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

Aangetekend
Nationale Politie
T.a.v. de korpschef
[VERTROUWELIJK]
Nieuwe Uitleg 1
2514 BP DEN HAAG

Datum	Ons kenmerk	
6 februari 2017	z2015-00910	
	Contactpersoon	Uw kenmerk
	[VERTROUWELIJK]	[VERTROUWELIJK]

Onderwerp
Last onder dwangsom

Samenvatting

1. De Autoriteit Persoonsgegevens (AP) heeft ingevolge artikel 35, tweede lid van de Wet politiegegevens (Wpg) in samenhang bezien met artikel 60 van de Wet bescherming persoonsgegevens (Wbp) en artikel 44 van Verordening (EG) Nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (hierna: de Verordening) en artikel 60 van het Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (hierna: het Besluit) een ambtshalve onderzoek verricht naar het gebruik van het nationaal Schengeninformatiesysteem van de tweede generatie (N.SIS II) door de Nationale Politie (hierna: de NP). Naar aanleiding van dit onderzoek heeft de AP besloten om op grond van artikel 35, tweede lid van de Wpg, in samenhang bezien met artikel 65 van de Wbp en artikel 5:32, eerste lid, van de Algemene wet bestuursrecht (Awb) een last onder dwangsom op te leggen. Met de last onder dwangsom (hierna: het dwangsombesluit) beoogt de AP een einde te maken aan de geconstateerde overtredingen.

2. Het dwangsombesluit strekt tot het nemen van een aantal maatregelen. Binnen de begunstigingstermijn van zes maanden moet aan de last zijn voldaan. Bij het niet naleven van de last is de NP een dwangsom verschuldigd van € 12.500,-- (zegge: twaalfduizendvijfhonderd euro) voor iedere week dat de last niet (geheel) is uitgevoerd tot een maximum van € 200.000,-- (zegge: tweehonderdduizend euro).

3. De AP baseert het dwangsombesluit op het rapport definitieve bevindingen van 22 oktober 2015 (hierna: onderzoeksrapport) en de nadien door de NP verstrekte informatie.

Achtergrond en verloop van de procedure

4. Het onderzoeksrapport is op 22 oktober 2015 door de AP vastgesteld en aan de korpschef toegezonden. De openbare versie van het onderzoeksrapport is op 30 november 2015 op de website van de AP gepubliceerd.

5. Naar aanleiding van het onderzoeksrapport heeft de Minister van Veiligheid en Justitie de Tweede Kamer bij brief van 7 december 2015 erover geïnformeerd dat de NP maatregelen zal nemen teneinde de geconstateerde overtredingen te beëindigen.

6. Bij brief van 12 februari 2016 heeft de AP de NP in kennis gesteld van haar voornemen om handhavend op te treden en is de NP in de gelegenheid gesteld om een zienswijze ten aanzien van dit voornemen kenbaar te maken.

7. Op 18 februari 2016 is door de NP het Verbeterplan Wet politiegegevens en Informatiebeveiliging, concept versie 0.4 van februari 2016, aan de AP overgelegd. Het definitieve Verbeterplan Wet politiegegevens en Informatiebeveiliging, van maart 2016 (hierna: het verbeterplan) is op 9 mei 2016 aan de AP overgelegd. Dit verbeterplan bevat een overzicht van de maatregelen die de NP de komende jaren neemt om beter aan de Wpg te voldoen en bevat tevens de maatregelen op het gebied van informatiebeveiliging die moeten leiden tot het oplossen van de tekortkomingen die zijn geconstateerd in de onderzoeken naar het Visum Informatiesysteem (VIS) en N.SIS II. In het verbeterplan is vermeld dat met het uitvoeren van deze maatregelen de politie eind 2019 (de duur van het programma) grotendeels maar nog niet volledig de Wpg zal naleven.

8. Op 23 maart 2016 heeft de NP tijdens een hoorzitting een mondelinge zienswijze gegeven op het voornemen om handhavend op te treden. Van de hoorzitting is een verslag gemaakt. Dit verslag is bij brief van 11 mei 2016, in concept, aan de NP toegezonden om de NP in de gelegenheid te stellen om op het verslag te reageren.

