de reikwijdte van het begrip *verwerking* van persoonsgegevens in de zin van artikel 4, onder 2, AVG. De AP stelt vast dat er persoonsgegevens worden verwerkt door middel van het NVIS bij het doorlopen van het visumproces voor kortlopend verblijf.

[18] Artikel 5, lid 1, Verordening (EG) Nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf ('VIS-Verordening'), *PB* 2008, L218/60.
[19] Artikel 8, lid 1 jo. 9 VIS-Verordening.
[20] Artikel 6, lid 1, VIS-Verordening.
[21] Artikel 10 tot en met 14 VIS-Verordening.
[22] Artikel 24 en 25 VIS-Verordening.
[23] Omdat onder meer naam en adresgegevens en ook het BSN worden verwerkt, staat de identiteit van de personen vast en betreft het dus geïdentificeerde personen.

2.2 Verwerkingsverantwoordelijke en verwerker(s)

2.2.1 Feitelijke bevindingen

Ministerie van Buitenlandse Zaken

25. De AP stelt vast dat voor Nederland de minister van BZ de aangewezen verantwoordelijke is voor verwerkingen van de persoonsgegevens in het VIS.[24]

26. De AP stelt vast dat een belangrijk deel van de taken op het gebied van NVIS dienstverlening organisatorisch is belegd bij het Directoraat-Generaal Europese Samenwerking.[25] Onder dit Directoraat valt een aantal directies, waarvan er twee met name een rol hebben bij de verlening van visa. Ten eerste de directie Consulaire Zaken en Visumbeleid (DCV). DCV is onder andere belast met het verlenen van consulaire diensten aan Nederlanders in het buitenland en met het aansturen van de consulaire functie op het departement en op de posten.[26]Ten tweede de Consulaire Service Organisatie (CSO) in Den Haag. CSO is een shared serviceorganisatie die als primaire taak heeft om backoffice processen met betrekking tot het toekennen van visa en reisdocumenten vorm te geven. De AP heeft vastgesteld, en BZ heeft dat bevestigd, dat de backoffice van het consulaat Londen en het consulaat Dublin zich bevindt bij CSO. Daarnaast verzorgt CSO de backofficewerkzaamheden ten aanzien van een aantal andere consulaire diensten en producten.[27]

Verwerker 1

27. Verwerker 1 is een outsourcing- en technologiedienstenbedrijf dat voor Nederland in diverse landen uitvoerende zaken regelt met betrekking tot visum- en paspoortafgifte. Het hoofdkantoor, [VERTROUWELIJK] is gevestigd in Dubai, Verenigde Arabische Emiraten.

28. Verwerker 1 is als externe dienstverlener[28] aangewezen om visa aanvraagvoorzieningen te faciliteren. Het bedrijf richt fysieke bezoekerscentra in waar betrokkenen hun aanvragen kunnen indienen. In Londen verzorgt Verwerker 1 voor BZ de frontoffice voor de visumaanvragen die in het Verenigd Koninkrijk worden ingediend. Met betrekking tot deze werkzaamheden is op 21 maart 2019 een concessieovereenkomst gesloten tussen Verwerker 1 en BZ.[29] Op grond van deze opdracht moet Verwerker 1 visumaanvragen en biometrische informatie verwerken. Medewerkers van Verwerker 1 nemen deze gegevens in ontvangst van de aanvrager. Op de locatie van [VERTROUWELIJK] in Londen zijn ICT-voorzieningen aangelegd [VERTROUWELIJK].[30] Verwerker 1 heeft geen toegang tot NVIS, dit gebeurt bij de CSO. Bij Verwerker 1 kunnen aanvragers hun paspoorten inleveren en ophalen.

[24] Lijst van de bevoegde nationale autoriteiten waarvan de naar behoren gemachtigde personeelsleden toegang hebben tot het Visum Informatie Systeem (VIS) om gegevens in te voeren, te wijzigen, te verwijderen of te raadplegen (2012/C79/05).
[25] Artikel 7, lid 2, sub d, Organisatiebesluit Buitenlandse Zaken 2019.
[26] Artikel 7, lid 2, sub c, Organisatiebesluit Buitenlandse Zaken 2019.
[27] Artikel 7, lid 2, sub d, Organisatiebesluit Buitenlandse Zaken 2019.
[28] Artikel 40, lid 3, Visumcode.
[29] Dossierstuk 3, bijlage 4a: [VERTROUWELIJK].
[30] Dossierstuk 3, bijlage 4d: Appendix 1 to the standard contractual clauses.

29. Voor de doorgifte van verwerkte persoonsgegevens door BZ naar Verwerker 1 is tussen partijen een regeling getroffen op basis van de door de Europese Commissie, conform artikel 46, lid 2, onder c, AVG vastgestelde standaard contractbepalingen inzake gegevensbescherming (´Standard Contractual Clauses´).[31] In artikel 1, sub b en c, is het volgende neergelegd:

(b) ´the data exporter´ means the controller who transfer the personal data;
(c)´the data importer´ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country´s system ensuring adequate protection within the meaning of Chapter V of Regulation (EU) 2016-679.

30. Artikel 4 van de Standard Contractual Clauses bevat verplichtingen die zijn neergelegd bij de ´data exporter´. Op grond van artikel 4, sub b, Standard Contractual Clauses verbindt de ´data exporter´ zich aan de verplichting 'that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses'.

31. In appendix 1 bij de Standard Contractual Clauses staat dat BZ de ´data exporter´ is en [VERTROUWELIJK] de ´data importer´.[32]

Verwerker 2

32. Uit het onderzoek van de AP is gebleken dat Verwerker 2 een belangrijke rol vervult binnen het visumverleningsproces. Verwerker 2 is een consultancybedrijf dat zich richt op advisering over en leveren van informatietechnologie.

33. De dienstverlening ten behoeve van NVIS wordt door de volgende organisatieonderdelen van Verwerker 2 uitgevoerd: [VERTROUWELIJK] als onderdeel van [VERTROUWELIJK] en [VERTROUWELIJK]. [VERTROUWELIJK] (en derhalve Verwerker 2 Nederland BV) maakt gebruik van diensten van het [VERTROUWELIJK] in India dat onderdeel uitmaakt van Verwerker 2 [VERTROUWELIJK].[33]

34. Verwerker 2 heeft op 31 augustus 2010 een overeenkomst gesloten met BZ voor het leveren van ondersteunende diensten ten behoeve van NVIS. De dienstverlening omvat het applicatie- en technisch beheer, beschikbaar stellen (waaronder hosting), het onderhouden van, het ontwikkelen en vernieuwen van de functionaliteit voor en advisering ten behoeve van o.a. het NVIS. Verwerker 2 levert in dit kader onder meer maatwerkapplicaties die specifiek zijn ontwikkeld om het visum verstrekking proces te ondersteunen.[34] Verwerker 2 rapporteert aan de Directeur Consulaire Zaken en Visumbeleid van BZ.[35]

35. In artikel 2.1 van de Verwerkersovereenkomst (Bijlage bij de Overeenkomst Beschikbaar stellen, Onderhouden en ontwikkelen NVIS van 31 augustus 2010) staat dat met betrekking tot de verwerking van

[31] Dossierstuk 3, bijlage 4b: Standard contractual clauses (processors).
[32] Dossierstuk 3, bijlage 4d: Appendix 1 to the standard contractual clauses
[33] Dossierstuk 23, bijlage 05: Organogram Verwerker 2 wereldwijd t.b.v. NVIS
[34] Dossierstuk 14, bijlage 02.1: AVG Wijzigingsovereenkomst Verwerker 2 – Min BZ NVIS 20180529, p.14.
[35] Dossierstuk 14, bijlage 02.1: AVG Wijzigingsovereenkomst Verwerker 2 –Min BZ NVIS 20180529, p. 1.

persoonsgegevens van BZ door Verwerker 2 onder deze Verwerkersovereenkomst geldt dat BZ de verwerkingsverantwoordelijke is en dat Verwerker 2 de verwerker is.[36]

36. Uit artikel 4.1 van de Verwerkersovereenkomst tussen Verwerker 2 en BZ volgt dat Verwerker 2 sub-verwerkers kan inschakelen voor het verwerken van persoonsgegevens wanneer sprake is van voorafgaande schriftelijke specifieke of algemene toestemming van BZ. Verwerker 2 moet op basis van de overeenkomst met BZ aan sub-verwerkers dezelfde verplichtingen opleggen met betrekking tot de verwerking van persoonsgegevens als die waaraan Verwerker 2 zelf gebonden is door deze Verwerkersovereenkomst.

37. In artikel 5.1 van de verwerkersovereenkomst tussen BZ en Verwerker 2 is vastgesteld dat BZ het recht heeft om eenmaal per contractjaar door een gecertificeerde interne of externe auditor een audit te laten uitvoeren naar Verwerker 2's naleving van haar verplichtingen onder de verwerkersovereenkomst. De AP heeft vastgesteld dat BZ de naleving van Verwerker 2 evalueert door het verlangen van zogeheten assurance verklaringen van Verwerker 2. De AP heeft van BZ twee assurance rapporten ontvangen met betrekking tot Verwerker 2 over de periode 1 november 2017-31 oktober 2018.[37]

38. De AP heeft vastgesteld dat Verwerker 2 in het kader van haar dienstverlening ten behoeve van NVIS het bedrijf Verwerker 3 inzet als sub-verwerker. Verwerker 3 (voorheen [VERTROUWELIJK]) ontwikkelt en beheert wereldwijd centra voor de opslag van data. In Nederland heeft Verwerker 3 een datacentrum in Amsterdam. Verwerker 3 levert diensten aan Verwerker 2,[38] namelijk de beschikbaarheid realiseren van het datacentrum, inclusief fysieke voorzieningen.

[VERTROUWELIJK][39]

2.2.2 Juridische beoordeling

Verwerkingsverantwoordelijke

39. Conform de VIS-Verordening (artikel 41, lid, 4) wijst elke lidstaat voor de verwerking van persoonsgegevens in het VIS de autoriteit aan die moet worden beschouwd als de verantwoordelijke die de centrale verantwoordelijkheid voor de gegevensverwerking door deze lidstaat heeft. De verantwoordelijke is bekendgemaakt bij de Europese Commissie en gepubliceerd in het Publicatieblad van de Europese Unie.[40] Op basis hiervan is de Minister van Buitenlandse Zaken aangemerkt als

[36] Dossierstuk 14, bijlage 02.1: AVG Wijzigingsovereenkomst Verwerker 2 – Min BZ NVIS 20180529.
[37] Dossierstuk 14, bijlage 12.2: [VERTROUWELIJK].
[38] Dossierstuk 20: [VERTROUWELIJK].
[39] Dossierstuk 20: [VERTROUWELIJK].
[40] Lijst van de bevoegde nationale autoriteiten waarvan de naar behoren gemachtigde personeelsleden toegang hebben tot het Visum Informatie Systeem (VIS) om gegevens in te voeren, te wijzigen, te verwijderen of te raadplegen, *PB* 2012, C79/05.

verwerkingsverantwoordelijke van NVIS. Dit wordt ook bevestigd door de door het Ministerie aan de AP verstrekte stukken.[41]

40. De Minister (met ondersteuning van zijn ministerie) bepaalt op welke wijze de visumaanvragen behandeld dienen te worden en neemt ook de uiteindelijke beslissing op visumaanvragen. Daarmee bepaalt de Minister het doel en de middelen voor de verwerking van persoonsgegevens binnen NVIS.

41. De AP stelt vast dat de minister van Buitenlandse Zaken de verwerkingsverantwoordelijke is, in de zin van artikel 4, aanhef onder 7, AVG, voor de verwerking van persoonsgegevens in het kader van NVIS. Waar in dit besluit BZ wordt genoemd stelt de AP dit gelijk aan de minister van Buitenlandse Zaken.

Verwerkers

42. Blijkens artikel 43 Visumcode mogen lidstaten samenwerken met een externe dienstverlener die de verwerkingsverantwoordelijke ondersteunt in het visumproces. Lidstaten zijn verplicht afspraken te maken in een rechtsinstrument waarbij de minimumvereisten zijn bepaald in de Visumcode.[42]

43. De AP constateert dat BZ een aantal partijen inschakelt om de gegevensverwerkingen in het visumproces te ondersteunen, namelijk Verwerker 1 (de externe dienstverlener die de visumaanvragen in behandeling neemt), Verwerker 2 (voor het applicatie- en technisch beheer van NVIS) en Verwerker 3 die als verwerker ondersteuning biedt aan de processen van Verwerker 2. Er zijn met deze partijen verwerkingsovereenkomsten gesloten. Uit de verschillende verwerkersovereenkomsten gesloten tussen deze partijen en BZ volgt dat de Minister als verwerkingsverantwoordelijke wordt aangemerkt en de genoemde partijen als verwerkers.

44. De AP stelt daarom vast dat Verwerker 2 en Verwerker 1 verwerkers zijn zoals bedoeld in artikel 4, onder 8, AVG. Verwerker 3 is een verwerker die door Verwerker 2 in dienst is genomen, zoals bedoeld in artikel 28, lid 2 en lid 4, AVG (sub-verwerker).

2.3 Beveiligingsplan NVIS

2.3.1 Wettelijk kader

45. Artikel 32, lid 2, VIS Verordening schrijft voor dat iedere lidstaat de nodige technische en organisatorische beveiligingsmaatregelen vaststelt, waaronder een beveiligingsplan. Dit plan is één van de beveiligingsmaatregelen die zij moet treffen om de gegevens te beveiligen voor en tijdens de verzending naar het NVIS. Een dergelijke verplichting vloeit ook voort uit artikel 32 en 24 AVG. Artikel 24 AVG schrijft meer in het algemeen voor dat de verantwoordelijke maatregelen op het gebied van compliance met de AVG moet nemen en dat die periodiek geëvalueerd moeten worden.

46. Artikel 32, lid 3, VIS Verordening stelt verder dat de beheersautoriteit de nodige maatregelen moet nemen ter verwezenlijking van de doelstellingen, zoals bedoeld in lid 2 ten aanzien van de werking van het VIS, met inbegrip van de vaststelling van een beveiligingsplan. De strategische uitgangspunten en

[41] Bijvoorbeeld dossierstuk 12, bijlage 44a: pia aanvraagstation getekend en dossierstuk 12, bijlage 44b: nvis pia ondertekend.
[42] Bijlage X Visumcode.

randvoorwaarden die BZ hanteert voor informatiebeveiliging ten opzichte van NVIS moeten duidelijk uit het beveiligingsplan blijken. Concreet betekent dit dat BZ een beveiligingsplan moet hebben opgesteld voor het NVIS, waarin ten minste aandacht wordt besteed aan de punten a tot en met k die in artikel 32, lid 2, VIS Verordening zijn opgenomen.

47. Ook de Baseline Informatiebeveiliging Overheid (BIO) schrijft de aanwezigheid van een informatiebeveiligingsplan voor dat periodiek wordt beoordeeld, hierbij zijn de volgende normen relevant:

5.1.1	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a. De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f. De bevordering van het beveiligingsbewustzijn.
5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.

2.3.2 Feitelijke bevindingen

48. De AP heeft gedurende het onderzoek aan BZ schriftelijk vragen gesteld over het beveiligingsplan met betrekking tot persoonsgegevens in NVIS. De AP heeft tevens het bestaan van een beveiligingsplan en de inhoud daarvan in de praktijk gecontroleerd tijdens het onderzoek ter plaatse bij de consulaire posten in Londen en Dublin. Verder heeft de AP schriftelijke documentatie opgevraagd die betrekking heeft op het bestaan en de inhoud van een beveiligingsplan.

Ministerie van Buitenlandse Zaken

49. De AP stelt vast dat BZ tijdens het onderzoek op de vraag van de AP[43] om een beveiligingsplan (N)VIS te verstrekken, heeft geantwoord met drie documenten, te weten:
- Kwetsbaarheidsanalyse en IB-plan DCV[44]
- PIA Aanvraagstation[45]

[43] Dossierstuk 1: Aankondiging onderzoek VIS/ informatieverzoek AP van 29 mei 2019.
[44] Dossierstuk 3, bijlage 5a: Kwetsbaarheidsanalyse en IB-plan DCV.
[45] Dossierstuk 3, bijlage 5b: PIA Aanvraagstation.

- Quickscan Schengenvisum februari 2019[46]

50. De "Kwetsbaarheidsanalyse en IB-plan DCV" van januari 2015 bevat een risicoafweging, met betrekking tot de bedrijfsprocessen voor visumverlening van DCV en de posten, die de directie DCV heeft laten uitvoeren om te voldoen aan de verplichtingen van het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007. Het rapport bevat o.a. een verslaglegging van de relevante dreigingen en kwetsbaarheden van de informatiesystemen. Ook bevat het rapport maatregelen die de vastgestelde risico's tot een acceptabel niveau kunnen brengen. Het rapport kwalificeert deze voorgestelde maatregelen als een 'informatiebeveiligingsplan' inclusief prioritering.

51. De "PIA Aanvraagstation" betreft een Privacy Impact Assessment van het aanvraagstation. Het eindresultaat van de PIA is een set van risico's en aanbevelingen voor de beveiligingsmaatregelen die onder verantwoordelijkheid van DCV dienen te worden gerealiseerd.

52. De "QuickScan Schengenvisum februari 2019" is een QuickScan die op verzoek van DCV is uitgevoerd naar de beveiligingseisen die vanuit de bedrijfsprocessen worden gesteld aan het proces Schengenvisum waar bijzondere persoonsgegevens worden opgenomen. Het doel van de QuickScan is om zo objectief mogelijk de beveiligingseisen vast te stellen die aan het Schengenvisum gesteld worden. Hierbij is tevens gekeken of deze eisen binnen de Baseline informatiebeveiliging vallen of dat deze daar bovenuit stijgen. Uit de QuickScan volgt dat het Schengenvisumproces buiten de Baseline informatiebeveiliging van BZ valt en dat een aanvullende risicoanalyse vereist is. In de QuickScan wordt hiertoe opdracht gegeven.

53. Op basis van deze drie documenten constateert de AP dat BZ een aantal verschillende documenten heeft, waar (voorgenomen) beveiligingsmaatregelen in staan genoemd. Een aantal van die maatregelen heeft direct betrekking op NVIS.

Consulaire post Londen

54. Tijdens het onderzoek ter plaatse op 2 juli 2019 in Londen, heeft de AP volledigheidshalve gevraagd om inzage in het beveiligingsplan met betrekking tot NVIS. De consulaire post Londen beschikt over een standaardformat beveiligingsplan dat door BZ wordt aangeleverd en lokaal door de consulaire post wordt ingevuld. Twee inspecteurs van de AP en de FG van BZ hebben inzage gehad in de meest recente versie van het beveiligingsplan. [VERTROUWELIJK]:
[VERTROUWELIJK]

De genoemde documenten hebben betrekking op de beveiliging van de consulaire post Londen, met name [VERTROUWELIJK], en zijn niet gericht op de informatiebeveiliging van NVIS en het visumproces. De AP stelt vast dat zij op de consulaire post in Londen documentatie heeft ingezien die niet ziet op de informatiebeveiliging met betrekking tot NVIS.[47]

[46] Dossierstuk 3, bijlage 5c: Quickscan Schengenvisum februari 2019.
[47] Dossierstuk 8: Verslag van Ambtshandelingen beveiligingsplan OTP consulaire post Londen.