9. Bij e-mail van 24 maart 2016 heeft de AP aan de NP verzocht om schriftelijk en concreet aan de hand van stukken te onderbouwen welke maatregen de NP heeft getroffen, dan wel voornemens is te treffen en binnen welke termijn de desbetreffende maatregelen zullen worden geïmplementeerd.

10. Bij brief van 6 april 2016, ontvangen op 11 april 2016, heeft de NP op dit verzoek gereageerd door nadere informatie te verstrekken.

11. Bij brief van 13 mei 2016, ontvangen op 17 mei 2016, heeft de NP gereageerd op het concept verslag van de hoorzitting. Het verslag van de hoorzitting is op 18 mei 2016 door de AP vastgesteld. Dit verslag en de reactie van de NP zijn aan dit dwangsombesluit gehecht.

12. Bij brief van 13 juli 2016 heeft de AP de NP erover geïnformeerd dat de AP medio september 2016 een besluit zal nemen met betrekking tot het onderhavige handhavingstraject.

13. Bij brief van 1 september 2016 heeft de NP de AP, samengevat, bericht dat de NP de opdracht zal uitzetten om een beveiligingsanalyse uit te voeren naar het proces van 'signaleringen' binnen de NP. De beveiligingsanalyse zal in september 2016 aanvangen. De verwachting is dat deze analyse binnen vier maanden kan worden afgerond. In dit verband heeft de NP verzocht om de besluitvorming met betrekking tot het handhavingstraject op te schorten.

14. Bij brief van 5 september 2016 heeft de AP de NP bericht dat zij geen aanleiding ziet om de besluitvorming op te schorten.

15. Bij brief van 13 september 2016 heeft de NP de AP bericht dat zij sinds begin 2016 bezig is om de eerdere toezeggingen, die onderdeel uitmaken van het verbeterprogramma, uit te voeren. In de bijlage bij deze brief heeft de NP met betrekking tot de geconstateerde overtredingen een toelichting gegeven op de aanpak van deze overtredingen, de stand van zaken en de vervolgplanning. Daarnaast heeft de NP de AP verzocht om in de gelegenheid te worden gesteld om tijdens een gesprek een toelichting te geven op de door de NP te treffen maatregelen en heeft de NP nogmaals verzocht om de besluitvorming over eventuele handhaving op te schorten.

16. Naar aanleiding van laatstgenoemde brief heeft de AP de NP uitgenodigd voor een gesprek op 4 oktober 2016. Ten behoeve van dit gesprek is bij e-mail van 29 september 2016 een aantal vragen aan de NP voorgelegd.

17. Bij e-mail van 3 oktober 2016 heeft de NP een reactie gegeven op laatstgenoemde e-mail en heeft de NP stukken toegezonden die zien op de procedure met betrekking tot het beleid ten aanzien van informatiebeveiligingsincidenten.

18. Het gesprek tussen de AP en de NP heeft plaatsgevonden op 4 oktober 2016. Tijdens dit gesprek heeft de NP een mondelinge toelichting gegeven op de door de NP getroffen en nog te treffen maatregelen. Van dit gesprek is een verslag opgesteld.

19. Per e-mail van 7 oktober 2016 heeft de NP nog een document toegezonden met betrekking tot het beleid ten aanzien van informatiebeveiligingsincidenten.

20. Bij brief van 10 oktober 2016, toegezonden per e-mail van gelijke datum, heeft de NP – zoals was toegezegd tijdens het gesprek op 4 oktober 2016 – de AP een schriftelijke toelichting gegeven over de context waarbinnen de ontwikkelingen op het gebied van beveiliging en de vernieuwing van de informatievoorziening bij de NP plaatsvinden.

21. Op 5 december 2016 heeft de AP, op verzoek van de NP, de NP in de gelegenheid gesteld om een mondelinge toelichting te geven op de context waarbinnen de NP opereert. Tijdens dit gesprek is afgesproken dat de NP begin januari 2017 aan de hand van stukken inzicht geeft in de door haar getroffen en nog te treffen maatregelen om de geconstateerde overtredingen weg te nemen en om inzicht te geven in de stand van zaken daaromtrent.