Consulaire post Dublin

55. De AP heeft ook in Dublin gecontroleerd of er in de praktijk een beveiligingsplan met betrekking tot NVIS voorhanden was. Tijdens het onderzoek ter plaatse op 22 januari 2020 bij de consulaire post in Dublin is verklaard dat een beveiligingsplan aanwezig is. Het betreft een standaardformat beveiligingsplan dat door BZ wordt aangeleverd en lokaal op de post wordt ingevuld. Een aanpassing van het beveiligingsplan wordt één keer per jaar gedaan door de plaatsvervangend chef de post.[48]

56. Twee inspecteurs van de AP en de FG van BZ hebben op 23 januari 2020, mede tijdens het onderzoek ter plaatse bij de consulaire post in Dublin, desgevraagd inzage gekregen in een beveiligingsplan met betrekking tot NVIS .[49] [VERTROUWELIJK]:
[VERTROUWELIJK].[50]

De AP stelt vast dat op de consulaire post in Dublin overgelegde documentatie niet ziet op de informatiebeveiliging met betrekking tot NVIS.[51]

CSO Den Haag

57. De AP heeft bij CSO gecontroleerd of er een beveiligingsplan in de zin van de VIS Verordening voorhanden is. De AP constateert dat de CSO op de vraag van de AP[52] om een beveiligingsplan (N)VIS te verstrekken heeft geantwoord met 9 documenten[53], te weten:

- Baseline informatiebeveiliging BZ 2018, versie 1.00 definitief;[54]
- Beveiliging Security Management Pakket, versie 0.2 definitief;[55]
- Beveiligingsplan Risicoanalyse rapportage – [VERTROUWELIJK];[56]
- Beveiliging analyse ontvreemde beveiligde post CSO;[57]
- Beveiliging analyse inbraak gebouw;[58]
- Beveiliging analyse binnendringen mer en ser;[59]
- Beveiliging voorbeeld Onbevoegden [VERTROUWELIJK];[60]
- Beveiliging voorbeeld info bij onverwacht bezoek;[61]

[48] Dossierstuk 27: Verslag van Ambtshandelingen consulaire post Dublin.
[49] Dossierstuk 28: Verslag van Ambtshandelingen beveiligingsplan OTP consulaire post Dublin.
[50] Ter plaatse stelden de AP-inspecteurs vast dat inzage in dit document niet noodzakelijk was voor het onderzoek.
[51] Dossierstuk 27: Verslag van Ambtshandelingen consulaire post Dublin.
[52] Dossierstuk 13: Informatieverzoek AP van 25 juli 2019.
[53] Dossierstuk 14: Reactie BZ van 8 augustus 2019 op Informatie AP van 25 juli 2019.
[54] Dossierstuk 14, bijlage 14.1 Baseline informatiebeveiliging BZ 2018 v1.00 Definitief.pdf.
[55] Dossierstuk 14, bijlage 16.1: Beveiliging Security Management Pakket 0.2 definitief.
[56] Dossierstuk 14, bijlage 16.2: Beveiligingsplan Risicoanalyse rapportage - [VERTROUWELIJK].
[57] Dossierstuk 14, bijlage 16.3: Beveiliging analyse ontvreemden beveiligde post CSO.
[58] Dossierstuk 14, bijlage 16.4: Beveiliging analyse inbraak gebouw.
[59] Dossierstuk 14, bijlage 16.5: Beveiliging analyse binnendringen mer en ser.
[60] Dossierstuk 14, bijlage 16.6: Beveiliging voorbeeld Onbevoegden [VERTROUWELIJK].
[61] Dossierstuk 14, bijlage 16.7: Beveiliging voorbeeld info bij onverwacht bezoek.

- Overzicht toegang CSO.[62]

58. Deze documenten beschrijven aspecten van informatiebeveiliging. De AP constateert dat deze aspecten niet specifiek gericht zijn op of gerelateerd zijn aan NVIS. Er zijn ook geen concrete verwijzingen naar het visumproces aangetroffen.

2.3.3 Juridische beoordeling

59. De AP stelt vast dat BZ in verschillende documenten bepaalde beveiligingsmaatregelen heeft opgenomen. Een aantal van deze documenten is verstrekt aan de AP naar aanleiding van informatieverzoeken gericht aan de minister. Andere documenten zijn naar voren gebracht bij of naar aanleiding van het bezoek van AP aan CSO.

60. Met betrekking tot de overgelegde documenten stelt de AP het volgende vast.
De "Kwetsbaarheidsanalyse en IB-plan DCV" bevat een aantal beveiligingsmaatregelen, maar is niet actueel (dateert van 2015). De lokale beveiligingsmaatregelen, die tijdens het onderzoek ter plaatse volledigheidshalve bij de consulaire post in Dublin en Londen zijn ingezien en de documenten die bij de CSO zijn opgevraagd, zijn niet specifiek gericht op NVIS en zien slechts op een beperkt aantal beveiligingsmaatregelen (en niet op informatiebeveiliging) die op grond van artikel 32 VIS Verordening worden voorgeschreven. De maatregelen uit deze documenten zien vooral op de brede beveiliging van gebouwen en systemen, inclusief daaraan gerelateerde potentiële beveiligingsrisico's. De AP stelt vast dat een overkoepelend beveiligingsplan ten aanzien van NVIS, met aandacht voor de maatregelen, zoals neergelegd in artikel 32, lid 2, onder a tot en met k van de VIS Verordening, echter niet aanwezig is.

61. BZ stelt in haar zienswijze dat de AVG, de VIS-verordening en de BIR/BIO geen eisen stellen aan de vorm van een beveiligingsplan en ook niet een beveiligingsplan vereisen dat uitsluitend op het nationaal visum informatiesysteem ziet. BZ beschouwt een aantal documenten in samenhang als beveiligingsplan voor NVIS[63]:
   - Privacy Impact Assessment Schengen en Caribische Visa van 25 oktober 2018.
   - Baseline toets NVIS
   - Quickscan Schengenvisum februari 2019 en de Risicoanalyse 'Kwetsbaarheidsanalyse en IB-plan DCV'.

62. BZ heeft in haar zienswijze aangegeven dat BZ tot haar spijt heeft geconstateerd dat op het eerdere informatieverzoek van de AP de eerste twee documenten niet aan de AP zijn verstrekt. BZ merkt verder op dat de externe auditor die in opdracht van de AP in het kader van de VIS-audit heeft geoordeeld dat BZ met de Baselinetoets, PIA en de risicoanalyse voldoet aan de norm dat een beveiligingsplan is vastgesteld.

63. De AP volgt de zienswijze van BZ niet. Gedurende het onderzoek heeft de AP op verschillende momenten gevraagd naar het beveiligingsplan van NVIS. BZ had meerdere mogelijkheden om de relevante stukken te verstrekken. De AP ziet onderhavig ambtshalve onderzoek en de VIS-audit die door de externe partij is uitgevoerd als twee separate trajecten die niet tegelijkertijd hebben plaatsvonden. De VIS-audit was

[62] Dossierstuk 14, bijlage 16.8: Overzicht toegang CSO.
[63] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 4.

breder van opzet en maakte gebruik van een ander toetsingskader. Daarnaast heeft de externe auditor slechts vastgesteld dat 1) niet hij maar BZ de combinatie van de Baselinetoets, PIA en risicoanalyse samen beschouwd als Informatiebeveiligingsplan en 2) een concreet informatiebeveiligingsplan rondom het Visum proces ontbreekt.

64. De AP heeft de nieuw aangeleverde documentatie van BZ beoordeeld. De AP stelt vast dat de 'Privacy Impact Assessment Schengen en Caribische Visa van 25 oktober 2018', zoals de titel al suggereert, een Privacy Impact Assessment betreft. Dit is een zeer nuttig instrument om de privacyrisico's van een gegevensverwerking in kaart te brengen, maar vormt geen plan dat gericht is op informatiebeveiliging in zijn geheel. De overgelegde 'Baseline toets NVIS' is een soort ingevulde vragenlijst/checklist. Het is een opsomming van BIO-normen met daaruit opdrachten voor het maken en nemen van beveiligingsmaatregelen, waarbij het voor de AP niet begrijpelijk is hoe de gegeven antwoorden moeten worden geduid. Het is op basis van deze documenten voor de AP onduidelijk welke beleidsmaatregelen en beheersmaatregelen BZ concreet genomen heeft voor NVIS.

65. De vorm van een beveiligingsplan is vrij maar de strategische uitgangspunten en randvoorwaarden die BZ hanteert voor informatiebeveiliging ten opzichte van NVIS moeten wel duidelijk uit het beveiligingsplan blijken. Daarnaast vereist artikel 32, lid 2, VIS Verordening dat BZ een beveiligingsplan moet hebben opgesteld voor NVIS, waarin ten minste aandacht wordt besteed aan de punten a tot en met k uit artikel 32, lid 2, VIS Verordening. BZ heeft dit naar het oordeel van de AP onvoldoende aangetoond. BZ heeft bijvoorbeeld niet een beveiligingsplan overgelegd waarin staat welke randvoorwaarden er gelden voor de fysieke beveiliging van NVIS waarmee de passende bescherming van de persoonsgegevens gewaarborgd wordt. Evenmin heeft de AP een formele procedure van BZ ontvangen waarin omschreven staat hoe en wanneer BZ controles uitvoert op logging. De algemene procedure die BZ ten tijde van het onderzoek heeft verstrekt voor het melden van beveiligingsincidenten door BZ-medewerkers, voldeed niet. En de procedures over toekennen en controleren van toegangsrechten tot NVIS-omgeving zijn pas door BZ in januari 2022 vastgesteld. De AP verwijst naar paragraaf 2.4, 2.5, 2.6 en 2.7 voor de uitgebreide beoordeling van deze procedures. De AP concludeert dat de documenten die BZ heeft gepresenteerd als - in zijn gehele bezien - een informatiebeveiligingsplan, niet voldoet aan de daaraan te stellen randvoorwaarden.

66. Gelet op de BIO-normen stelt de AP verder vast dat door het ontbreken van (essentiële onderdelen in) beleid voor informatiebeveiliging, dit beleid niet met geplande tussenpozen (of als zich significante veranderingen voordoen) door BZ beoordeeld is om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. Het beveiligen van informatie is een proces waarbij steeds een Plan-Do-Check-Act cyclus moet worden doorlopen, zoals onder andere neergelegd in BIO-norm 5.1.2.1.

67. BZ heeft in haar zienswijze enkele documenten verstrekt over de PDCA-cyclus die zij doorlopen heeft.[64] De AP stelt hierover vast dat BZ in de 'Baseline informatiebeveiliging BZ 2021' op een hoog abstractieniveau heeft vastgesteld wie voor implementatie en uitvoering van BIO-normen verantwoordelijk is. Het beleid voor Bescherming persoonsgegevens beschrijft de PDCA-cyclus ten opzichte van de bescherming van persoonsgegevens, maar bevat niet de beveiligingsaspecten daarover. Ditzelfde geldt voor het document Grip op privacy, de AVG-handleiding, in control-verklaringen en het overgelegde opvolgingenmemo. BZ heeft met risicoanalyses uit 2015 en 2020 en een maatregelenplan uit

[64] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 4.

november 2021 laten zien dat zij slechts af en toe beveiligingsmaatregelen met betrekking tot NVIS heeft geëvalueerd en daarop heeft geacteerd.

68. Op grond van het bovenstaande komt de AP tot de conclusie dat BZ geen beveiligingsplan heeft (en dit dus ook niet heeft geëvalueerd) dat voldoet aan de eisen van artikel 24 en 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, aanhef, VIS Verordening en BIO-normen 5.1.1, 5.1.1.1 en 5.1.2.1.

2.4 Fysieke beveiliging toegang tot NVIS

2.4.1 Wettelijk kader

69. Artikel 32, lid 2, onder a, VIS Verordening schrijft voor dat maatregelen vastgesteld moeten worden om gegevens fysiek te beschermen, met inbegrip van het opstellen van noodplannen voor de fysieke infrastructuur. Deze eis is ook in algemene bewoordingen neergelegd in artikel 32 AVG. Verder zijn in de BIO-normen opgenomen die illustreren op welke punten de fysieke beveiliging gecontroleerd kunnen worden. De BIO beschrijft doelen die gerealiseerd moeten worden (het "wat") niet letterlijk *hoe* dat geregeld moet zijn. De AP heeft de fysieke beveiliging gecontroleerd op basis van een checklist (zie toelichting in de volgende paragraaf). De volgende bepalingen uit de BIO zijn voor de beoordeling van deze checklist relevant:

11.1.1	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
11.1.2	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
11.1.3	**Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
11.1.4	**Beschermen tegen bedreigingen van buitenaf** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
11.1.5	**Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
11.2.2	**Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.

2.4.2 Feitelijke bevindingen

70. De AP heeft de fysieke beveiliging onderzocht bij de consulaire posten Londen en Dublin, de CSO in Den Haag, Verwerker 2 in Utrecht en Verwerker 3 in Amsterdam. Bij de controles heeft de AP per locatie

gebruik gemaakt van twee (identieke) checklists. De eerste checklist was gericht op de fysieke beveiliging van het *gebouw* en de tweede checklist op de fysieke beveiliging van de *ruimtes* waarbinnen toegang tot de NVIS-omgeving mogelijk is en/of het intakeproces voor Schengenvisa plaatsvindt.[65] Hieronder staat per locatie de situatie beschreven die aangetroffen is tijdens de onderzoeken ter plaatse.

Consulaire post Londen

71. [VERTROUWELIJK][66]

Verwerker 1 Londen

72. [VERTROUWELIJK] [67]

[65] [VERTROUWELIJK]
[66] Dossierstuk 7: Verslag van Ambtshandelingen OTP consulaire post Londen.
[67] Dossierstuk 9: Verslag van Ambtshandelingen OTP Verwerker 1 Londen.

Consulaire post Dublin

73. [VERTROUWELIJK] [68]

CSO Den Haag

74. [VERTROUWELIJK][69]

[68] Dossierstuk 27: Verslag van Ambtshandelingen OTP consulaire post Dublin.
[69] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september 2019.

Verwerker 2 Utrecht

75. [VERTROUWELIJK]

Verwerker 3 Amsterdam

76. [VERTROUWELIJK][70] [71] [72]

2.4.3 Juridische beoordeling

77. De AP stelt allereerst vast dat op alle onderzochte locaties maatregelen zijn genomen op het gebied van fysieke beveiliging. De AP concludeert dat er maatregelen zijn genomen om de gebouwen en de ruimte(n) waarin gegevens van visumaanvragers worden verwerkt fysiek te beschermen, onder meer met camera's en bewegingssensoren. Voorts concludeert de AP dat de ruimtes waarin persoonsgegevens van visumaanvragers worden verwerkt aangemerkt zijn als beveiligde zones.

[70] Dossierstuk 19: Verslag van Ambtshandelingen OTP Verwerker 3 8 november 2019.
[71] Dossierstuk 20: [VERTROUWELIJK]
[72] Dossierstuk 21: Email BZ van 13 november 2019 met stukken n.a.v. OTP 8 november.

78. De AP stelt echter vast dat er door BZ niet expliciet is bepaald welke onderdelen van de IT-infrastructuur aangemerkt dienen te worden als de kritieke infrastructuur van het visumproces. Om in dit geval te kunnen voldoen aan artikel 32 AVG jo. 32, lid 2, onder a, VIS Verordening is dit wél een vereiste. BZ heeft in haar zienswijze verklaard dat zij in het voorjaar van 2020 verschillende systemen als kritiek is gaan vaststellen. BZ heeft tijdens de zienswijzezitting d.d. 4 november 2021 een (ongedateerde) lijst met informatiesystemen aan de AP overhandigd, waarop BZ heeft aangegeven welke systemen als kritieke infrastructuur zijn aangemerkt. NVIS is een van die systemen op deze lijst en is dus door BZ inmiddels aangemerkt als kritieke infrastructuur.

79. De AP heeft voorts tijdens onderzoeken ter plaatse geconstateerd dat BZ geen noodplannen heeft opgesteld ter bescherming van de fysieke infrastructuur van het visumproces. De consulaire post Londen, de consulaire post Dublin en CSO hebben verder geen noodstroomvoorziening terwijl paragraaf 11.2.2 van de BIO bepaalt dat apparatuur behoort te worden beschermd tegen stroomuitval. Dit betekent dat BZ, waar het gaat om het opstellen van noodplannen en de bescherming van apparatuur tegen ontregelingen in nutsvoorzieningen, naar het oordeel van de AP niet voldoet aan het bepaalde in artikel 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, sub a, VIS Verordening en BIO-normen 11.1.4 en 11.2.2.

80. BZ heeft in haar zienswijze aangegeven dat BZ uit eigen dreigingsanalyses heeft geconcludeerd dat overstromingsdetectoren en noodstroomvoorzieningen bij de posten London en Dublin niet nodig zijn. De AP volgt deze zienswijze gedeeltelijk. Van overstromingsdetectoren kan worden afgezien na een expliciete risicoafweging. Voor wat betreft stroomuitval vereist de BIO dat apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. Kritieke infrastructuur zoals NVIS moet in hoge mate beveiligd worden, waarbij de onderbreking van de bedrijfsvoering zoveel mogelijk voorkomen dient te worden. BZ heeft onvoldoende uitgelegd waarom NVIS als kritiek systeem geen noodstroomvoorziening nodig heeft.

81. Voorts stelt de AP vast dat er met betrekking tot de ruimten op het consulaat in Londen, waar gewerkt wordt met visumstickers en het NVIS-systeem, er tekortkomingen waren op het gebied van fysieke beveiliging. [VERTROUWELIJK]. Nu er in de praktijk geen beveiligingswaarborgen waren bij het betreden van de zone die extra beveiligd moet zijn, stelt de AP vast dat de fysieke beveiliging van de ruimtes waarin gewerkt wordt aan het visumproces in Londen niet voldeed aan artikel 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, sub a, VIS Verordening en BIO-normen 11.1.1 t/m 11.1.5 en 11.2.2.

82. BZ heeft in haar zienswijze vermeld (en bewijsstukken overhandigd) waaruit blijkt dat er in de afgelopen twee jaar maatregelen zijn genomen om de toegang tot de consulaire afdeling te beveiligen.[73] [VERTROUWELIJK]. De AP stelt vast dat de tekortkomingen op het gebied van fysieke beveiliging op het consulaat London daarmee inmiddels zijn verholpen.

[73] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 5.

83. De AP heeft verder geconstateerd dat wat betreft de werkzaamheden van Verwerker 2 in het kader van het visumproces, van belang is dat medewerkers van Verwerker 2 overwegend plaats- en tijd-onafhankelijk mogen werken. Zodra er buiten de gebouwen van Verwerker 2 wordt gewerkt bieden de fysieke beveiligingswaarborgen op de locaties van Verwerker 2 uiteraard geen soelaas. Het wettelijke vereiste dat persoonsgegevens van visum-aanvragers slechts mogen worden verwerkt in ruimtes met afdoende fysieke beveiliging geldt echter onverminderd. Voor de AP is het onduidelijk hoe gegevens binnen databases van NVIS fysiek worden beschermd in geval van plaats- en tijd-onafhankelijk werken door medewerkers van Verwerker 2 die zowel in Nederland als [VERTROUWELIJK] zijn gestationeerd. De AP heeft tijdens het onderzoek geen documentatie van BZ gekregen die ziet op de fysieke bescherming van NVIS-gegevens bij plaats- en tijd-onafhankelijk werken. BZ moet als verwerkingsverantwoordelijke partij zorg dragen voor passende beveiligingsmaatregelen op het gebied van de fysieke bescherming van NVIS-gegevens, en de doelmatigheid van deze beveiligingsmaatregelen controleren.

84. BZ stelt in haar zienswijze dat er voldoende beveiligingswaarbogen gelden voor medewerkers van Verwerker 2 die thuiswerken. Allereerst weten onbevoegden niet waar Verwerker 2-medewerkers wonen en wordt de verbinding met het netwerk en het management-VPN direct verbroken als een laptop uit een woning gestolen wordt. Het opzetten van de VPN-verbinding werkt middels multi-factor authenticatie en er geldt een streng werknemersbeleid. BZ heeft in dat kader twee reglementen verstrekt.[74]

85. De AP heeft deze reglementen beoordeeld en voor wat betreft plaats- en tijd-onafhankelijk werken staat vermeld dat de medewerker alle nodige voorzorgsmaatregelen moet nemen bij het gebruik van het persoonlijke apparaat in een openbare ruimte, zodat het scherm niet door anderen kan worden bekeken. Welke voorzorgsmaatregelen van een medewerker verwacht worden is echter niet duidelijk. In reactie hierop heeft de AP aan BZ de vraag gesteld of en onder welke voorwaarden medewerkers van Verwerker 2 op openbare plekken met NVIS mogen werken, hoe BZ het thuiswerkbeleid van Verwerker 2 beoordeelt en welke schriftelijke afspraken tussen BZ en Verwerker 2 over de fysieke beveiliging van NVIS bij plaats- en tijd-onafhankelijk werken er gelden. Tot slot heeft de AP enkele auditverklaringen opgevraagd.

86. BZ heeft verklaard dat alle bij de NVIS-dienstverlening betrokken medewerkers van Verwerker 2 het kantoorbeleid voor remote werken toepassen, hetgeen in theorie ook buiten het eigen huis kan plaats vinden.[75] BZ heeft het thuiswerkbeleid van Verwerker 2 als voldoende beoordeeld op basis van het reeds eerder verstrekte werknemersbeleid. De AP stelt echter vast dat in de door BZ overgelegde controlverklaringen, auditverklaringen en de verwerkersovereenkomst het onderwerp plaats- en tijd-onafhankelijk werken niet behandeld/beoordeeld is.[76] Het is daarom voor de AP onduidelijk op basis van welke afwegingen BZ het plaats- en tijd-onafhankelijk werken als voldoende heeft beoordeeld.

[74] Schriftelijke Zienswijze BZ van 15 oktober 2021, bijlage 19 en 20.
[75] E-mail BZ van 10 december 2021.
[76] E-mail BZ van 10 december 2021, bijlage 11.1 t/m 13.3.

87. Op grond van het bovenstaande is de AP van oordeel dat BZ niet heeft aangetoond dat er voldoende waarborgen gelden voor de fysieke beveiliging bij het werken in NVIS in openbare plekken. Zoals vermeld in paragraaf 2.1.2 verwerkt BZ zeer veel - ook - bijzondere persoonsgegevens in NVIS. Dit maakt dat de aard van de verwerking gevoelig is en de negatieve gevolgen voor betrokkenen bij onrechtmatige verwerkingen ingrijpend kunnen zijn. Bovendien heeft BZ het NVIS-systeem als kritieke infrastructuur aangemerkt. Terwijl er bij de consulaire posten en CSO er een pas-toegangssysteem en camerabewaking toegepast wordt, zijn dergelijke waarborgen niet aanwezig in openbare ruimtes.

88. Nu BZ niet heeft aangetoond dat er voldoende waarborgen gelden voor de fysieke beveiliging bij het werken in NVIS in openbare ruimtes en BZ evenmin de doelmatigheid van het beleid hieromtrent heeft gecontroleerd, komt de AP tot de conclusie dat er sprake is van een inbreuk van artikel 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, sub a en k, VIS Verordening.

2.5 Toegangsrechten tot NVIS en personeelsprofielen

2.5.1 Wettelijk kader

89. Artikel 6, lid 1, VIS Verordening bepaalt dat slechts naar behoren gemachtigde personeelsleden van de visumautoriteiten toegang hebben tot het VIS voor het invoeren, wijzigen of verwijderen van visumgegevens. Artikel 32, lid 2, onder f, VIS Verordening schrijft voor dat de nodige maatregelen worden vastgesteld om te waarborgen dat degenen die bevoegd zijn om het VIS te raadplegen, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft en uitsluitend met persoonlijke en unieke gebruikersidentiteiten (**controle op de toegang tot de gegevens**).

90. Artikel 32, lid 2, onder g, VIS Verordening schrijft voor dat de nodige maatregelen worden vastgesteld om te waarborgen dat alle autoriteiten met toegangsrecht tot het VIS profielen opstellen waarin de taken en verantwoordelijkheden worden omschreven van de personen die bevoegd zijn om gegevens in te zien, op te nemen, bij te werken, te wissen en te doorzoeken, en deze profielen desgevraagd en onverwijld ter beschikking te stellen aan de nationale toezichthoudende autoriteiten, als bedoeld in artikel 41 (**personeelsprofielen**). Dit staat ook omschreven in artikel 28, lid 4, sub c, VIS Verordening waarin staat dat “elke lidstaat verantwoordelijk is voor het beheer en de regelingen op grond waarvan naar behoren gemachtigde personeelsleden van de bevoegde nationale autoriteiten overeenkomstig deze verordening toegang krijgen tot het VIS, en de opstelling en regelmatige bijwerking van een lijst van dergelijke personeelsleden en hun profiel”.

91. Artikel 32, lid 2, onder k, VIS Verordening schrijft voor dat de nodige maatregelen worden vastgesteld om de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen te controleren en met betrekking tot de interne controle de nodige organisatorische maatregelen te nemen om ervoor te zorgen dat deze verordening wordt nageleefd (**interne controle**). Hiermee wordt aangesloten bij het algemeen bepaalde in artikel 32 van de AVG.

De BIO verplicht beheers- en implementatiemaatregelen intern toe te delen. Uit het informatiebeveiligingsbeleid moet blijken welke rollen binnen een organisatie verantwoordelijk zijn voor

de te nemen maatregelen. Daarbij is van belang dat beveiligingsprocedures door de desbetreffende verantwoordelijke worden vastgesteld. Van de BIO zijn concreet de volgende bepalingen relevant:

9.2.1	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9.2.2	**Gebruikers toegang verlenen** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
9.2.5	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9.2.6	**Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

2.5.2 Feitelijke bevindingen

92. Tijdens de onderzoeken heeft de AP vragen gesteld aan BZ over de inrichting van de toegangsrechten tot NVIS en de interne controle hierop. Hiervoor heeft de AP de actuele autorisatielijsten, personeelsprofielen, autorisatieprocedures en andere relevante documentatie opgevraagd met betrekking tot het toekennen van toegangsrechten tot de NVIS-omgeving. Het onderzoek van de AP richtte zich op de volgende vragen met betrekking tot toegangsrechten:
    - Beschikt BZ over vastgestelde procedures over het toekennen en controleren van toegangsrechten tot NVIS?
    - Heeft BZ-personeelsprofielen met betrekking tot NVIS opgesteld waarin de taken en verantwoordelijkheden worden omschreven van de personen die bevoegd zijn om gegevens in het systeem in te zien, op te nemen, bij te werken, te wissen en te doorzoeken? Worden NVIS-personeelsprofielen regelmatig bijgewerkt?
    - Worden de toegekende toegangsrechten (autorisatielijsten) regelmatig beoordeeld?

93. De AP heeft dit onderdeel alleen bij de partijen onderzocht die toegang tot de NVIS-omgeving hebben.

2.5.2.1 Procedures over toekennen en controleren van toegangsrechten tot NVIS

Consulaire post Londen

94. BZ heeft drie documenten aan de AP verstrekt die betrekking hebben op autorisatieprocedures in verband met NVIS: (1) 'Handleiding Gegevensbeheer NVIS'[77], (2) een document getiteld 'Autorisatieprocedure NVIS Ambassade Londen'[78] en (3) 'Werkinstructie/procedure: logging autorisaties applicaties'.[79]

95. Het eerste document heeft de vorm van een praktische gebruikershandleiding, waarbij het niet duidelijk is welke verantwoordelijke binnen BZ deze handleiding heeft vastgesteld. In hoofdstuk 3 van het document staat een korte alinea over het toekennen van toegangsrechten tot NVIS, met vermelding van alle praktische stappen in het systeem met betrekking tot de toewijzing en de verwijdering van NVIS-rollen en de wijziging van de autorisatieperiode. Verder wordt vermeld dat het beheer van de taken bij de NVIS-rollen op het departement door Directie Consulaire Zaken en Visumbeleid, cluster Informatiemanagement en -Beheer (hierna: DCM/MB-IB) wordt uitgevoerd. [80] Uit het document blijkt niet bij wie de verantwoordelijkheid is belegd voor het toekennen, wijzigen en controleren van autorisaties.

96. Het tweede document bestaat uit één bladzijde, is ongedateerd en is niet (op een managementniveau) vastgesteld. Het is de AP niet duidelijk geworden of dit stuk opgesteld is naar aanleiding van haar verzoek om inlichtingen, of dat het al eerder bestond. In het document staat beschreven op welke wijze medewerkers van de consulaire post Londen toegang tot NVIS verkrijgen.[81] Verder vermeldt het document: "naast de jaarlijkse controle door functioneel beheer vinden ad-hoc controles (van de autorisaties) op de post plaats.".

97. Het derde document bestaat uit twee bladzijden en ziet op de controle van autorisaties. Daarin staat het volgende vermeld: "Ten behoeve van de controle op logging autorisaties vraagt DCV/MB-IB de posten en RSO's ééns per jaar (na de jaarlijkse overplaatsingsronde) om een check uit te voeren op welke medewerkers welke rollen in bepaalde applicaties zouden moeten hebben…". Het document bevat verder stroomdiagrammen die schematisch een 'check op logging autorisaties applicaties' afbeelden. Het document is generiek en niet-specifiek gericht op de controle van toegangsrechten tot NVIS. Het stuk is ongedateerd en is niet (op een managementniveau) vastgesteld.

98. De AP constateert op basis van de controle bij de consulaire post Londen dat BZ niet over formeel vastgestelde procedures beschikt voor het toekennen, wijzigen en beëindigen van toegangsrechten tot

[77] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018.
[78] Dossierstuk 12, bijlage 04: Autorisatieprocedure NVIS Consulaire post Londen.
[79] Dossierstuk 3, bijlage 6b: Werkinstructie logging en autorisaties applicaties.
[80] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018, p. <16: "..NVIS neemt alle namen van medewerkers automatisch over uit [VERTROUWELIJK]. ICT beheert deze technische functionaliteit. Er kunnen in NVIS dus geen medewerkers handmatig worden toegevoegd. Een medewerker heeft pas toegang tot NVIS, als deze is geautoriseerd voor een bepaalde rol. Rollen bepalen wat een medewerker wel en niet kan doen binnen NVIS. Een rol bestaat uit verscheidene taken. Elke taak geeft toegang tot een specifiek NVIS onderdeel. Beheren van de taken bij de rollen wordt op het departement uitgevoerd door [VERTROUWELIJK].".
[81] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018: "De toegang tot NVIS is gekoppeld aan de BZ-account van de medewerker en de post waar deze medewerker werkzaam is. Wanneer de medewerker de post verlaat wordt de toegang tot NVIS automatisch beëindigd doordat de BZ-account van de medewerker bij de post wordt gesloten of overgeheveld naar een andere post. [VERTROUWELIJK]

NVIS. Evenmin beschikt BZ over vastgestelde procedures om de tot NVIS-verleende toegangsrechten te controleren.

Consulaire post Dublin

99. Voorafgaand aan het onderzoek in Dublin[82] heeft de AP BZ schriftelijk verzocht[83] om autorisatieprocedures NVIS en andere relevante documentatie met betrekking tot de inrichting van toegangsrechten tot NVIS. BZ heeft een document getiteld 'Autorisatieprocedure NVIS Ambassade Dublin'[84] aan de AP verstrekt.

100. Het document bestaat uit een halve bladzijde tekst, is ongedateerd en is niet op (managementniveau) vastgesteld. Het is de AP niet duidelijk geworden of dit stuk opgesteld is naar aanleiding van haar verzoek om inlichtingen, of dat het al eerder bestond. In het overgelegde document wordt beschreven dat de leidinggevende een aanvraag bij [VERTROUWELIJK] worden toegekend. De toegang tot NVIS is gekoppeld aan [VERTROUWELIJK]. De [VERTROUWELIJK] regelt mutaties van de NVIS-accounts en rollen. Verder wordt de jaarlijkse controle van de toegekende autorisaties door [VERTROUWELIJK] uitgevoerd.

101. De AP stelt naar aanleiding van haar onderzoek bij de consulaire post Dublin vast dat BZ niet over formele procedures beschikt voor het toekennen, wijzigen en beëindigen van toegangsrechten tot NVIS en voor het controleren van de verleende autorisaties tot NVIS.

CSO Den Haag

102. Tijdens het onderzoek van de AP hebben de geïnterviewde CSO-medewerkers een toelichting gegeven over de werkwijze die de CSO volgt bij het verkrijgen van de toegangsrechten tot NVIS.[85] [VERTROUWELIJK]

103. Bij het verlenen van toegangsrechten tot NVIS maakt de CSO gebruik van de 'Handleiding Gegevensbeheer NVIS'[86] (de beschrijving van dit document is te vinden in paragraaf 2.5.2). Tevens beschikt de CSO over een werkinstructie[87] [VERTROUWELIJK]. De (ongedateerde) werkinstructie bestaat uit 13 ongenummerde pagina's. Het is onbekend of het document op managementniveau is vastgesteld. Uit het document blijkt niet wie formeel verantwoordelijk is voor het verlenen van autorisaties, het doorvoeren van wijzigingen in de accounts, het toekennen van NVIS-rollen en de controles hierop. De AP constateert naar aanleiding van haar onderzoek bij de CSO dat niet gebleken is dat BZ beschikt over

[82] Dossierstuk 27: Verslag van Ambtshandelingen OTP consulaire post Dublin.
[83] Dossierstuk 25: Aankondiging OTP consulaat Dublin en Informatieverzoek AP van 19 december 2019.
[84] Dossierstuk 26, bijlage 4.1: Medewerker - Rollen – Dublin.
[85] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september 2019.
[86] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018.
[87] Dossierstuk 14, bijlage 23.1: Werkinstructie toewijzen rollen NVIS bij CSO.

formele procedures met betrekking tot het toekennen, wijzigen en beëindigen van toegangsrechten en de controle van de verleende toegangsrechten tot NVIS.

Verwerker 2

104. Naar aanleiding van het onderzoek[88] dat de AP bij Verwerker 2 heeft uitgevoerd, zijn de volgende documenten met betrekking tot autorisaties verstrekt: (1) een procedure voor het interne access management systeem,[89] (2-4) autorisatieprocedure van Cloud Infrastructure Management, bestaande uit drie documenten[90], en een autorisatielijst[91] met namen van medewerkers van Verwerker 2 die toegangsbevoegdheid hebben tot het NVIS-platform en databases.

105. De overgelegde autorisatieprocedures (1 tot en met 4) beschrijven de werkwijze die bij Verwerker 2 wordt toegepast bij het aanmaken, wijzigen en/of verwijderen van accounts van medewerkers. Verder bevatten de procedures schematische weergaven van de (praktische) stappen die relevant zijn voor het aanvragen, wijzigen en verwijderen van toegangsrechten tot de systemen waarmee Verwerker 2 werkt. Daarnaast gaan de autorisatieprocedures in op de typen accounts waarover medewerkers kunnen beschikken. Door een nadere toelichting door BZ tijdens de zienswijzefase is het voor de AP voldoende duidelijk geworden wat de relatie is tussen deze typen accounts en verantwoordelijkheden enerzijds en de NVIS-omgeving anderzijds.[92]

2.5.2.2 Personeelsprofielen

Consulaire post Londen, consulaire post Dublin en CSO

106. BZ heeft een generiek document verstrekt, getiteld 'NVIS profielen'.[93] Het is een tabel waarin de toe te kennen NVIS-rollen staan in relatie tot taken die onder de toegekende NVIS-rol vallen. De taken zijn summier aangeduid en het is onduidelijk met welke concrete handelingen (bijv. gegevens inzien, opnemen, bijwerken, wissen en doorzoeken) in de NVIS-context zij gepaard gaan. Verder is de relatie tussen de functie van de medewerker en de toegekende NVIS-rollen en taken niet omschreven.

107. De AP heeft BZ verzocht om personeelsprofielen te verstrekken[94] die betrekking hebben op de medewerkers van de CSO. BZ heeft een sjabloon tekst[95] overgelegd met resultaatgebieden en competenties, die mogelijk wordt gebruikt ten behoeve van de beschrijving van vacatures bij de CSO. De beschrijving opgenomen in dit document ziet niet op de taken en verantwoordelijkheden in relatie tot handelingen in NVIS.

108. De AP heeft tijdens het onderzoek vastgesteld dat BZ geen personeelsprofielen heeft opgesteld waarin de taken en verantwoordelijkheden worden omschreven van de medewerkers bij de consulaire post Londen,

[88] Dossierstuk 17: Verslag van Ambtshandelingen OTP Verwerker 2 1 november 2019.
[89] Dossierstuk 17, bijlage 8: [VERTROUWELIJK].
[90] Dossierstuk 18, bijlage 3: [VERTROUWELIJK]; Dossierstuk 63: [VERTROUWELIJK]; en Dossierstuk 18, bijlage 1: [VERTROUWELIJK].
[91] Dossierstuk 21, bijlage 4: Autorisatielijst NVIS.
[92] Zienswijze BZ 14 oktober 2021, p. 8 en brief BZ aan AP van 19 november 2021, bijlage 1 Gespreksverslag, p. 33 en 34.
[93] Dossierstuk 5, bijlage 1: NVIS profielen.
[94] Dossierstuk 4: Informatieverzoek AP van 13 juni 2019.
[95] Dossierstuk 16, bijlage 2.1: Functieprofielen CSO visa, versie 15 oktober 2019.

consulaire post Dublin en CSO die bevoegd zijn om gegevens in NVIS in te zien, bij te werken, te wissen en te doorzoeken.

2.5.2.3 Controle van toegangsrechten tot NVIS

Consulaire post Londen

109. BZ heeft een actuele autorisatielijst[96] van alle medewerkers van de consulaire post Londen aan de AP overgelegd.

110. Ten tijde van het onderzoek waren bij de consulaire post Londen 17 medewerkers werkzaam met de toegangsrechten tot NVIS. Aan deze medewerkers zijn de volgende (meerdere) NVIS-rollen toegekend: [VERTROUWELIJK].

De meeste medewerkers hadden meer dan twee NVIS-rollen, met een maximum van zes NVIS-rollen waarover één medewerker beschikte.

111. De AP heeft de rol [VERTROUWELIJK] nader gecontroleerd. Op de autorisatielijst die BZ aan de AP heeft verstrekt was één medewerker (hierna: medewerker X) vermeld met deze NVIS-rol. [VERTROUWELIJK]. Medewerker X werkte al langere tijd niet meer bij de Consulaire afdeling, maar wel als [VERTROUWELIJK] bij een andere afdeling van de ambassade. Voor de huidige werkzaamheden heeft medewerker X geen toegang tot NVIS nodig. Tijdens de AP-controle is gebleken dat het inloggen in het systeem in de rol van [VERTROUWELIJK] nog steeds mogelijk was. Na het inloggen kon medewerker X actuele NVIS-gegevens inzien en muteren.

112. Uit de verstrekte autorisatielijst blijkt tevens dat sommige medewerkers van de consulaire post Londen over een autorisatie beschikten met onderling onverenigbare NVIS-rollen,[97] zoals die van [VERTROUWELIJK]. In NVIS was geen motivering opgenomen waarin de toekenning van deze conflicterende rollen was toegelicht.