22. Op 9 januari 2017 heeft de NP naar aanleiding van het gesprek van 5 december 2016 een aantal stukken overgelegd, waarbij een mondelinge toelichting is gegeven. De stukken hebben, samengevat, betrekking op de incidentenrapportage 2015, het autorisatieproces, de informatiebeveiligingsarchitecteur en de voortgangsrapportage op het verbeterplan Q3 2016. Verder is door de NP toegelicht dat, alhoewel de stand van zaken is dat de NP wat achter loopt op schema, de verwachting is dat de eindplanning zoals is aangegeven in de bijlage bij de brief van 13 september 2016, kan worden gerealiseerd.

23. Bij e-mail van 31 januari 2017 heeft de NP het beveiligingsplan 2017-2019, versie 1. 0, status definitief, aan de AP toegezonden. Dit beveiligingsplan heeft onder meer betrekking op de verwerking van politiegegevens in het kader van N.SIS II.

Onderzoeksrapport

24. Aanleiding voor deze last onder dwangsom vormen de bevindingen in het onderzoeksrapport van 22 oktober 2015. De AP heeft in het onderzoeksrapport geconcludeerd dat de NP in strijd handelt met de Wpg, de Verordening en het Besluit wat betreft de beveiligings- en opleidingsvoorschriften die zien op N.SIS II.

25. Ten aanzien van de beveiligingsvoorschriften heeft de AP geconcludeerd dat de NP in het kader van de gegevensverwerking in N.SIS II:
    a. geen beveiligingsplan heeft vastgesteld;
    b. de toegangsrechten niet juist heeft geregeld en geen profielen heeft opgesteld;
    c. geen specifieke schriftelijke procedure heeft vastgelegd met betrekking tot de autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND. Evenmin voert de NP (doorlopende) controles uit op de toegekende autorisaties en zijn er geen afspraken gemaakt met de regionale eenheden over de af te leggen verantwoording;
    d. geen snelle doeltreffende en ordelijke respons op een N.SIS II informatiebeveiligingsincident heeft neergelegd in een procedure.
    e. geen (doorlopende) controles uitvoert op de logbestanden en niet alle applicaties logt.

26. Ten aanzien van de opleidingsvoorschriften heeft de AP geconcludeerd dat het personeel van de NP geen specifieke en degelijke opleiding krijgt met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties. Voorts is geconcludeerd dat evenmin in de algemene opleiding aandacht wordt besteed aan N.SIS II.

Wettelijk kader

27. Het relevante juridisch kader wordt met name gevormd door de Wpg, de Verordening en het Besluit. Dit kader is opgenomen in bijlage I van dit dwangsombesluit.

Zienswijze NP

28. Naar aanleiding van het voornemen van de AP om handhavend op te treden heeft de NP tijdens de hoorzitting van 23 maart 2016 mondeling een zienswijze gegeven. Samengevat komt deze zienswijze erop neer dat zij de in het onderzoeksrapport geconstateerde conclusies onderschrijft. De NP heeft in haar zienswijze erop gewezen dat zij belang hecht aan een goede beveiliging van informatie en de daarmee samenhangende waarborgen voor privacy. Ten einde de geconstateerde overtredingen te beëindigen heeft de NP aangekondigd maatregelen te treffen.

Beoordeling

29. De AP stelt vast dat de NP toegangsrechten heeft tot N.SIS II en in dat kader politiegegevens verwerkt. Dit betekent, gelet op het bepaalde in artikel 2, eerste lid, van de Wpg, dat de Wpg van toepassing is. Voorts zijn het Besluit en de Verordening op de gegevensverwerking van toepassing. De Verordening en het Besluit bevatten gemeenschappelijke bepalingen over de architectuur, de financiering en de verantwoordelijkheden, alsmede algemene gegevensverwerkings- en -beschermingsregels voor SIS II. Afgezien van deze gemeenschappelijke regels bevat het Besluit specifieke bepalingen over de verwerking van SIS II-gegevens ten behoeve van de samenwerking van justitie en politie in strafzaken, terwijl de Verordening regels bevat voor de verwerking van SIS II-gegevens ten behoeve van de uitvoering van het beleid op het gebied van het vrije verkeer van personen dat deel uitmaakt van het Schengenacquis.

30. Op grond van artikel 4, derde lid, van de Wpg dient de NP passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via directe geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's van de verwerking en de aard van de politiegegevens.

31. De AP sluit voor de beoordeling of sprake is van passende technische en organisatorische beveiligingsmaatregelen aan bij de nadere invulling die daaraan wordt gegeven in de Code voor Informatiebeveiliging, de NEN-ISO/IEC 27002:2013 norm (hierna de NEN-norm). De NEN-norm is een norm waarin internationaal geldende maatregelen voor informatiebeveiliging nader zijn uitgewerkt. Als een organisatie voldoet aan de NEN-norm, gaat de AP ervan uit dat ook wordt voldaan aan artikel 4, derde lid van de Wpg.[1] Daarnaast sluit de AP, daar waar sprake is van een bijzondere regeling voor de politie, aan bij de Regeling informatiebeveiliging politie (Rip). De Rip is een ministeriële regeling die berust op artikel 23, eerste lid, onder b, van de Politiewet 2012. Op grond van artikel 2, eerste lid, van de Rip is deze regeling van toepassing op het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

[1] CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 2

Ten aanzien van het beveiligingsplan

32. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Dit betekent gelet op artikel 4, aanhef en onder e, van de Rip onder meer dat de NP een (informatie)beveiligingsplan dient vast te stellen dat betrekking heeft op N.SIS II. In dit beveiligingsplan dient expliciet te worden opgenomen welke maatregelen de NP treft om de verwerkte gegevens te beveiligen.[2] De noodzaak om een beveiligingsplan vast te stellen volgt ook uit artikel 10, eerste lid, aanhef, van het Besluit en artikel 10, eerste lid, aanhef, van de Verordening.[3]

33. Tijdens het onderzoek zijn door de NP aan de AP stukken overgelegd die betrekking hebben op de beveiligingsmaatregelen binnen de NP. De AP heeft op grond van deze stukken geconcludeerd dat deze stukken niet kunnen worden aangemerkt als een beveiligingsplan dat betrekking heeft op N.SIS II. Tijdens de hoorzitting van 23 maart 2016 heeft de NP, tevens bevestigd bij brief van 13 mei 2016, aan de AP medegedeeld dat zij de conclusies uit het onderzoeksrapport niet betwist. Daarnaast is door de NP toegelicht dat zij over verschillende documenten beschikt die betrekking hebben op het beveiligingsplan, maar dat nog moet worden beoordeeld welke documenten moeten worden herzien en geïndexeerd kunnen worden. Ten einde de geconstateerde overtredingen te doen beëindigen heeft de NP in het verbeterplan en in de bijlage bij de brief van 13 september 2016 aangekondigd maatregelen te treffen.[4] Bij e-mail van 31 januari 2017 heeft de NP het beveiligingsplan 2017-2019, versie 1.0, status definitief, aan de AP toegezonden. Dit beveiligingsplan heeft onder meer betrekking op de verwerking van politiegegevens in het kader van N.SIS II. Met de toezending van dit beveiligingsplan stelt de AP vast dat op dit punt wordt voldaan aan artikel 4, derde lid, van de Wpg, in samenhang bezien met artikel 4, aanhef en onder e, van de Rip.

Ten aanzien van de toegangsrechten tot N.SIS II en de personeelsprofielen

34. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Toegangsbeveiliging door middel van autorisaties is hiervan een uitwerking en is nader bepaald in artikel 6 van de Wpg. De NP dient op grond van artikel 6, eerste lid, van de Wpg een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. De vereisten van zorgvuldigheid en evenredigheid vormen het uitgangspunt van het systeem van autorisaties. Deze vereisten brengen onder meer mee dat personen niet ruimer worden geautoriseerd dan nodig voor de vervulling van hun taken.[5] Dit betekent dat de autorisaties dienen te worden gekoppeld aan een bepaalde functie of functionaliteit. Daartoe dient de NP profielen op te stellen waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om persoonsgegevens in N.SIS II in te zien en te verwerken.

[2] Zie ook NEN-ISO-IEC 27002:2013, paragraaf 5.1.1 en CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22
[3] Opgemerkt moet worden dat in artikel 10, eerste lid, aanhef, van het Besluit spreekt over een *beveiligingsplan*, terwijl artikel 10, eerste lid, aanhef van de Verordening spreekt over een *veiligheidsplan*. Met deze begrippen wordt hetzelfde bedoeld.
[4] Ten aanzien van alle door de NP aangekondigde maatregelen moet evenwel worden opgemerkt dat deze onvoldoende concreet zijn om een oordeel te kunnen geven m.b.t. de vraag of met deze maatregelen de geconstateerde overtredingen worden opgeheven.
[5] Tweede Kamer, vergaderjaar 2005–2006, 30 327, nr. 3, p. 34

Het opstellen van personeelsprofielen dient onder meer als middel om te kunnen beoordelen of de autorisaties juist geregeld zijn. Dit volgt ook uit de NEN-norm[6], artikel 10, eerste lid, onder f en g, van de Verordening en artikel 10, eerste lid, onder f en g, van het Besluit.