113. Ten tijde van het onderzoek bij de consulaire post Londen heeft BZ tevens verklaard dat de tot NVIS toegekende autorisaties ééns per jaar worden gecontroleerd door [VERTROUWELIJK]. Op de consulaire post Londen is [VERTROUWELIJK] verantwoordelijk voor het doorgeven van alle mutaties in de NVIS-toegangsrechten.[98] De operationeel manager was niet aanwezig tijdens het onderzoek en het is onbekend hoe vaak de mutaties met betrekking tot NVIS toegangsrechten aan [VERTROUWELIJK] worden doorgegeven. BZ heeft geen documenten verstrekt[99] waaruit blijkt wanneer de laatste controle van de autorisaties en NVIS-rollen bij de consulaire post Londen heeft plaatsgevonden.

114. De AP stelt vast dat ten tijde van haar controle bij de consulaire post Londen een medewerker ten onrechte over toegangsrechten tot NVIS beschikte. Deze medewerker was ten tijde van het AP-onderzoek aangesteld in een andere functie bij de ambassade, waarvoor het gebruik van NVIS niet nodig was. Verder

[96] Dossierstuk 3, bijlage 7: Overzicht NVIS-autorisaties ZMA Londen.
[97] De onderling onverenigbare NVIS-rollen staan opgesomd in Dossierstuk 12, bijlage 06a: Taken - rollen - onverenigbaar- NVIS.
[98] Dossierstuk 7: Verslag van Ambtshandelingen consulaire post Londen.
[99] Dossierstuk 10: Informatieverzoek AP van 12 juli 2019.

beschikten diverse medewerkers van de consulaire post Londen over NVIS-rollen die onderling onverenigbaar zijn. De AP heeft tijdens het onderzoek geen motivering voor de onverenigbare rollen in NVIS aangetroffen en documentatie ontvangen waaruit blijkt wanneer de laatste controle van de autorisaties en NVIS-rollen heeft plaatsgevonden.

Consulaire post Dublin

115. BZ heeft een overzicht van de verleende autorisaties bij de consulaire post Dublin aan de AP overgelegd.[100] Bij de consulaire post waren ten tijde van het onderzoek zes medewerkers werkzaam die over toegangsrechten tot NVIS beschikten, in de volgende toegekende NVIS-rollen: [VERTROUWELIJK].
Twee medewerkers beschikten over NVIS-rollen [VERTROUWELIJK] die onderling onverenigbaar zijn. De toekenning van deze conflicterende rollen in NVIS is ten tijde van het onderzoek door of namens BZ niet nader gemotiveerd.

116. Tijdens het onderzoek van de AP hebben de medewerkers van de consulaire post Dublin verklaard dat één keer per jaar de lijst met alle toegekende autorisaties bij de consulaire post wordt gecheckt. Daarnaast voert de afdeling Functioneel beheer in Den Haag controles uit van de toegekende autorisaties.[101]

CSO

117. De CSO heeft tijdens het onderzoek verklaard dat de toegekende NVIS-rollen toegespitst zijn op de functiescheiding. De rollen van registreren en beslissen zijn onderling onverenigbaar volgens het functioneel ontwerp van de NVIS-applicatie.[102]
[VERTROUWELIJK][103]

De AP heeft geen motivering in NVIS aangetroffen met betrekking tot [VERTROUWELIJK].

118. Uit het aan de AP verstrekte overzicht 'NVIS rolverdeling per functie'[104] blijkt dat er bij de CSO 79 medewerkers toegang hebben tot NVIS. Op de lijst staan de volgende functies vermeld: [VERTROUWELIJK].

Aan deze functies zijn drie of meer NVIS-rollen toegekend. Met betrekking tot de rol [VERTROUWELIJK] blijkt uit het onderzoek van de AP dat deze rollen sinds enkele jaren niet meer in gebruik zijn.[105]

119. Uit het bovengenoemde overzicht blijkt ook dat sommige NVIS-rollen, waarover sommige medewerkers van de CSO beschikken, als onderling onverenigbaar zijn aangemerkt.[106] Het gaat hierbij om de volgende NVIS-rollen: [VERTROUWELIJK].

[100] Dossierstuk 26, bijlage 4.1: Medewerker - Rollen – Dublin.
[101] Dossierstuk 27: Verslag van Ambtshandelingen OTP consulaire post Dublin.
[102] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september 2019.
[103] Dossierstuk 16, bijlage 3.1: Proces Beschrijving Afdeling Registratie, versie 1 augustus 2019.
[104] Dossierstuk 14, bijlage 23.2: NVIS rolverdeling per functie.
[105] Dossierstuk 5, bijlage 2 en 3 en dossierstuk 11.
[106] Dossierstuk 14, bijlage 23.2: NVIS rolverdeling per functie.

De CSO heeft tijdens het onderzoek geen stukken aan de AP overgelegd die de inhoudelijke motivering bevatten over de conflicterende NVIS-rollen.

120. Tijdens het onderzoek op 18 juli 2019 heeft de CSO verklaard dat de controle op het toekennen van autorisaties volgens een intern controleplan plaatsvindt. De toegekende autorisaties worden twee keer per jaar door [VERTROUWELIJK] gecontroleerd. Daarnaast wordt ééns per jaar een controle uitgevoerd door [VERTROUWELIJK].
[VERTROUWELIJK][107]

De CSO heeft tevens op 8 augustus 2019 de managementrapportage april 2018[108] aan de AP overgelegd, waaruit blijkt dat de toegekende autorisaties tot NVIS, inclusief de NVIS-rollen werden gecontroleerd. De laatste controle vond plaats in 2018.

121. De AP stelt vast dat de toegekende autorisaties voor toegang tot NVIS bij de CSO worden gecontroleerd. Verder stelt de AP vast dat er bij meerdere medewerkers bij de CSO sprake is van de toekenning van onderling onverenigbare NVIS-rollen, en dat [VERTROUWELIJK]medewerkers standaard over toegangsrechten beschikken met [VERTROUWELIJK] in NVIS. De motivering van de onderling onverenigbare rollen ontbreekt in NVIS. Tot slot hadden enkele medewerkers van CSO een rol die niet meer in gebruik was.

Verwerker 2

122. Ten tijde van het onderzoek is de AP tot de conclusie gekomen dat BZ geen documentatie heeft verstrekt waaruit (voldoende) blijkt welke afspraken met Verwerker 2 zijn gemaakt over de procedures ten aanzien van toegangsrechten tussen de verwerkingsverantwoordelijke en verwerker.

123. BZ stelt in haar zienswijze dat de afspraken tussen haar en Verwerker 2 over de toegangsrechten tot NVIS volgen uit overeenkomsten tussen BZ en Verwerker 2. BZ heeft in dat verband ook een kwartaalrapportage over de controle op deze toegangsrechten van Verwerker 2 overgelegd.[109] De AP heeft deze documenten beoordeeld en komt tot de conclusie dat op dit punt geen overtreding kan vaststellen van artikel 32, lid 2, onder k, VIS Verordening en zal dit dus niet verder behandelen bij de onderstaande juridische beoordeling.

2.5.3 Juridische beoordeling

Consulaire posten Londen en Dublin en CSO

124. De AP constateert naar aanleiding van haar onderzoek dat de consulaire posten Londen en Dublin en de CSO toegang hebben tot NVIS.
[VERTROUWELIJK]

[107] Dossierstuk 14: Reactie BZ van 8 augustus 2019 op informatieverzoek AP van 25 juli 2019. Schriftelijk antwoord op de vraag van de AP: "Wie is formeel verantwoordelijk voor controle op het NVIS-gebruik bij het ministerie van Buitenlandse Zaken en specifiek bij de CSO?'
[108] Dossierstuk 14, bijlage 24.1: Managementrapportage visa april 2018, versie 30 mei 2018.
[109] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 8.

Procedures over toekennen en controleren van toegangsrechten tot NVIS-omgeving

125. Bij het toekennen van toegangsrechten, inclusief NVIS-rollen, maakt BZ gebruik van de werkwijze die in de praktijk vrijwel identiek is voor de medewerkers van de onderzochte consulaire posten en de CSO in Den Haag. De AP stelt vast dat BZ niet over formele registratie- en afmeldingsprocedures beschikt ten aanzien van de toewijzing aan medewerkers van toegangsrechten tot NVIS. De AP overweegt daarbij dat er weliswaar gebruik wordt gemaakt van een handleiding tot het systeem,[110] waarin allerlei praktische stappen zijn toegelicht, maar dat dit een niet formeel vastgestelde gebruikerstoegangsverleningsprocedure omvat met betrekking tot het registreren en afmelden van autorisaties. De andere documenten[111] die als autorisatieprocedures door BZ zijn verstrekt, betreffen een ongedateerde, summiere beschrijving van de werkwijze die BZ hanteert bij het autoriseren van medewerkers van de consulaire posten en zijn geen formeel vastgestelde registratie- en afmeldingsprocedures. De AP stelt vast dat dat BZ op dit punt in strijd handelt met artikel 32, lid 1, AVG en nader uitgewerkt in BIO-normen 9.2.1 en 9.2.2.

126. BZ heeft in haar zienswijze aangegeven dat de bestaande werkinstructies uiterlijk 1 januari 2022 formeel worden vastgesteld.[112] De AP heeft dat document op 9 januari 2022 ontvangen, en is van oordeel dat hierin de procedure omtrent het aanvragen, wijzigen en stopzetten van toegangsrechten in NVIS voldoende is beschreven.[113]

Personeelsprofielen

127. De AP heeft tijdens het onderzoek vastgesteld dat BZ geen personeelsprofielen heeft opgesteld waarin de taken en verantwoordelijkheden worden omschreven van de medewerkers van de consulaire posten Londen en Dublin die bevoegd zijn om in NVIS gegevens in te zien, op te nemen, bij te werken, te wissen en te doorzoeken. Ten aanzien van de verstrekte personeelsprofielen[114] van de medewerkers bij de CSO, is de AP van oordeel dat deze profielen onvoldoende inzicht geven in de taken en verantwoordelijkheden van de CSO-medewerkers die bevoegd zijn om in NVIS gegevens te verwerken.

128. BZ stelt in haar zienswijze dat de aan de functies toegekende toegangsrechten wel zijn bepaald op basis van taken en verantwoordelijkheden.[115] Naar aanleiding hiervan heeft de AP opnieuw documentatie opgevraagd waaruit dit zou moeten blijken. BZ heeft een autorisatiematrix d.d. 7 januari 2014 verstrekt.[116] De AP komt op basis hiervan tot het oordeel dat BZ tóch over personeelsprofielen beschikt die voldoende inzicht geven in de taken en verantwoordelijkheden van daartoe bevoegde medewerkers. Hieruit volgt dat BZ naar het oordeel van de AP op dit punt in overeenstemming heeft gehandeld met artikel 32, lid 2, onder g, VIS Verordening. Deze bepaling schrijft tevens voor dat personeelsprofielen voorhanden moeten zijn en op aanvraag van de AP verstrekt moeten worden.[117] De AP moet wel concluderen dat dat BZ ten tijde van het onderzoek door AP niet de volledige personeelsprofielen heeft verstrekt, op het moment dat de AP daar om verzocht. Daaruit volgt dat BZ op dat punt in strijd heeft gehandeld met artikel 32, lid 2, onder g, VIS Verordening.

[110] Dossierstuk 3, bijlage 1 en Dossierstuk 26, bijlage 1.1: Handleiding Gegevensbeheer NVIS februari 2018.
[111] Dossierstuk 12, bijlage 4: Autorisatieprocedure NVIS consulaire post Londen; en Dossierstuk 26, bijlage 3.1: Autorisatieprocedure NVIS consulaire post Dublin.
[112] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 6.
[113] E-mail BZ aan de AP van 9 januari 2022, BZ proces NVIS autorisatie.
[114] Dossierstuk 16, bijlage 2.1: Functieprofielen CSO visa.
[115] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 7.
[116] E-mail BZ van 10 december 2021, bijlage 14.
[117] Gelet op artikel 41, lid 1, VIS-Verordening is de AP de bevoegde toezichthouder

Controle van toegangsrechten tot NVIS

129. De AP heeft allereerst vastgesteld dat BZ niet over formele procedures beschikt ten aanzien van het periodiek controleren van de toegekende toegangsrechten tot NVIS en NVIS-rollen. Uit de door BZ verstrekte documentatie[118] blijkt dat de toegekende autorisaties één keer per jaar door [VERTROUWELIJK] worden gecontroleerd. Daarnaast is verklaard dat er interne controles plaatsvinden bij de consulaire posten Londen en Dublin en bij de CSO.[119]

130. De AP overweegt dat zij tijdens het onderzoek geen documenten heeft ontvangen waaruit de frequentie blijkt van de controles door [VERTROUWELIJK]. Evenmin heeft BZ aangetoond wanneer de meest recente controle is uitgevoerd. Ten aanzien van de interne controles overweegt de AP dat in geval van de consulaire post Londen geen documenten zijn verstrekt die zien op de interne controles van de toegekende autorisaties. Ten aanzien van de CSO en de consulaire post Dublin constateert de AP aan de hand van de verstrekte informatie[120] dat er enkele interne controles met betrekking tot autorisaties in het verleden hebben plaatsgevonden. De laatste interne controle bij de CSO vond plaats in april 2018. De consulaire post Dublin voert minstens één keer per jaar controle uit; de laatste controle is in 2019 gedaan.[121]

131. Voorts heeft de AP vastgesteld dat meerdere medewerkers van CSO en een medewerker van de consulaire post Londen over NVIS-rol(len) beschikten die zij niet nodig hadden en van sommige rollen bleek dat die al geruime tijd niet meer in gebruik waren. Dit wijst op het feit dat de toegekende toegangsrechten tot NVIS en NVIS-rollen onvoldoende zijn gecontroleerd.

132. BZ heeft tijdens de zienswijzezitting verklaard dat [VERTROUWELIJK] bij consulaire posten verantwoordelijk zijn voor de controle op toegangsrechten tot NVIS. De eenmalige najaarscontrole van [VERTROUWELIJK] fungeert als vangnet.[122] BZ heeft verder aangegeven de procedure voor controle van toegangsrechten formeel te zullen vaststellen.

133. In reactie hierop heeft de AP documentatie bij BZ opgevraagd van de controles die [VERTROUWELIJK] van de consulaire post London en Dublin hebben uitgevoerd op toegangsrechten tot NVIS van 2018 tot en met 2021. BZ heeft als antwoord hierop het volgende verstrekt: autorisatielijsten (uit 2019, 2020 en 2021), de intrekking van toegangsrechten van één medewerker in 2019 en twee evaluatierapporten die niet meer dan een algemeen beeld geven van de doorlichting van consulaire posten (uit 2018 en 2019). De door BZ overgelegde documenten brengen de AP niet tot een ander oordeel. De AP stelt vast dat BZ niet heeft aangetoond dat de operationele managers van de consulaire post London en Dublin regelmatig controles hebben uitgevoerd op de toegangsrechten tot NVIS.

[118] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018; Dossierstuk 12, bijlage 4: Autorisatieprocedure NVIS Consulaire post Londen; en Dossierstuk 26, bijlage 3.1: Autorisatieprocedure NVIS consulaire post Dublin.
[119] Dossierstuk 7: Verslag van Ambtshandelingen consulaire post Londen; Dossierstuk 27: Verslag van Ambtshandelingen consulaire post Dublin; en Dossierstuk 11: Verslag van Ambtshandelingen CSO 18 juli 2019 en 12 september 2019.
[120] Dossierstuk 14, bijlagen 24.1 en 24.2: Managementrapportage visa apr 2018 en Managementrapportage visa sep 2018; en Dossierstuk 27, bijlage 6: 6. Correspondence over aanpassen rollen NVIS.
[121] Dossierstuk 27: Verslag van Ambtshandelingen OTP consulaat Dublin.
[122] Brief BZ aan AP van 19 november 2021, bijlage 1 Gespreksverslag, p. 30.

134. Voor wat betreft de door BZ verstrekte procedure over de controle op toegangsrechten constateert de AP dat hierin het proces rondom de eenmalige najaarscontrole van [VERTROUWELIJK] is beschreven.[123] De AP stelt vast dat in deze procedure geen duidelijkheid wordt verschaft over de vraag hoe BZ ervoor zorgt dat toegangsrechten *regelmatig* gecontroleerd worden. De eenmalige najaarscontrole fungeert, zoals BZ stelt, als een vangnet. Gezien de soort gegevensverwerkingen in NVIS acht de AP een jaarlijkse controle onvoldoende om te waarborgen dat alleen bevoegde medewerkers toegang hebben tot dit systeem. Deze werkwijze mitigeert het risico onvoldoende dat een van functie wisselende medewerker maandenlang ten onrechte toegang houdt tot NVIS, [VERTROUWELIJK].

135. De AP heeft voorts vastgesteld dat een medewerker bij de consulaire post Londen ten onrechte over toegangsrechten tot NVIS beschikte in de rol van [VERTROUWELIJK], en hierdoor in NVIS gegevens kon inzien en muteren. Deze medewerker was aangesteld in een andere functie bij de ambassade, waarvoor het gebruik van NVIS niet nodig was. BZ heeft in haar zienswijze gesteld dat de [VERTROUWELIJK]-applicatie ten tijde van het onderzoek gebreken vertoonde, waardoor de rol [VERTROUWELIJK] nog behouden moest blijven voor het geval de [VERTROUWELIJK]-applicatie niet zou functioneren. Dit betoog slaagt niet. Een medewerker die geruime tijd niet meer op de consulaire afdeling werkzaam is, behoort geen toegang tot NVIS te hebben. Voor wat betreft de rol [VERTROUWELIJK] volgt de AP de zienswijze van BZ dat de bevinding hierover een onjuiste bronvermelding had. De desbetreffende bevinding had betrekking op medewerkers van CSO en heeft de AP hierboven met de juiste bronvermelding gecorrigeerd.

136. De AP heeft tot slot tijdens het onderzoek vastgesteld dat een motivering van toegekende onverenigbare rollen binnen NVIS ontbreekt. BZ stelt in haar zienswijze dat in voorkomende gevallen niet voorkomen kan worden dat conflicterende rollen worden toegekend aan een persoon. Dit kan bijvoorbeeld gaan om kleinere posten waar plotseling een medewerker uitvalt. Volgens BZ is de motivering van conflicterende rollen wel gedocumenteerd. De AP heeft naar aanleiding hiervan documentatie opgevraagd over de verantwoordelijkheid en motivering rondom het toewijzen van onverenigbare rollen. Op basis hiervan stelt de AP vast dat BZ meerdere voorbeelden heeft laten zien waaruit blijkt dat BZ onverenigbare rollen in het verleden heeft gemotiveerd.[124] Voor wat betreft dit punt volgt de AP de zienswijze van BZ. De AP heeft echter geen beleid kunnen inzien waaruit blijkt hoe BZ omgaat met onverenigbare rollen en hoe BZ onverenigbare rollen definieert. In de NVIS Handleiding gegevensbeheer staat alleen dat de onverenigbare rollen in NVIS momenteel niet zijn ingesteld.[125] Beleid omtrent functiescheiding is bij uitstek geschikt om op te nemen in het beveiligingsbeleid zoals bedoeld in paragraaf 2.3.

137. Gelet op het bovenstaande is de AP van oordeel dat BZ, ten aanzien van procedures over toegangsrechten tot de NVIS-omgeving en de controle daarop, in strijd handelt met artikel 32, lid 1 AVG en nader uitgewerkt in 32, lid 2, onder f en k, VIS Verordening en BIO-normen 9.2.1, 9.2.2, 9.2.5 en 9.2.6. (en relevante normen uit de BIO over de Plan-Do-Check-Act cyclus).[126]

[123] E-mail BZ aan de AP van 9 januari 2022, BZ proces NVIS autorisatie.
[124] E-mail BZ van 10 december 2021, bijlage 20 en 20.1 en de schriftelijke Zienswijze BZ van 15 oktober 2021, bijlage 22.
[125] Dossierstuk 3, bijlage 1: Handleiding Gegevensbeheer NVIS februari 2018, p. 16.
[126] Dit betekent dat er regelmatig moet worden nagegaan of het beveiligingsbeleid nog nageleefd wordt in de praktijk en of de maatregelen nog voldoen. Mochten onvolkomenheden aan het licht komen, dan vereist het principe Plan-Do –Check-Act uit de BIO –kort gezegd- dat fouten

2.6 Controle van NVIS-gebruik: logbestanden

2.6.1 Wettelijk kader

138. De verplichting om logbestanden aan te houden en regelmatig te controleren, vormt een essentieel onderdeel van de voorschriften voor informatiebeveiliging. Op die manier kan een organisatie er zicht op houden welke medewerker wanneer en met welk doel bepaalde informatie raadpleegt of wijzigt. Het is daarnaast noodzakelijk dat periodiek monitoring van de vastgelegde logbestanden plaatsvindt om ongebruikelijke patronen te kunnen detecteren en bijvoorbeeld te kunnen nagaan of ongeoorloofde toegang plaatsvindt tot de gegevens.

139. In artikel 32, lid 2, onder i en k, VIS Verordening is bepaald dat BZ moet kunnen nagaan en vaststellen welke persoonsgegevens wanneer, door wie en voor welk doel in NVIS zijn verwerkt. BZ moet ook de doelmatigheid van deze beveiligingsmaatregelen controleren en met betrekking tot de interne controle de nodige organisatorische maatregelen nemen. Artikel 32, lid 2, onder f, VIS Verordening schrijft voor dat degenen die bevoegd zijn om het VIS te raadplegen, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend met persoonlijke en unieke gebruikersidentiteiten en geheime toegangsprocedures (controle op de toegang tot de gegevens).

140. De BIO-normen schrijven voor dat BZ logbestanden met de registratie van activiteiten van NVIS-gebruikers moet bijhouden en deze logbestanden regelmatig moet beoordelen. De BIO-normen specificeren welke informatie over het NVIS-gebruik minimaal in een logbestand dient te worden geregistreerd. BZ moet ook een overzicht hebben van alle logbestanden die in de context van NVIS worden gegenereerd. In de BIO zijn met name de volgende voorschriften relevant:

12.4.1	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12.4.1.1	Een logregel bevat minimaal: a. de gebeurtenis; b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c. het gebruikte apparaat; d. het resultaat van de handeling; e. een datum en tijdstip van de gebeurtenis.
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.

hersteld worden en dat het beleid zodanig aangepast wordt dat de betreffende problemen zich een volgende keer niet meer voor zullen doen. De hierboven beschreven resultaten van de controle ter plaatse door inspecteurs van de AP tonen aan dat dit niet is gebeurd ten aanzien van autorisaties en rollenbeheer. Daarmee ontbreekt een passende interne controle op het gebied van toegangsbeveiliging. Mogelijk ontstaat hiermee het risico op toegang tot NVIS voor onbevoegden, zoals bedoeld in artikel 32 lid 2 onder b VIS Verordening.

2.6.2 Feitelijke bevindingen

141. Om de naleving van de wettelijke voorschriften met betrekking tot logbestanden te controleren heeft de AP een steekproef van de logbestanden bij BZ opgevraagd. Deze logbestanden bevatten logs van de consulaire posten, van CSO en van Verwerker 2. Tevens heeft de AP tijdens de onderzoeken ter plaatse[127] vragen gesteld over de inrichting van de logging en de interne controle hierop door BZ. Voorts heeft de AP de opgevraagde logbestanden gecontroleerd en deze vergeleken met de corresponderende autorisatielijsten die betrekking hebben op dezelfde periode.

Logging van NVIS-gebruik bij consulaire posten Londen en Dublin

142. [VERTROUWELIJK]

143. [VERTROUWELIJK][128]

Analyses van logbestanden

144. De AP heeft twee logbestanden opgevraagd met betrekking tot het NVIS-gebruik door de medewerkers van de consulaire post Londen. Het eerste bestand (hierna te noemen: Log 1) betreft het logbestand van 4 juli 2019, tussen 9.00 en 12.00 uur. Dit tijdvak valt samen met het onderzoek van de AP ter plaatse. Het tweede bestand (hierna: Log 2) ziet op de periode van 1 april tot en met 4 juli 2019.

145. [VERTROUWELIJK][129]

146. [VERTROUWELIJK] [130]

[127] Onderzoeken ter plaatse bij het consulaire post Londen (2 en 4 juli 2019), de CSO Den Haag (18 juli en 12 september 2019), Verwerker 2 (1 november 2019) en het consulaire post Dublin (22 en 23 januari 2020).
[128] Schriftelijke Zienswijze BZ van 15 oktober 2021, bijlage 2 onder nummer 6.3.
[129] Dossierstuk 12, bijlagen 40a en 40b: Logging gebruik NVIS, versie 25 juli 2019 en Toelichting.
[130] Dossierstuk 16, bijlage 8.1: LON_01April2019_04July2019_Overzicht.

Logging van NVIS-gebruik bij CSO Den Haag

147. Tijdens het onderzoek ter plaatse bij de CSO[131] heeft de AP interviews afgenomen bij de medewerkers van BZ over de verschillende aspecten van de beveiliging ten aanzien van NVIS, waarbij het onderwerp 'logging van NVIS' is onderzocht. Tevens heeft de AP aanvullende documentatie over dit onderwerp bij BZ opgevraagd[132] en geanalyseerd. Daarnaast heeft de AP analyses van logbestanden uitgevoerd.

<u>Proces van logging en controle van logbestanden</u>

148. [VERTROUWELIJK][133]

149. [VERTROUWELIJK] [134] [135]

[131] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september 2019.
[132] Dossierstuk 13: Informatieverzoek AP van 25 juli 2019; en Dossierstuk 17: Informatieverzoek AP van 1 oktober 2019.
[133] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september 2019.
[134] Dossierstuk 13: Informatieverzoek AP van 25 juli 2019.
[135] Dossierstuk 14, bijlage 18.1: Verantwoordelijkheid controle NVIS-gebruik.

150. De AP heeft bij BZ (uitgebreide) documentatie op het gebied van de beveiliging opgevraagd en geanalyseerd op relevante informatie over logging. Hierbij heeft de AP de focus gelegd op informatie over het loggen van de handelingen binnen het NVIS-platform, met name hoe het logproces en controle hierop zijn ingericht, welke logbestanden worden gegenereerd, en hoe controle van logbestanden plaatsvindt. Het betreft de volgende documenten: [VERTROUWELIJK];[136] [VERTROUWELIJK];[137] [VERTROUWELIJK]; [138] [VERTROUWELIJK];[139] [VERTROUWELIJK];[140] [VERTROUWELIJK].[141]

151. [VERTROUWELIJK]

Analyses van logbestanden

152. Verder heeft de AP bij BZ logbestanden NVIS opgevraagd waarin de NVIS-handelingen van de medewerkers van de CSO zijn vastgelegd. BZ heeft de volgende logbestanden aan de AP overgelegd die betrekking hebben op de volgende periodes:
(1) 1 september 2018 tot en met 30 november 2018; (hierna: Log 3);[142]
(2) 1 april tot en met 18 juli 2019, (hierna: Log 4);[143]
(3) op 12 september 2019 (hierna: Log 5).[144]

153. [VERTROUWELIJK]

154. [VERTROUWELIJK][145]

[136] Dossierstuk 14, bijlage 14.1: [VERTROUWELIJK]
[137] Dossierstuk 12, bijlage 44b: [VERTROUWELIJK]
[138] Dossierstuk 14, bijlage 16.1: [VERTROUWELIJK]
[139] Dossierstuk 14, bijlage 16.2: [VERTROUWELIJK]
[140] Dossierstuk 14, bijlage 19.1: [VERTROUWELIJK]
[141] Dossierstuk 14, bijlage 19.2: [VERTROUWELIJK]
[142] Dossierstuk 16, bijlage 9.1: CSO_01Sept2018_30Nov2018_Overzicht.
[143] Dossierstuk 16, bijlage 9.2: CSO_01April2019_18Juli2019_Overzicht.
[144] Dossierstuk 16, bijlage 9.3: CSO_12Sept2019_Overzicht.
[145] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 10 en 11.

Verwerker 2

155. [VERTROUWELIJK]

156. [VERTROUWELIJK][146]

157. [VERTROUWELIJK][147]

158. De AP heeft tot slot enkele logbestanden van Verwerker 2 geanalyseerd. De AP stelt vast dat zij, door het gebrek aan voldoende bewijs over de feitelijk situatie in combinatie met de toelichting van BZ, voor wat betreft de inhoud van deze logbestanden geen overtreding kan vaststellen en zal dit dus niet verder behandelen bij de onderstaande juridische beoordeling.[148]

2.6.3 Juridische beoordeling

159. De AP heeft beoordeeld in hoeverre BZ passende maatregelen heeft genomen op het gebied van logging van de NVIS-omgeving.

160. De AP constateert dat er logbestanden worden bijgehouden met betrekking tot NVIS. In de logbestanden staan de namen van medewerkers geregistreerd en slechts een zeer beperkt aantal andere gegevens met betrekking tot handelingen in NVIS, zoals een aanduiding voor sommige stappen in het kader van het visumproces (bijv. [VERTROUWELIJK]).

[146] Dossierstuk 13: Informatieverzoek AP van 25 juli 2019; en Dossierstuk 15: Informatieverzoek AP van 1 oktober 2019 en aankondiging OTP Verwerker 2 op 1 november 2019.
[147] Dossierstuk 17: Verslag van Ambtshandelingen OTP Verwerker 2 1 november 2019, p. 7 en 8.
[148] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 11.

161. Uit Log 1 blijkt niet welke handelingen in NVIS door de medewerkers van de consulaire post Londen zijn uitgevoerd en op welk tijdstip dat gebeurde. Met betrekking tot Log 2 stelt AP vast dat niet na te gaan is welke gegevens van visumaanvragers de medewerkers van de consulaire post hebben verwerkt, met welk doel, op welk moment dit heeft plaatsgevonden en welk apparaat hierbij werd gebruikt. De AP stelt daarnaast vast dat er discrepanties zijn tussen beide logbestanden. Aangezien Log 1 gaat over 4 juli 2019 en Log 2 over de periode 1 juli 2019 tot en met 3 juli 2019, sluiten Log 2 en Log 1 chronologisch op elkaar aan. Beide bestanden verschillen echter in de opbouw.[149]

162. In Log 3, Log 4 en Log 5 staat naast de naam van de medewerker ook het visumaanvraagnummer en een globale aanduiding van het onderdeel van het visumproces dat is uitgevoerd en het tijdstip waarop dat onderdeel is afgerond. Uit deze logbestanden blijkt echter niet welke persoonsgegevens van visumaanvragers de medewerkers van de CSO hebben verwerkt, met welk doel en op welk moment dit heeft plaatsgevonden.

163. Gelet op de vaststellingen hierboven, stelt de AP vast dat BZ geen adequaat overzicht heeft van de logbestanden die worden gegenereerd in de NVIS-omgeving. Het NVIS-gebruik wordt weliswaar gelogd, maar de overgelegde logbestanden vertonen qua opbouw en type data dat erin is opgenomen inconsistenties.[150] De logbestanden die de AP heeft ontvangen en beoordeeld, laten bovendien zien dat niet alle verplichte acties worden gelogd. [VERTROUWELIJK][151]

164. BZ stelt in haar zienswijze (voor zover nog relevant voor de overtreding) over de logbestanden het volgende. Voor wat betreft logbestand 1 had het volgens BZ op de weg van de AP gelegen om BZ erop te wijzen dat niet alleen de loggegevens over de toegang gevraagd werd, maar ook welke handelingen in NVIS zijn uitgevoerd en op welk tijdstip. Dit betoog faalt. In haar informatieverzoek heeft de AP een logbestand gevraagd over het NVIS-gebruik bij de ambassade Londen.[152] Het behoeft naar het oordeel van de AP weinig betoog dat bij het gebruik van NVIS, waarin - onbetwist - persoonsgegevens worden verwerkt, de AP niet slechts geïnteresseerd is in informatie over het inloggen tot dit systeem.

165. Voor wat betreft logbestand 2 stelt BZ dat artikel 32 lid 2 onder i van de VIS-verordening, waaraan AP de logging toetst, vereist dat wordt vastgelegd welke gegevens worden verwerkt. Maar dit artikel vereist niet dat elk gegeven dat wordt verwerkt wordt gelogd. Een aanduiding van welke gegevens worden verwerkt kan daarom volgens BZ volstaan zonder exacte weergave van die gegevens. Daarbij komt betekenis toe aan artikel 32 AVG. Het doel van de logging is controle op rechtmatig gebruik van toegangsrechten. Doordat BZ vastlegt welke aanvraaggegevens worden verwerkt, staat daardoor voldoende precies vast welke gegevens zijn verwerkt. Met het visumaanvraagnummer is volgens BZ ook bekend van welke betrokkene persoonsgegevens zijn verwerkt. Het zou te ver voeren om per visumaanvrager te laten vastleggen of de NVIS-medewerker bijvoorbeeld alleen de naam heeft verwerkt of alleen de geboortedatum of beide.

[149] De verschillen betreffen het aantal gelogde variabelen en hun benaming in de logbestanden.
[150] Vergelijk bijvoorbeeld het type handelingen dat is opgenomen in Log 1 met het type handelingen dat is opgenomen in Log 2.
[151] Informatie verstrekt door BZ tijdens OTP's CSO op 16 juli 2019 en 12 september 2019 (zie dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 16 juli 2019 en 12 september 2019).
[152] Dossierstuk 10, bijlage 1 onder punt 40.

166. De AP volgt de zienswijze van BZ niet. Artikel 32 lid 2 onder i van de VIS-verordening vereist dat het mogelijk moet zijn om na te gaan en vast te stellen welke gegevens wanneer, door wie en met welk doel in het VIS zijn verwerkt. Het loggen van een visumaanvraagnummer geeft onvoldoende duiding welke gegevens worden verwerkt. Hierdoor kan men achteraf niet zien welke gegevens wanneer zijn verwerkt. Hoe gevoeliger het persoonsgegeven dat wordt verwerkt is, hoe hoger de eisen aan logging hieromtrent zijn. In deze context, waarbij zeer veel – ook – bijzondere persoonsgegevens verwerkt worden, is het van groot belang dat wijzigingen in gegevens te herleiden zijn. BZ moet kunnen controleren welke gegevens door wie zijn gewijzigd, niet uitsluitend na een incident. Deze informatie mag ook uit een combinatie van (log)bestanden afgeleid worden. Het doel van logging beperkt zich aldus niet, zoals BZ stelt, alleen tot de controle op rechtmatig gebruik van toegangsrechten.

167. BZ stelt verder in haar schriftelijke zienswijze dat de conclusie van de AP, dat controles op het NVIS-gebruik die BZ uitvoert gericht zijn op de toegekende autorisaties en niet op logbestanden en handelingen die in NVIS door medewerkers zijn uitgevoerd, onjuist en voorbarig is. BZ is van mening dat het informatieverzoek hierover door de AP te algemeen geformuleerd was. Volgens BZ zitten in NVIS vele mogelijkheden om rapportages te maken op het daadwerkelijk gebruik van NVIS. BZ stelt tot slot dat de vraag van de AP onduidelijk was over logging en hoe de controle hierop in het beveiligingsbeleid was ingeregeld.

168. Hoewel de AP van oordeel is dat het op de weg van BZ ligt om tijdig – en niet pas in een zienswijze - kenbaar te maken dat een informatieverzoek vragen oproept, heeft de AP BZ nogmaals in de gelegenheid gesteld om procedures te overleggen die omschrijven op welke wijze BZ ten opzichte van NVIS logt en controles hierop uitvoert.[153] BZ heeft in reactie hierop een ongedateerd document met enkele alinea's verstrekt met daarin een feitelijk beschrijving wat er bij gebruik van NVIS gelogd wordt.[154] [VERTROUWELIJK][155]

169. Gezien de tekortkomingen in logbestanden in combinatie met het feit dat BZ de logbestanden niet regelmatig beoordeelt én hieromtrent een procedure ontbreekt, komt de AP tot de conclusie dat BZ in strijd handelt met artikel 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, onder f, i en k van de VIS Verordening en de BIO-normen betreffende logbestanden (met name norm 12.4.1).

2.7 Controle van NVIS-gebruik: beveiligingsincidenten

2.7.1 Wettelijk kader

170. In artikel 32, lid 2, onder c en d, van de VIS Verordening is respectievelijk bepaald dat BZ passende maatregelen neemt ter voorkoming dat gegevensdragers onrechtmatig worden gelezen, gekopieerd,

[153] Brief AP aan BZ van 19 november 2021, p. 3.
[154] E-mail BZ aan AP van 10 december 2021, bijlage 16.
[155] Zie paragraaf 2.6.2 en brief BZ aan AP van 19 november 2021, bijlage 1 Gespreksverslag, p. 36.

gewijzigd of verwijderd, en dat gegevens onrechtmatig worden ingezien, gewijzigd of verwijderd. Indien sprake is van onbevoegde (externe of interne) toegang tot gegevensdragers en/of persoonsgegevens opgeslagen in de NVIS-omgeving, dan is er sprake van een beveiligingsincident. Onder de vereisten van artikel 32, lid 2, onder k, VIS Verordening geldt dat de nodige organisatorische maatregelen genomen moeten worden voor de opvolging van dergelijke beveiligingsincidenten. Deze bepalingen schrijven dus voor dat interne controles op de NVIS-gegevensdragers en de opslag van NVIS-gegevens dienen plaats te vinden, en dat de doelmatigheid van de beveiligingsmaatregelen dient te worden gecontroleerd.

Hoofdstuk 16.1 van de BIO beschrijft de verplichte standaarden voor het beheer van de beveiligingsincidenten en verbeteringen. Hierbij zijn onder meer de volgende BIO-normen van toepassing:

16.1.1 1	Verantwoordelijkheden en procedures: Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
16.1.2.2	Er is een meldprocedure waarin taken en verantwoordelijkheden van het meldloket staan beschreven.
16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.
16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
16.1.2.6	Opvolging van incidenten wordt maandelijks gerapporteerd aan verantwoordelijke.
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
16.1.6	Lering uit informatiebeveiligingsincidenten: Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.

171. In de bovenstaande BIO-normen wordt aangegeven dat een consistente en doeltreffende aanpak dient te worden bewerkstelligd van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. Hiertoe dienen verantwoordelijkheden en procedures te worden vastgesteld, een meldloket te worden ingericht, waarin beveiligingsincidenten worden gemeld, inclusief de meldprocedure. Informatiebeveiligingsincidenten en de opvolging hiervan worden maandelijks aan de verantwoordelijke gerapporteerd. Hiervoor worden

beveiligingsincidenten onder meer geanalyseerd, met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.

2.7.2 Feitelijke bevindingen

172. In het kader van haar onderzoek heeft de AP gecontroleerd of BZ over een procedure beschikt voor het melden en opvolgen van beveiligingsincidenten/datalekken in relatie tot NVIS en het visumproces. In dat verband heeft de AP BZ gevraagd om een uittreksel uit het meldingsregister over 2018 en 2019 waarin alle NVIS-gerelateerde beveiligingsincidenten worden geregistreerd. Tijdens het onderzoek hebben de AP-inspecteurs hierover vragen gesteld en de relevante documentatie over beveiligingsincidenten opgevraagd.

Consulaire posten: Londen en Dublin en CSO Den Haag

Procedure beveiligingsincidenten

173. De consulaire posten Londen en Dublin en de CSO volgen dezelfde BZ-brede werkwijze met betrekking tot het melden van beveiligingsincidenten/datalekken: een beveiligingsincident wordt direct aan [VERTROUWELIJK] gemeld, en indien sprake is van een datalek wordt er een [VERTROUWELIJK] aangemaakt en digitaal verstuurd aan [VERTROUWELIJK]. Deze procedure staat op [VERTROUWELIJK], te raadplegen door medewerkers van BZ [VERTROUWELIJK].

174. Ter plaatse bij de consulaire posten maken medewerkers ook gebruik van 'Factsheets datalekken' die in het Nederlands en Engels zijn opgesteld. Deze factsheets zijn een schematische weergave van de procedure met een opsomming van alle stappen die medewerkers moeten volgen indien sprake is van een datalek. Tijdens de onderzoeken zijn de genoemde factsheets-datalekken aan de AP-inspecteurs getoond [VERTROUWELIJK].

175. Naar aanleiding van het onderzoek in Londen heeft de AP BZ gevraagd[156] om de procedure melding datalekken te verstrekken. BZ heeft de volgende stukken overgelegd:
- Factsheets datalek augustus 2018[157], zowel in het Nederlands als het Engels. Deze factsheets zien op de schematische weergave van de werkwijze bij datalekken, zoals hierboven beschreven en getoond bij de consulaire posten.
- Instructievideo's over datalekken[158]: in deze korte films wordt een voorlichting gegeven over datalekken.
- Uitdraai van het informatiemateriaal over datalekken op [VERTROUWELIJK], met voorbeelden van datalekken[159] en de beschrijving van de werkwijze voor BZ-medewerkers in geval van datalekken[160]. Dit laatste document bevat een beschrijving van de stappen die medewerkers van

[156] Dossierstuk 10: Informatieverzoek AP van 12 juli 2019.
[157] Dossierstuk 12, bijlage 11a: Factsheet datalek NL aug 2018; Dossierstuk 12, bijlage 11b: Factsheet datalek EN aug 2018; en Dossierstuk 12, bijlage 11d: Datalekken sharepoint.
[158] Dossierstuk 12, bijlage 11c: Instructievideo - Help, een datalek; en Dossierstuk 12, bijlage 11f: Data breach movie. Deze dossierstukken zijn video-bestanden.
[159] Dossierstuk 12, bijlage 11e: Datalekken voorbeelden sharepoint.
[160] Dossierstuk 12, bijlage 12c: Datalekken informatie voor BZ medewerkers.

BZ moeten nemen indien er sprake is van datalekken, overeenkomstig de procedure die tijdens de onderzoeken in Londen en Dublin is toegelicht.

176. De AP stelt vast dat de medewerkers van de consulaire posten Londen en Dublin en de CSO, met betrekking tot het melden van beveiligingsincidenten/datalekken, de procedure volgen die voor alle medewerkers van BZ geldt. Deze procedure is een praktische handleiding over de stappen die medewerkers moeten ondernemen bij beveiligingsincidenten: deze moeten zo snel mogelijk aan [VERTROUWELIJK] worden gemeld en in geval van datalekken wordt een melding gemaakt bij [VERTROUWELIJK]. De genoemde procedure is niet op een managementniveau vastgesteld, en geeft verder geen inzicht in de stappen die worden gevolgd *nadat* een melding over een beveiligingsincident/ datalek heeft plaatsgevonden. De procedure beschrijft ook niet de taken en verantwoordelijkheden van het meldloket en wie als proceseigenaar verantwoordelijk is voor het oplossen van beveiligingsincidenten en de rapportage hierover.

<u>Beveiligingsincidenten</u>

177. [VERTROUWELIJK]

178. De AP heeft bij BZ een beveiligingsincidentenregister opgevraagd[161] waarin alle beveiligingsincidenten in relatie tot NVIS en het visumproces staan vermeld, met betrekking tot de volgende periodes: (1) 1 oktober 2018 tot en met 31 december 2018, en (2) 1 april 2019 tot en met 1 juli 2019. De AP heeft negen meldingen van incidenten[162] bij de consulaire post Londen gekregen. [VERTROUWELIJK]. Door het ontbreken van een nadere toelichting op deze meldingen was de AP tijdens het onderzoek in de veronderstelling dat BZ geen kopie van het beveiligingsincidentenregister heeft verstrekt.

179. [VERTROUWELIJK][163]

180. [VERTROUWELIJK] [164]

[161] Dossierstuk 10: Informatieverzoek AP van 12 juli 2019.
[162] [VERTROUWELIJK]
[163] [VERTROUWELIJK]
[164] Dossierstuk 11: Verslag van Ambtshandelingen OTP CSO 18 juli 2019 en 12 september.

181. Een medewerker van [VERTROUWELIJK] heeft tijdens het onderzoek verklaard dat BZ over een incidentenregister beschikt waarin beveiligingsincidenten worden geregistreerd. De AP heeft gevraagd om een beveiligingsincidentenregister te verstrekken met betrekking tot NVIS en betreffende het jaar 2018 en de eerste helft van 2019. [VERTROUWELIJK][165]. BZ heeft geen (blanco) incidentenregister aangeleverd. Daarnaast heeft de AP ook gevraagd om een halfjaarsrapportage over beveiligingsincidenten. Dit document is verstrekt.[166] Het beschrijft datalekken met betrekking tot reisdocumenten.

182. BZ heeft tijdens de zienswijzefase onder andere de volgende toelichting gegeven over het proces van beveiligingsincidenten. Meldingen worden door [VERTROUWELIJK] behandeld in [VERTROUWELIJK]. Alle handelingen die nodig zijn voor het afhandelen van een melding worden hierin vastgelegd en opgeslagen. Deze gemelde incidenten/inbreuken, ongeacht de vraag of die aan de AP gemeld hadden moeten worden, worden na volledig afgehandeld te zijn, afgesloten, gelogd en opgeslagen in een afgeschermde, alleen voor [VERTROUWELIJK] toegankelijke omgeving achter het [VERTROUWELIJK] (het datalekregister). Alle uitgevoerde (vervolg)stappen worden vastgelegd in de individuele meldingsdossiers in het centrale register van incidentmeldingen dat wordt gevuld door [VERTROUWELIJK]. Tot slot heeft BZ verklaard dat alle incidenten inmiddels wel op één centrale plaats worden bijgehouden en bewaard.

183. Naar aanleiding van het voorgaande heeft BZ nadere vragen van de AP beantwoord over de vormgeving van het centrale register met beveiligingsincidenten. Op grond hiervan en op grond van bovenstaande toelichting acht de AP het voldoende aannemelijk dat BZ wel beschikt over een beveiligingsincidentenregister waarin beveiligingsincidenten in relatie tot NVIS worden geregistreerd.

Verwerker 2

184. Op 1 november 2019 heeft de AP een onderzoek uitgevoerd bij Verwerker 2. Hierbij heeft de AP de procedure ontvangen die Verwerker 2 hanteert in geval van beveiligingsincidenten.[167] In deze escalatieprocedure wordt beschreven welke stappen binnen de organisatie genomen moeten worden wanneer een beveiligingsincident zich voordoet, welke rollen/functies bij Verwerker 2 dienen te worden geïnformeerd en naar welke rollen/functies dient te worden geëscaleerd. Verwerker 2 heeft ook een beleid overgelegd dat ziet op beveiligingsincidenten[168] en datalekken[169].

185. Voor wat betreft beveiligingsincidenten heeft Verwerker 2 tijdens het onderzoek verklaard dat er in 2018 en 2019 geen incidenten zijn geweest in relatie tot de NVIS-omgeving. Dit zag specifiek op incidenten [VERTROUWELIJK]

[165] Dossierstuk 14, bijlage 20.1: Toelichting.
[166] Dossierstuk 14, bijlage 21.1: [VERTROUWELIJK].
[167] Dossierstuk 17, bijlage 3: Incident Escalation Procedure.
[168] Dossierstuk 17, bijlage 4: [VERTROUWELIJK].
[169] Dossierstuk 17, bijlage 5: Procedure Data Breach Controller.

186. Op de vraag of Verwerker 2 een logboek of register bijhoudt met beveiligingsincidenten, heeft Verwerker 2 verklaard verschillende registers te hanteren afhankelijk van het incident. Verwerker 2 heeft toegelicht dat er twee incidentenregisters worden gebruikt.
[VERTROUWELIJK][170] [171]

187. [VERTROUWELIJK]. Verwerker 2 heeft aangegeven dat er geen beveiligingsincidenten bij Verwerker 2 zijn geweest met betrekking tot NVIS in de onderzoeksperiode. Er waren hierdoor geen interne meldingen die Verwerker 2 aan AP kon verstrekken.[172]

188. Op grond van het bovenstaande en de toelichting van BZ tijdens de zienswijzefase acht de AP de taakverdeling tussen BZ en Verwerker 2 met betrekking tot beveiligingsincidenten voldoende duidelijk.

2.7.3 Juridische beoordeling

189. De AP komt tot het oordeel dat de algemene procedure die BZ ten tijde van het onderzoek heeft verstrekt voor het melden van beveiligingsincidenten door BZ-medewerkers, niet voldoet. Deze procedure is een niet meer dan een handleiding over de stappen die medewerkers moeten ondernemen bij beveiligingsincidenten: deze moeten zo snel mogelijk aan [VERTROUWELIJK] worden gemeld en in geval van datalekken wordt een melding gemaakt bij [VERTROUWELIJK]. De genoemde procedure is niet op managementniveau vastgesteld en geeft verder geen inzicht in de specifieke stappen die worden gevolgd *nadat* een melding over een beveiligingsincident/datalek heeft plaatsgevonden. De procedure beschrijft ook niet de taken en verantwoordelijkheden van het meldloket en wie als proceseigenaar verantwoordelijk is voor het oplossen van beveiligingsincidenten en de rapportage hierover.

190. Tijdens de zienswijzefase heeft BZ als reactie hierop een AVG-handleiding (geaccordeerd op 13 oktober 2021) en een Procesbeschrijving Incident management beveiligingsincidenten en datalekken (juli 2020) aan de AP verstrekt. De AP heeft deze documentatie beoordeeld en komt tot de conclusie dat BZ vanaf 13 oktober 2021 wel volledig inzicht verschaft over de stappen die worden gevolgd nadat een melding over een beveiligingsincident/datalek heeft plaatsgevonden. Ook zijn de taken en verantwoordelijkheden van het meldloket vermeld en heeft BZ vastgesteld wie als proceseigenaar verantwoordelijk is voor het oplossen van beveiligingsincidenten en de rapportage hierover.

[170] Dossierstuk 23, bijlage 06.2: Toelichting op Incidentenregister oktober 2018 tot en met 1 november 2019.
[171] Dossierstuk 23, bijlage 06.1: -AP-z2019-12207-06-Incidentenregister extract.
[172] Schriftelijke Zienswijze BZ van 15 oktober 2021, p. 13.

191. Op grond van het bovenstaande komt de AP tot het oordeel dat BZ, voor wat betreft de gebreken aan de procedure voor het melden van beveiligingsincidenten, tot 13 oktober 2021 onvoldoende passende organisatorische maatregelen heeft genomen ter voorkoming van onrechtmatige gegevensverwerkingen in NVIS. Hierdoor heeft BZ inbreuk gemaakt op de vereisten die zijn neergelegd in artikel 32, lid 1, AVG en nader uitgewerkt in artikel 32, lid 2, onder c en d, VIS Verordening en de BIO-normen 16.1.1 en 16.1.2.2. Per 13 oktober 2021 zijn de hiervoor genoemde gebreken door BZ hersteld en is de inbreuk aldus op dit punt beëindigd.

2.8 Opleiding personeel inzake bescherming van persoonsgegevens

192. Artikel 28, lid 5, VIS Verordening schrijft voor dat het personeel van de autoriteiten met toegangsrecht tot het VIS een degelijke opleiding moet krijgen over de regels inzake gegevensbeveiliging en –bescherming. Ook wordt het personeel op de hoogte gebracht van ter zake doende strafbare feiten en sancties. De AP heeft echter niet de inhoud van deze opleidingen noch de wijze waarop die zijn aangeboden getoetst gedurende het onderzoek. Artikel 38, lid 3, Visumcode schrijft verder voor dat de 'centrale autoriteiten van de lidstaten zowel de uitgezonden als de lokale medewerkers op passende wijze [dienen] op te leiden en hen te voorzien van volledige, nauwkeurige en bijgewerkte informatie over de relevante wetgeving.'

193. De AP constateert op basis van de verklaringen van medewerkers en de door BZ verstrekte documenten ten aanzien van het trainen van medewerkers die toegang hebben tot gegevens in het NVIS dat er sprake is van training op het gebied van gegevensbescherming- en beveiliging. Daarnaast worden de opleidingen aangeboden voor zowel medewerkers die pas kort in dienst zijn als medewerkers die al langer bij BZ werken. De opleidingen behelzen o.a. de te gebruiken systemen (waaronder NVIS), relevante wet- en regelgeving en beveiliging. Ook constateert de AP dat sprake is van opleidingen van zowel uitgezonden als lokale medewerkers.

194. Hiermee is, voor wat betreft de vraag of in de opleidingen aandacht wordt besteed aan informatiebeveiliging en de regelgeving inzake de verwerking van persoonsgegevens, voldaan aan de eisen die zijn neergelegd in BIO doelstelling 7.2.2 en artikel 38, lid 3, Visumcode.

2.9 Informatievoorziening aan visumaanvragers

2.9.1 Wettelijk kader

195. Transparant zijn over gegevensverwerkingen is één van de algemene beginselen voor een behoorlijke gegevensverwerking. Het informeren van de betrokkene over een gegevensverwerking draagt bij aan transparantie. Artikel 37 VIS Verordening schrijft voor dat visumaanvragers worden ingelicht over de verantwoordelijke, de doelen van de verwerking van de persoonsgegevens van de visumaanvragen, de categorieën ontvangers van verwerkte persoonsgegevens, de bewaringstermijn, de verplichting van het verzamelen van deze gegevens en de rechten van de betrokkene. Dit betekent dat BZ de visumaanvragers

schriftelijk informeert bij het verzamelen van de gegevens ten behoeve van het aanvraagformulier, de foto en de vingerafdrukken.[173] Deze verplichting vloeit ook voort uit artikel 13 AVG.

2.9.2 Feitelijke bevindingen

196. De AP heeft een onderzoek uitgevoerd bij de consulaire post in Londen en Dublin. Uit deze onderzoeken en de verkregen informatie volgt, dat betrokkenen op drie manieren geïnformeerd kunnen worden over het verwerken van hun foto's, vingerafdrukken en persoonsgegevens ten behoeve van een visumaanvraag. Informatieverstrekking vindt plaats middels (1) een "Privacy statement regarding Short-Stay Visa Applications" (hierna: Privacy Statement)[174], (2) een bijlage bij het aanvraagformulier voor de visumaanvraag (hierna: Bijlage)[175], en (3) een folder[176] op locatie van de consulaire post.

197. De eerste mogelijkheid van informatieverstrekking is de Privacy Statement. Op de (in het Engels geschreven) websites van de ambassades in Ierland en het Verenigd Koninkrijk staat informatie over de vraag hoe een (Schengen)visumaanvraag in zijn werk gaat. [177] De websites verwijzen naar deze Privacy Statement, die te vinden is op de website van BZ.[178]

198. In de Privacy Statement worden verschillende privacy componenten behandeld zoals de doelen voor de verwerking van de persoonsgegevens van de visumaanvragen, de verwerkingsverantwoordelijke, de bewaringstermijn van 5 jaar, de verplichting tot het verzamelen van de gegevens en de rechten van betrokkenen. In een apart document worden de risicolanden opgesomd die van invloed kunnen zijn in het visumproces inzake risicoanalyses.[179] De Privacy Statement stelt verder dat er sprake kan zijn van het delen van persoonsgegevens met derde partijen zoals andere Europese autoriteiten binnen het Schengen gebied en instanties zoals Europol. In de Privacy Statement wordt geen melding gemaakt van de mogelijke verwerkers van persoonsgegevens zoals bijvoorbeeld private partijen die betrokken kunnen zijn bij het proces van de visumaanvragen. De AP stelt verder vast dat de nationale "Data Protection Authority", inclusief de adresgegevens, genoemd wordt in de privacy statement als de aangewezen instantie in het geval de betrokkene haar/zijn rechten zou willen uitoefenen.[180]

199. De tweede mogelijkheid van informatieverstrekking vindt plaats via de Bijlage.[181] De Bijlage wordt schriftelijk aan de betrokkene verstrekt op het moment dat de gegevens van het aanvraagformulier worden verzameld. In de Bijlage wordt BZ genoemd als verwerkingsverantwoordelijke voor de gegevensverwerking, worden de doelen van de verwerking van persoonsgegevens benoemd, worden de bewaringstermijnen genoemd en wordt de verplichting tot het verzamelen van de persoonsgegevens

[173] Artikel 37, lid 2, Verordening "De in lid 1 bedoelde informatie wordt schriftelijk aan de aanvrager meegedeeld bij het verzamelen van de gegevens van het aanvraagformulier, de foto en de vingerafdrukgegevens zoals bedoeld in artikel 9, leden 4, 5 en 6."
[174] Dossierstuk 7, bijlage 2: Privacy Statement re. Short stay visa applications.
[175] Dossierstuk 7, bijlage 6: Schengen Visa Application (voorbeeldformulier), verstrekt t.t.v. het OTP consulaire post Londen.
[176] Dossierstuk 7, bijlage 4: Informatieblad over SIS II; en Dossierstuk 27, bijlage 10: Folder publieksinformatie over SIS II.
[177] Zie voor Ierland: https://www.netherlandsandyou.nl/your-country-and-the-netherlands/ireland/travel-and-residence/applying-for-a-short-stay-schengen-visa (voor het laatst geraadpleegd op 14 augustus 2020) en voor het Verenigd Koninkrijk: https://www.netherlandsandyou.nl/your-country-and-the-netherlands/united-kingdom/travel-and-residence/applying-for-a-short-stay-schengen-visa (voor het laatst geraadpleegd op 14 augustus 2020).
[178] https://www.netherlandsandyou.nl/documents/publications/2017/12/06/privacystatement-regarding-short-stay-visa-applications-en (voor het laatst geraadpleegd op 23 februari 2022).
[179] Conform artikel 22 Visumcode.
[180] Artikel 37, lid 1, onder f, VIS Verordening.
[181] Dossierstuk 7, bijlage 6: Schengen Visa Application (voorbeeldformulier), verstrekt t.t.v. het OTP consulaire post Londen.

uitgelegd. Ook wordt naar het College Bescherming Persoonsgegevens verwezen voor klachtbehandeling. De AP merkt verder op dat om toestemming wordt gevraagd aan de betrokkene. In de lijst van categorieën van ontvangers van persoonsgegevens worden geen derde private partijen genoemd.

200. De derde mogelijkheid van informatieverstrekking is gebleken bij het onderzoek in Dublin,[182] toen door de medewerkers van de consulaire post een folder SIS II[183] is getoond die beschikbaar wordt gesteld aan de visumaanvragers in de wachtruimte. Deze folder heeft betrekking op SIS II en behelst geen informatie over rechten van betrokkenen inzake een visumaanvraag en het uitoefenen van rechten van betrokkenen gedurende het visumaanvraag proces. Hoewel de folder op zichzelf informatief is inzake SIS II tegen de achtergrond van de visumaanvraag, is de folder niet toepasbaar voor wat betreft het uitoefenen van rechten van betrokkenen in het visumproces.

2.9.3 Juridische beoordeling

201. De AP stelt vast dat BZ in de Privacy Statement en in de Bijlage (1) de doelen van de gegevensverwerking noemt, (2) duidelijk maakt dat het verzamelen van de gegevens verplicht is, (3) bewaartermijnen opneemt, en (4) de bevoegde (privacy)toezichthouder noemt.[184] Ten aanzien van beide documenten geldt echter dat niet alle (categorieën van) ontvangers van persoonsgegevens door BZ worden vermeld. De AP stelt vast dat slechts een aantal categorieën ontvangers is genoemd, zoals andere Europese autoriteiten en Europol. De Privacy Statement en de Bijlage maken geen melding van het delen van persoonsgegevens met derde private partijen, zoals de verwerkers Verwerker 2 en Verwerker 3 die betrokken zijn bij het proces van de visumaanvraag. Hiermee is niet voldaan aan de eis van artikel 37, lid 1, onder c, VIS Verordening en artikel 13, lid 1, onder e, AVG.

202. BZ stelt in haar zienswijze dat het geen uitgemaakte zaak is dat betrokkenen geïnformeerd moeten worden over de verstrekking van gegevens aan een verwerker. BZ is van oordeel dat Verwerker 2 uitsluitend als verwerker kwalificeert en niet als ontvanger van persoonsgegevens. Zonder de gehoudenheid daartoe te erkennen zal BZ in de Privacy statement en/of de Bijlage opnemen dat BZ persoonsgegevens laat verwerken door verwerkers.

203. De AP volgt de stelling van BZ niet. Uit artikel 13, lid 1 sub e, AVG volgt dat de verwerkingsverantwoordelijke de betrokkene informeert over de ontvangers of categorieën van ontvangers van de persoonsgegevens. Artikel 4, onderdeel 9, AVG definieert een ontvanger als een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Verwerkers als Verwerker 2 en Verwerker 3 zijn rechtspersonen die de persoonsgegevens over de betrokkenen ontvangen. De Richtsnoeren inzake transparantie benoemen overigens ook dat een ontvanger een verwerker kan zijn.[185]

[182] Dossierstuk 27: Verslag van Ambtshandelingen OTP consulaire post Dublin.
[183] Dossierstuk 7, bijlage 4: Informatieblad over SIS II; en Dossierstuk 27, bijlage 10: Folder publieksinformatie over SIS II..
[184] In de Bijlage wordt echter nog verwezen naar het College Bescherming Persoonsgegevens.
[185] Groep gegevensbescherming artikel 29 Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, p. 18.

2.10 Conclusies

204. De AP komt met betrekking tot de vastgestelde overtredingen tot de volgende conclusies.

Beveiligingsplan

205. De AP komt tot de conclusie dat BZ met betrekking tot NVIS geen beveiligingsplan heeft (en dit dus ook niet heeft geëvalueerd). BZ handelt hiermee tenminste vanaf 1 september 2018 tot heden in strijd met artikel 24 en 32, lid 1, AVG, dat nader is uitgewerkt in artikel 32, lid 2, aanhef, VIS Verordening en BIO-normen 5.1.1, 5.1.1.1 en 5.1.2.1.

Fysieke beveiliging

206. BZ heeft, door niet expliciet te bepalen welke onderdelen van de IT-infrastructuur aangemerkt dienen te worden als de kritieke infrastructuur van het visumproces, vanaf tenminste 1 september 2018 tot in ieder geval het voorjaar van 2020 in strijd gehandeld met artikel 32, lid 1, AVG, dat nader is uitgewerkt in artikel 32, lid 2, onder a, VIS Verordening.

207. De AP komt verder tot de conclusie dat BZ, waar het gaat om het opstellen van noodplannen en de bescherming van apparatuur tegen ontregelingen in nutsvoorzieningen, vanaf tenminste 1 september 2018 tot heden niet voldoet aan het bepaalde in artikel 32, lid 1, AVG dat nader is uitgewerkt in artikel 32, lid 2, sub a, VIS Verordening en BIO-normen 11.1.4 en 11.2.2.

208. Voorts is de AP van oordeel dat door het ontbreken van beveiligingswaarborgen bij het betreden van de zone die extra beveiligd moet zijn, de fysieke beveiliging van de ruimtes waarin gewerkt wordt aan het visumproces in Londen niet voldeed. Hierdoor heeft BZ van tenminste 1 september 2018 tot april 2020 in strijd gehandeld met artikel 32, lid 1, AVG dat nader uitgewerkt is in artikel 32, lid 2, sub a, VIS Verordening en BIO-normen 11.1.1 t/m 11.1.5 en 11.2.2.

209. Nu BZ tot slot niet heeft aangetoond dat er voldoende waarborgen gelden voor de fysieke beveiliging bij het werken in NVIS in openbare ruimtes en BZ evenmin de doelmatigheid van het beleid hieromtrent heeft gecontroleerd, komt de AP tot de conclusie dat BZ van tenminste 1 september 2018 tot heden in strijd handelt met artikel 32, lid 1, AVG dat nader is uitgewerkt in artikel 32, lid 2, sub a en k, VIS Verordening.

Toegangsrechten tot NVIS

210. De AP komt tot de conclusie dat BZ van tenminste 1 september 2018 tot 1 januari 2022 niet over formele registratie- en afmeldingsprocedures beschikte ten aanzien van de toewijzing van toegangsrechten tot NVIS. Hiermee heeft BZ in strijd gehandeld met artikel 32, lid 1, AVG dat nader is uitgewerkt in BIO-normen 9.2.1 en 9.2.2.

211. De AP is verder van oordeel dat BZ, ten aanzien van de procedure over de controle op toegangsrechten tot de NVIS-omgeving en de controle hiervan in de praktijk, van tenminste 1 september 2018 tot heden in strijd handelt met artikel 32, lid 1, AVG dat nader is uitgewerkt in 32, lid 2, onder f en k, VIS Verordening en BIO-normen 9.2.1, 9.2.2, 9.2.5 en 9.2.6.

Controle NVIS-gebruik: logging

212. Gezien de tekortkomingen in logbestanden in combinatie met het feit dat BZ de logbestanden niet regelmatig beoordeelt én hieromtrent een procedure ontbreekt, komt de AP tot de conclusie dat BZ van tenminste 1 september 2018 tot heden niet in overeenstemming handelt met artikel 32, lid 1, AVG dat nader is uitgewerkt in artikel 32, lid 2, onder f, i en k van de VIS Verordening en de BIO-normen betreffende logbestanden (met name norm 12.4.1).

Controle NVIS-gebruik: beveiligingsincidenten

213. De AP komt voor wat betreft de gebreken aan de procedure voor het melden van beveiligingsincidenten tot de conclusie dat BZ van tenminste 1 september 2018 tot 13 oktober 2021 onvoldoende passende organisatorische maatregelen heeft genomen ter voorkoming van onrechtmatige gegevensverwerkingen in NVIS. Hierdoor heeft BZ inbreuk gemaakt op artikel 32, lid 1, AVG dat nader is uitgewerkt in artikel 32, lid 2, onder c en d, VIS Verordening en de BIO-normen 16.1.1 en 16.1.2.2.

Informatievoorziening aan visumaanvragers

214. De AP komt tot slot tot de conclusie dat BZ in het kader van de informatievoorziening aan visumaanvragers geen melding maakt van het delen van persoonsgegevens met derde private partijen, zoals Verwerker 2 en Verwerker 3. Hiermee overtreedt BZ van tenminste 1 september 2018 tot heden artikel 13, lid 1, onder e, AVG dat nader is uitgewerkt in artikel 37, lid 1, onder c, VIS Verordening.

3 Boete

3.1 Inleiding

215. BZ heeft in strijd gehandeld met artikel 32, lid 1, AVG en artikel 13, lid 1, onder e, AVG. Hierdoor heeft BZ niet in overeenstemming gehandeld met de basisbeginselen van de verwerking van persoonsgegevens zoals bedoeld in artikel 5 AVG. De AP maakt voor de vastgestelde overtredingen gebruik van haar bevoegdheid om aan BZ een boete op te leggen. BZ heeft in haar zienswijze gesteld dat door verschillende transitieprocessen en verbetermaatregelen het opleggen van een boete en/of last onder dwangsom niet redelijk is. Vanwege de ernst van de overtredingen, de mate waarin deze aan BZ kan worden verweten en het feit dat de overtredingen nog voortduren acht de AP, anders dan BZ, de oplegging van een boete en een last onder dwangsom wel gepast. De AP motiveert dit in het navolgende.

3.2. Boetebeleidsregels Autoriteit Persoonsgegevens 2019

216. Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, is de AP bevoegd aan BZ in geval van een overtreding van artikel 32 van de AVG een bestuurlijke boete op te leggen tot € 10.000.000.

217. Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vijfde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, is de AP bevoegd aan BZ in geval van een overtreding van artikel 13 van de AVG een bestuurlijke boete op te leggen tot € 20.000.000.

218. De AP heeft Boetebeleidsregels vastgesteld inzake de invulling van voornoemde bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[186] In de Boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte systematiek. Overtreding van artikel 32 van de AVG is ingedeeld in categorie II. Categorie II heeft een boetebandbreedte tussen € 120.000 en € 500.000 en een basisboete van € 310.000. Overtreding van artikel 13 van de AVG is ingedeeld in categorie III. Categorie III heeft een boetebandbreedte tussen € 300.000 en € 750.000 en een basisboete van € 525.000

219. De hoogte van de boete stemt de AP af op de factoren die zijn genoemd in artikel 7 van de Boetebeleidsregels, door het basisbedrag te verlagen of verhogen. Het gaat om een beoordeling van de ernst van de overtreding in het specifieke geval, de mate waarin de overtreding aan de overtreder kan worden verweten en, indien daar aanleiding toe bestaat, andere omstandigheden.

3.3 Boetehoogte inzake overtreding van de beveiliging van de verwerking

220. Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Ter voorkoming dat organisaties met verwerkingen van persoonsgegevens inbreuk maken op de privacy van burgers is het van

[186] Stcrt. 2019, 14586, 14 maart 2019.

groot belang dat zij een op risico afgestemd beveiligingsniveau toepassen. Bij het bepalen van het risico voor de betrokkene zijn onder andere de aard van de persoonsgegevens en de omvang van de verwerking van belang: deze factoren bepalen de potentiële schade voor de individuele betrokkene bij bijvoorbeeld verlies, wijziging of onrechtmatige verwerking van de gegevens. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. De AP heeft geconcludeerd dat BZ onvoldoende een op risico afgestemd beveiligingsniveau heeft gegarandeerd en gewaarborgd in het kader van het behandelen van aanvragen van Schengenvisa.

3.3.1 Aard, ernst en duur van de inbreuk

221. De AP heeft vastgesteld dat BZ zeer veel (gevoelige) persoonsgegevens verwerkt van betrokkenen. Voorbeelden hiervan zijn de combinatie van NAW-gegevens, land van geboorte, doel van de reis, nationaliteit en foto. Betrokkenen zijn verplicht om al deze persoonsgegevens aan BZ te verstrekken om een Schengenvisum te kunnen verkrijgen. In een dergelijke afhankelijke en ongelijke positie is het van groot belang dat BZ voldoende een op risico afgestemd beveiligingsniveau garandeert en waarborgt. De gevolgen en de daaruit voortvloeiende schade voor betrokkenen zijn namelijk groot ingeval van verlies, wijziging of onrechtmatige verwerking van de gegevens. Onbevoegden kunnen bijvoorbeeld persoonsgegevens inzien en wijzigen, maar ook bevoegde medewerkers kunnen tijdens de behandeling van de aanvraag invoerfouten maken. Hierdoor kunnen aanvragen onterecht geweigerd worden, wat weer een inbreuk oplevert op de bewegingsvrijheid van betrokkenen. De AP concludeert dan ook dat als gevolg van de omstandigheid dat BZ heeft nagelaten passende technische en organisatorische maatregelen te treffen de vertrouwelijkheid en de integriteit van de persoonsgegevens onvoldoende zijn gewaarborgd.

222. Daarnaast neemt de AP in overweging dat BZ persoonsgegevens verwerkt van zeer veel betrokkenen. Vaststaat dat BZ honderdduizenden aanvragen per jaar verwerkt (682.484 in 2018, 739.248 in 2019 en 169.926 in 2020).[187] De persoonsgegevens van al deze aanvragen zijn dus onvoldoende beveiligd. Tot slot merkt de AP op dat de overtreding reeds 3,5 jaar plaatsvindt, en nog immer voortduurt. De AP acht dit buitengewoon ernstig.

223. Gelet op het bovenstaande ziet de AP op grond van artikel 7, aanhef en onder a, van de Boetebeleidsregels aanleiding om BZ een boete op te leggen en het basisbedrag van de boete van € 310.000 te verhogen naar € 390.000.

3.3.2 Nalatige aard van de inbreuk

224. BZ is verplicht om een beveiligingsniveau te hanteren dat passend is voor de aard en omvang van de verwerkingen die BZ uitvoert. Nu BZ al jarenlang geen passend beveiligingsniveau waarborgt, is de AP van oordeel dat BZ ernstig nalatig is geweest en nog steeds is in het treffen van passende beveiligingsmaatregelen en het controleren en aanpassen van deze maatregelen. Burgers die verplicht worden om persoonsgegevens af te staan, moeten ervan uit kunnen gaan dat BZ als overheidsinstantie de nodige maatregelen heeft getroffen én treft om persoonsgegevens goed te beschermen.

[187] https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-policy_en, onder 'Statistics on short-stay visas issued by the Schengen States', laatst geraadpleegd op 23 februari 2022.

225. De AP neemt daarbij ook in overweging dat BZ in eigen analyses (uit 2015 en 2020) reeds risico's op het gebied van informatiebeveiliging met betrekking tot NVIS heeft gedetecteerd en hier niet tijdig en/of onvoldoende actie op heeft ondernomen.[188] BZ heeft bijvoorbeeld in 2015 als in 2020 het risico gedefinieerd dat als gevolg van stroomstoringen apparatuur defect kan raken en dat ongeautoriseerden mutaties in NVIS kunnen uitvoeren als gevolg van onvoldoende governance m.b.t. autorisaties. De AP wijst op dit punt bovendien nog op de Verantwoordingsonderzoeken door de Algemene Rekenkamer in 2017, 2018 en 2019, waaruit volgt dat de onvolkomenheden in de informatiebeveiliging voor BZ dus ook op grond daarvan al bekend waren. De Algemene Rekenkamer heeft geconstateerd dat BZ risico's loopt op de aandachtsgebieden governance, de inrichting van de organisatie en het risicomanagement. Ook heeft de Algemene Rekenkamer geoordeeld dat BZ geen beheerkader heeft om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie goed te initiëren en te beheersen.

226. Gelet op het bovenstaande ziet de AP op grond van artikel 7, aanhef en onder b, van de Boetebeleidsregels aanleiding om het boetebedrag nog verder te verhogen, en wel naar een bedrag van € 440.000.

3.3.3 Categorieën van persoonsgegevens

227. De AP heeft vastgesteld dat BZ in het kader van het behandelen van aanvragen van Schengenvisa bijzondere persoonsgegevens verwerkt, zoals vingerafdrukken. Dergelijke gegevens kwalificeren als biometrische gegevens. Voor bijzondere persoonsgegevens is een nog hogere bescherming vereist. De AP heeft vastgesteld dat BZ voor een zeer omvangrijke groep betrokkenen onvoldoende een op risico afgestemd beveiligingsniveau hanteert voor deze categorie bijzondere persoonsgegevens.

228. Gelet op het bovenstaande ziet de AP op grond van artikel 7, aanhef en onder g, van de Boetebeleidsregels aanleiding om het boetebedrag te verhogen naar € 465.000.

3.4 Boetehoogte inzake overtreding van informatievoorziening aan betrokkenen

229. De verwerkingsverantwoordelijke dient de betrokkene informatie te verstrekken die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen, met inachtneming van de specifieke omstandigheden en de context waarin de persoonsgegevens worden verwerkt.[189] De AP heeft vastgesteld dat BZ in het kader van de informatievoorziening aan visumaanvragers geen melding maakt van het delen van persoonsgegevens met derde private partijen en hiermee artikel 13, lid 1, onder e, AVG overtreedt.

230. Zoals hiervoor vermeld, verwerkt BZ veel (bijzondere) persoonsgegevens. Het moet voor betrokkenen transparant zijn met welke (categorieën van) ontvangers BZ deze persoonsgegevens deelt. Gezien de soort persoonsgegevens, het feit dat honderdduizenden betrokkenen onvoldoende zijn geïnformeerd en de overtreding al 3,5 jaar duurt én nog steeds voortduurt, acht de AP het opleggen van een bestuurlijk boete gepast.

[188] Dossierstuk 3, bijlage 5a: Kwetsbaarheidsanalyse en IB-plan DCV; Schriftelijke Zienswijze BZ van 15 oktober 2021, bijlage 3.
[189] Zie overweging 60 van de AVG.

231. Voor wat betreft de hoogte van de boete neemt de AP in overweging dat de gevolgen van deze overtreding beperkt zijn. Dit leidt ertoe dat de AP uit oogpunt van evenredigheid aanleiding ziet om het basisbedrag van de boete van € 525.000 te verlagen naar € 100.000.

3.5 Verwijtbaarheid en evenredigheid voor beide overtredingen

232. Ingevolge artikel 5:46, tweede lid, van de Awb houdt de AP bij de oplegging van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten. Nu het hier gaat om een overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet en mag de AP verwijtbaarheid veronderstellen als het daderschap vaststaat.

233. BZ is verplicht om door middel van passende technische en organisatorische maatregelen een op risico afgestemd beveiligingsniveau te hanteren. Daarnaast dient BZ aan betrokkenen voldoende duidelijk te maken aan welke partijen het persoonsgegevens verstrekt. Het is aan BZ te verwijten dat het niet aan deze twee verplichtingen voldoet. De AVG, maar ook de VIS Verordening en BIO waaraan BZ moet voldoen, hebben ten aanzien van de beveiliging van de verwerking van persoonsgegevens nadrukkelijk beschreven dat organisaties een op risico afgestemd beveiligingsniveau moeten hanteren. Voorts bepaalt de AVG (en bieden de richtsnoeren omtrent transparantie) voldoende uitleg over de vraag welke informatie met betrokkenen gedeeld moet worden. Van BZ mag worden verwacht dat het zich van de voor hem geldende normen vergewist en daarnaar handelt.

234. Tot slot beoordeelt de AP ingevolge artikelen 3:4 en 5:46 van de Awb of de toepassing van haar beleid voor het bepalen van de hoogte van de boetes gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt.

235. De AP is van oordeel dat (de hoogte van) beide boetes evenredig is.[190] De AP heeft in dit oordeel onder andere de ernst van de inbreuken meegewogen en de mate waarin deze aan BZ kunnen worden verweten. Vanwege de aard van de persoonsgegevens, de duur van de overtredingen, het feit dat de overtredingen nog immer niet zijn beëindigd en de risico's die betrokkenen lopen, kwalificeert de AP de desbetreffende inbreuken op de AVG als ernstig. Voor wat betreft de hoogte van de boete inzake de overtreding over de informatievoorziening aan betrokkenen, heeft de AP reeds in paragraaf 3.4 gemotiveerd waarom de vastgestelde boete naar haar oordeel evenredig is.

236. Gezien het voorgaande ziet de AP geen aanleiding het bedrag van beide boetes op grond van de evenredigheid en de in de Boetebeleidsregels genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, verder te verhogen of te verlagen.

3.6 Conclusie

237. De AP stelt het totale boetebedrag vast op € 565.000.

[190] Zie voor de motivering ook paragraaf 3.3 en 3.4.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

4. Last onder dwangsom

238. Nu het gaat om een voortdurende overtreding van artikel 32, lid 1, AVG en artikel 13, lid 1, onder e, AVG dient BZ deze overtredingen zo spoedig mogelijk te beëindigen. De AP legt om die reden op grond van artikel 58, lid 2, aanhef en onder d, AVG jo. artikel 16, lid 1, UAVG en artikel 5:32, lid 1, Awb aan de Minister ook een last onder dwangsom op.

239. De AP gelast de minister van Buitenlandse Zaken in het kader van het behandelen van aanvragen van Schengenvisa:

1. de overtreding van artikel 32, lid 1, AVG te beëindigen door passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen.

> De Minister dient daartoe voor het nationaal informatiesysteem ten behoeve van het behandelen van Schengenvisa:
> a. een informatiebeveiligingsbeleid op te stellen waar ook in staat vermeld hoe BZ dit beleid periodiek gaat beoordelen en eventueel bij gaat stellen.
> b. noodplannen op te stellen en apparatuur te beschermen tegen ontregelingen in nutsvoorzieningen.
> c. voldoende waarborgen te nemen voor de fysieke beveiliging bij het werken in dit nationale systeem in openbare ruimtes.
> d. vast te leggen hoe BZ de regelmatige controle op toegangsrechten tot dit systeem waarborgt. Tevens betekent dit dat toegangsrechten regelmatig dienen te worden gecontroleerd en onverwijld worden aangepast wanneer uit een controle blijkt dat een medewerker ten onrechte is geautoriseerd om inzage te hebben tot persoonsgegevens.
> e. te waarborgen dat het mogelijk is om na te gaan en vast te stellen welke gegevens wanneer, door wie en met welk doel zijn verwerkt.
> f. vast te leggen op welke wijze BZ logging en de regelmatige controle hierop in dit systeem waarborgt. Tevens betekent dit dat BZ logbestanden regelmatig moet controleren.
>
> Het is aan de Minister, als verwerkingsverantwoordelijke, om de exacte invulling van bovengenoemde herstelmaatregelen te bepalen.

2. de overtreding van artikel 13, lid 1 onder e, AVG te beëindigen.

> De Minister dient dit bewerkstelligen door informatie over de ontvangers of categorieën van ontvangers van de persoonsgegevens aan betrokkenen (bij de verkrijging van de persoonsgegevens) te verstrekken.

Begunstigingstermijn en hoogte dwangsom t.a.v. onderdeel 1

240. De AP verbindt aan onderdeel 1 van deze last een begunstigingstermijn die eindigt op 24 oktober 2022.

241. Indien de minister voor Buitenlandse Zaken niet vóór het einde van deze begunstigingstermijn aan de last voldoet, verbeurt hij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van € 50.000 voor iedere twee weken na afloop van de laatste dag van de gestelde termijn waarop de minister van Buitenlandse Zaken nalaat aan onderdeel 1 van de last te voldoen, tot een maximum van € 500.000.

Begunstigingstermijn en hoogte dwangsom t.a.v. onderdeel 2

242. Wat betreft onderdeel 2 van deze last is de AP van oordeel dat met de uitvoering daarvan minder inspanningen gemoeid zijn. De AP verbindt daarom aan onderdeel 2 een begunstigingstermijn die eindigt 24 maart 2022.

243. Indien de minister voor Buitenlandse Zaken niet vóór het einde van deze begunstigingstermijn aan de last voldoet, verbeurt hij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van € 10.000 voor iedere (gehele) week, na afloop van de laatste dag van de gestelde termijn, waarop de minister van Buitenlandse Zaken nalaat aan onderdeel 2 van de last te voldoen, tot een maximum van € 300.000.

244. Naar het oordeel van de AP staat de hoogte van bovenstaande bedragen voor beide onderdelen van de last in redelijke verhouding tot de zwaarte van de door de overtredingen geschonden belangen, namelijk de bescherming van (bijzondere) persoonsgegevens en de transparantie over de verwerkingen naar betrokkenen. Voorts vindt de AP de bedragen voldoende hoog om BZ te bewegen de overtreding te beëindigen.

245. De bovenstaande maatregelen liggen in de macht van BZ om te nemen en de termijn om deze maatregelen te nemen acht de AP realistisch. Daarbij heeft de AP in aanmerking genomen dat een groot deel van de maatregelen die BZ bij onderdeel 1 moet nemen primair het opstellen van documentatie omvat. En voor wat betreft onderdeel 2 hoeft BZ de informatievoorziening slechts op een klein deel aan te passen.

Nacontrole

246. Indien BZ het verbeuren van dwangsommen direct na afloop van de begunstigingstermijn wenst te voorkomen, geeft de AP BZ in overweging om de documenten – waarmee BZ kan aantonen dat zij voldoet aan de last – tijdig, doch uiterlijk een week voor het einde van de begunstigingstermijn aan de AP ter beoordeling toe te sturen.

247. De AP geeft BZ tot slot in overweging om aan de hand van een concrete planning regelmatig mededeling te doen aan de AP over de voortgang van de maatregelen die zij neemt om te kunnen voldoen aan onderdeel 1 van de opgelegde last.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

De AP is tot de conclusie gekomen dat de minister van Buitenlandse Zaken, als verwerkingsverantwoordelijke bij het proces van het verlenen van Schengenvisa, betrokkenen ontoereikend informeert en de beveiliging van de verwerking van persoonsgegevens onvoldoende waarborgt. Gezien het feit dat minister van Buitenlandse Zaken zeer veel (gevoelige) persoonsgegevens verwerkt van honderdduizenden betrokkenen en de overtredingen na 3,5 jaar nog steeds voortduren, kwalificeert de AP de desbetreffende inbreuken op de AVG als ernstig.

Daarom legt de AP aan de minister van Buitenlandse Zaken een bestuurlijke boete op en daarnaast ook een last onder dwangsom.

- De AP legt aan de minister van Buitenlandse Zaken wegens overtreding van artikel 32, lid 1, AVG en artikel 13, lid 1 onder e, AVG een bestuurlijke boete op ten bedrage van: **€ 565.000** (zegge: vijfhonderdvijfenzestigduizend euro).[191]

- De AP gelast de minister van Buitenlandse Zaken in het kader van het behandelen van aanvragen van Schengenvisa:
  1. passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen en daarmee de overtreding van artikel 32, lid 1, AVG te beëindigen; en
  2. informatie over de ontvangers of categorieën van ontvangers van de persoonsgegevens aan betrokkenen (bij de verkrijging van de persoonsgegevens) te verstrekken en daarmee de overtreding van artikel 13, lid 1 onder e, AVG te beëindigen.

Indien de minister van Buitenlandse Zaken voor wat betreft onderdeel 1 niet vóór **24 oktober 2022** aan de last voldoet, verbeurt hij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van **€ 50.000** (zegge: vijftigduizend euro) voor iedere twee weken na afloop van de laatste dag van de gestelde termijn waarop de minister van Buitenlandse Zaken nalaat aan onderdeel 1 van de last te voldoen, tot een maximum van **€ 500.000** (zegge: vijfhonderdduizend euro).

Indien de minister voor Buitenlandse Zaken voor wat betreft onderdeel 2 niet vóór **24 maart 2022** aan de last voldoet, verbeurt hij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op een bedrag van **€ 10.000** (zegge: tienduizend euro) voor iedere (gehele) week, na afloop van de laatste dag van de gestelde termijn, waarop de minister van Buitenlandse Zaken nalaat aan onderdeel 2 van de last te voldoen, tot een maximum van **€ 300.000** (zegge: driehonderdduizend euro).

[191] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB). De boete dient overeenkomstig artikel 4:87, eerste lid, Awb binnen zes weken te worden betaald. Voor informatie en/of instructie over de betaling kan contact opgenomen worden met de eerder vermelde contactpersoon bij de AP.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

ir. M.J. Verdier
vicevoorzitter

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Ingevolge artikel 38 van de UAVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op. Het indienen van een bezwaarschrift schort de werking van de last onder dwangsom in dit besluit niet op. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag. Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'. Schrijf in uw bezwaarschrift ten minste:
- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

Datum
24 februari 2022

Ons kenmerk
[VERTROUWELIJK]

BIJLAGE 1

De volgende wetgeving vormt de basis van het wettelijk kader voor het onderhavige besluit:

- De **Algemene Verordening Gegevensbescherming** (AVG) bepaalt het algemene wettelijke kader voor de verwerking van persoonsgegevens, en het toezicht van de AP.
- De **Verordening betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf** (hierna: VIS-verordening[192]) geeft de specifieke kaders ten aanzien van het Europese Visum Informatie Systeem die de lidstaten gebruiken voor de onderlinge samenwerking bij het verstrekken van visa. Deze verordening regelt onder meer welke instanties verantwoordelijk zijn voor de gegevensverwerking via het VIS. De VIS Verordening schrijft voor welke gegevens van betrokkenen die een visum voor het Schengengebied aanvragen moeten worden opgenomen in het (nationale) visuminformatiesysteem.[193]
  De VIS Verordening beschrijft verder onder meer het doel en de functies van VIS en stelt eisen aan de partijen die verantwoordelijk zijn voor het gebruik van het VIS.[194] Dit omvat onder meer waarborgen op het gebied van integriteit en vertrouwelijkheid van de visuminformatie.[195]
- De **Verordening tot vaststelling van een gemeenschappelijke visumcode** (hierna: Visumcode)[196] schetst het algemene kader waar Lidstaten aan moeten voldoen in het kader van de aanvraag- en afgifte van visa.[197] Dit kader bepaalt onder meer welke gegevens moeten worden verwerkt voor het aanvragen en verstrekken van een visum voor het Schengengebied en diverse randvoorwaarden waar de Lidstaten bij dit proces aan moeten voldoen.

De AP heeft daarbij getoetst aan de volgende bepalingen:

Toelichting
De AVG bevat het algemene wettelijk kader voor de verwerking van persoonsgegevens. De voor dit besluit relevante normen uit de AVG zijn:

Definities
Artikel 4 AVG definieert een aantal basisbegrippen uit het gegevensbeschermingsrecht die in dit besluit zijn toegepast. Specifiek aan de orde gekomen is het begrip “persoonsgegevens”, de verwerking van persoonsgegevens, de verwerkingsverantwoordelijke en de verwerker.[198]

[192] Vindplaats: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32008R0767
[193] Zie artikel 9 van de VIS Verordening
[194] Zie bijvoorbeeld Artikelen 1 en 47 VIS Verordening
[195] Zie bijvoorbeeld Artikelen 1 en 28 VIS Verordening
[196] Vindplaats: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32009R0810
[197] Artikel 1 Visumcode: In deze verordening worden de procedures en voorwaarden vastgesteld voor de afgifte van visa voor de doorreis over het grondgebied van de lidstaten of een voorgenomen verblijf op het grondgebied van de lidstaten van ten hoogste drie maanden binnen een periode van zes maanden.
[198] Artikel 4, onderdeel 1, 2, 7 en 8.

Beginselen
Artikel 5 AVG beschrijft een aantal basisbeginselen waaraan in het algemeen voldaan moet worden om persoonsgegevens te verwerken in overeenstemming met de Verordening. Met name de beginselen transparantie, integriteit en vertrouwelijkheid spelen in dit geval een rol. Deze beginselen uit artikel 5 lid 1, onder a en onder f, van de AVG worden nader ingevuld door de specifiekere bepalingen in de AVG en, in de context van het onderhavige besluit, in het specifieke wettelijk kader met betrekking tot visuminformatiesystemen.

Beveiliging van de verwerking
Artikel 32 AVG schrijft – kort samengevat - voor dat verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moet nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. De algemene norm ten aanzien van het beveiligen van persoonsgegevens in artikel 32 AVG houdt in dat de verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, 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, passende technische en organisatorische maatregelen moet nemen om een op het risico afgestemd beveiligingsniveau te waarborgen.

Het begrip 'passend' duidt mede op een proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van deze gegevens.[199]

Om nader vast te kunnen stellen welke beveiligingsmaatregelen passend zijn gelden in de meeste sectoren meer specifieke standaarden voor informatiebeveiliging. De meeste relevante beveiligingsnormen voor de overheid zijn vervat in De Baseline Informatiebeveiliging Overheid (BIO).[200] De BIO is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

De AP merkt hierbij op dat de Baseline informatiebeveiliging overheid geldt sinds 1 januari 2020. Hierin zijn diverse baselines en normen uit diverse publieke sectoren verenigd tot een overkoepelende standaard voor de gehele overheid. Bij aanvang van het onderzoek in 2019 waren de relevante beveiligingsaspecten nader uitgewerkt in de Baseline Informatiebeveiliging Rijksdienst (hierna: BIR). De BIR is eveneens gebaseerd op de ISO 27002 standaarden en gold tot en met eind 2019.

De AP heeft de stand van de beveiliging van gegevensverwerking via het nationale visuminformatiesysteem ook specifiek getoetst aan artikel 32, lid 2, VIS Verordening. Dit artikel ziet op het nemen van beveiligingsmaatregelen, met inbegrip van een beveiligingsplan. Deze bepalingen uit de VIS

[199] Autoriteit Persoonsgegevens: Beleidsregels beveiliging van persoonsgegevens, februari 201 3, pag. 1 0 en Kamerstukken II 1 997-1 998, 25 892, nr. 3, pag. 99.
[200] Voor de overheid geldt de Baseline informatiebeveiliging overheid (BIO) als de leidende standaard, In deze casus is ook diens voorganger de BIR van belang omdat het BIR gold als standaard bij aanvang van het onderzoek tot en met eind 2019. Beide standaarden zijn gebaseerd op de ISO27000 normen op het gebied van informatiebeveiliging.

Verordening vormen een *lex specialis*, van wat in artikel 32 AVG wordt omschreven als 'passende maatregelen'.

De AP heeft gelet op de reikwijdte van het onderhavige besluit aan de volgende aspecten van dit artikel getoetst:

- Artikel 32, lid 2, VIS Verordening schrijft allereerst voor dat er een beveiligingsplan moet zijn om de vertrouwelijkheid en integriteit van de gegevensverwerking door middel van NVIS te waarborgen.
- De lidstaten moeten maatregelen treffen om gegevens fysiek te beschermen, met inbegrip van het opstellen van noodplannen ter bescherming van kritieke infrastructuur, volgens artikel 32 lid 2 onder a, VIS Verordening.
- Volgens artikel 32, lid 2, onder f, VIS Verordening moeten de lidstaten maatregelen treffen om te waarborgen dat degenen die bevoegd zijn om het VIS te raadplegen, uitsluitend toegang hebben tot de gegevens waarop hun toegangsbevoegdheid betrekking heeft, en uitsluitend met persoonlijke en unieke gebruikersidentiteiten en geheime toegangsprocedures (controle op de toegang tot de gegevens) Dit betekent dat er een passend autorisatiebeleid moet zijn voor de toegang tot NVIS en dat de in dat kader toegekende rollen beheerd moeten worden.
- Om in de organisatie te bewaken welke personen in aanmerking kunnen komen voor autorisaties voor gebruik van NVIS stelt artikel 32, lid 2, onder g, VIS Verordening als aanvullende waarborg dat alle autoriteiten met toegangsrecht tot het VIS-personeelsprofielen opstellen waarin de taken en verantwoordelijkheden worden omschreven van de personen die bevoegd zijn om gegevens in te zien, op te nemen, bij te werken, te wissen en te doorzoeken. Deze profielen moeten desgevraagd en onverwijld ter beschikking gesteld kunnen worden aan de AP.
- Artikel 32, tweede lid, onder i, VIS Verordening schrijft voor dat elke lidstaat met betrekking tot zijn nationale systeem, de nodige maatregelen vaststelt om te waarborgen dat het mogelijk is om na te gaan en vast te stellen welke gegevens wanneer, door wie en met welk doel in het VIS zijn verwerkt. Dat betekent dat BZ logbestanden moet bijhouden.
- In artikel 32, tweede lid, onder k, VIS Verordening is bepaald dat de doelmatigheid van de beveiligingsmaatregelen wordt gecontroleerd en met betrekking tot deze interne controle de nodige organisatorische maatregelen worden genomen om ervoor te zorgen dat de voorschriften van deze verordening worden nageleefd (controle op de logbestanden). Hierop sluiten ook de beveiligingsvoorschriften van artikel 32 AVG aan.

Integriteit bij de verwerking van visuminformatie
Artikel 28, lid 5, VIS Verordening schrijft voor dat personeel dat gegevens wil verwerken die in het VIS zijn opgeslagen, eerst een degelijke opleiding ontvangen over de regels inzake gegevensbeveiliging- en bescherming. Pas nadat deze opleiding is ontvangen kan personeel toestemming krijgen om in het VIS opgeslagen gegevens te verwerken. Dit artikel kan gezien worden als een concrete uitwerking van het beginsel van integriteit, dat is vastgelegd in artikel 5 lid 1, onder f, AVG. Op basis van dit beginsel moet een verwerkingsverantwoordelijke organisatorische waarborgen implementeren die zorgen voor de integriteit en vertrouwelijkheid van gegevensverwerking.

Informatie verstrekken aan betrokkene
Transparant zijn over gegevensverwerkingen is, zoals hierboven genoemd, één van de algemene beginselen voor een behoorlijke gegevensverwerking. Het informeren van de betrokkene over een

gegevensverwerking draagt bij aan transparantie. In dit kader zijn artikel 13 AVG en met name artikel 37 VIS Verordening relevant. Artikel 37 VIS Verordening vormt een verbijzondering van hetgeen is neergelegd in artikel 13 AVG. De AP heeft getoetst of bij aanvang van de procedure voor het aanvragen van een Schengenvisum voldaan is aan de verplichting om daarover adequate informatie te verstrekken aan de betrokkene die een visum aanvraagt.

Dit levert het volgende beeld op van relevante normen, gerangschikt van algemeen naar specifiek voor het visumproces.

Figuur 1: Schematische weergave wettelijk kader:

<table>
<tr><td>Algemeen</td><td colspan="3">Bijzonder →</td></tr>
<tr><td rowspan="5">Vertrouwelijkheid en integriteit van gegevensverwerking
Art 5 lid 1(f) AVG
Art 24 AVG
Art. 32 AVG</td><td rowspan="5">Gegevensbeveiliging NVIS:
Art. 32 lid 2 VIS Vo</td><td>Beveiligingsplan:
Art 32 lid 2 aanhef VIS Vo</td><td>BIO versie 1.0.4, deel 2, hoofdstuk 5 (p. 27):
normen onder paragraaf 5.1.</td></tr>
<tr><td>Fysieke beveiliging:
Art 32 lid 2 sub a VIS Vo</td><td>BIO versie 1.0.4, deel 2, hoofdstuk 11 (p. 43):
normen onder paragraaf 11.1 en 11.2.</td></tr>
<tr><td>Toegangsrechten en personeelsprofielen
Art 6 lid 1 VIS Vo
Art 32 lid 2 sub f en k jo VIS Vo
Art Art 32 lid 2 sub g VIS Vo.</td><td>BIO versie 1.0.4, deel 2, hoofdstuk 9 (p. 37):
normen onder paragraaf 9.2.</td></tr>
<tr><td>Logging (interne controle):
Art 32 lid 2 sub f, i en k VIS Vo.</td><td>BIO versie 1.0.4, deel 2, hoofdstuk 12 (p. 50):
normen onder paragraaf 12.4.</td></tr>
<tr><td>Beveiligingsincidenten (interne controle):
Art 32 lid 2 sub c, d en k VIS Vo.</td><td>BIO versie 1.0.4, deel 2, hoofdstuk 16 (p. 63):
normen onder paragraaf 16.1.</td></tr>
<tr><td>Art. 5 lid 1(f) (waarborg in de organisatie op gebied van integriteit en vertrouwelijkheid)</td><td>Opleiding personeel inzake gegevensbescherming:
Art 28 lid 5 Vis Vo
Art 38 lid 3 Visumcode.</td><td colspan="2"></td></tr>
<tr><td>Informatie aan betrokkenen
Art. 5 lid 1(a) AVG
Art. 13 AVG</td><td>Recht op informatie:
Art. 37 VIS Vo.</td><td colspan="2"></td></tr>
</table>