35. De AP heeft in het onderzoeksrapport vastgesteld dat de NP een organisatie is met toegangsrecht tot N.SIS II en dat zij beheerder is van de op N.SIS II aangesloten partijen. In het onderzoeksrapport is geconcludeerd dat de NP de toegangsrechten niet juist heeft geregeld. In dit verband is vastgesteld dat niet alle partijen die toegangsrechten hebben tot N.SIS II in de autorisatiematrix staan en dat bij de in de matrix genoemde partijen niet alle typen van toegangsrechten worden vermeld. Voorts is geconcludeerd dat de NP geen profielen heeft opgesteld waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om persoonsgegevens in N.SIS II te zien en te verwerken. Tijdens de hoorzitting van 23 maart 2016, tevens bevestigd bij brief van 13 mei 2016, heeft de NP medegedeeld dat zij de conclusies uit het onderzoeksrapport niet betwist. Bij brief van 13 september 2016 heeft de NP een bijlage gevoegd waarin maatregelen zijn opgenomen die de NP voornemens is te treffen ten einde de geconstateerde overtredingen te doen beëindigen. Deze maatregelen hebben een implementatietermijn die loopt tot en met januari 2017. Op 9 januari 2017 heeft de NP ten aanzien hiervan mondeling toegelicht dat de NP op deze planning achterloopt en dat dit niet in januari 2017, maar in juni 2017 gerealiseerd kan worden. Gelet hierop stelt de AP vast dat de NP thans nog steeds in strijd handelt met artikel 6, eerst lid, in samenhang bezien met artikel 4, derde lid, van de Wpg.

Ten aanzien van de toekenning van autorisaties en de controle hierop

36. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Toegangsbeveiliging door middel van autorisaties is hiervan een uitwerking en is nader bepaald in artikel 6 van de Wpg. De NP dient op grond van artikel 6, eerste lid, van de Wpg een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Op grond van artikel 6, tweede lid, van de Wpg worden politiegegevens slechts verwerkt door ambtenaren van politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt. Om controle op de toegangsbeveiliging mogelijk te maken is in artikel 32 Wpg de protocolplicht neergelegd. Artikel 32, eerste lid, onder c, van de Wpg bepaalt dat de verantwoordelijke zorg draagt voor de schriftelijke vastlegging van de toekenning van de autorisaties, zoals bedoeld in artikel 6 van de Wpg.
Deze wettelijke bepalingen zijn nader uitgewerkt in de NEN-norm, waarbij ten behoeve van het beheer van toegangsrechten is voorgeschreven dat een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.[7] Voorts geldt dat de toegangsrechten van gebruikers regelmatig dienen te worden beoordeeld.[8] Dit volgt ook uit artikel 10, eerste lid, onder f en k, van de Verordening en artikel 10, eerste lid, onder f en k, van het Besluit.

[6] NEN-ISO-IEC 27002:2013, paragraaf 9.1.1 en paragraaf 9.2.1.
[7] NEN-ISO-IEC 27002:2013, paragraaf 9.2.1. Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22
[8] NEN-ISO-IEC 27002:2013, paragraaf 9.2.5

37. De AP heeft in het onderzoeksrapport geconcludeerd dat de (Landelijke Eenheid van de) NP geen formeel vastgestelde procedure heeft die betrekking heeft op de autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND die in het kader van N.SIS II persoonsgegevens verwerken. Daarnaast is in dit kader geconcludeerd dat de NP geen (periodieke) controle uitvoert op de aan de functioneel beheerders van de op N.SIS II aangesloten partijen en de aan medewerkers van de IND toegekende autorisaties in het kader van N.SIS II.

38. Tijdens de hoorzitting van 23 maart 2016, tevens bevestigd bij brief van 13 mei 2016, heeft de NP aan de AP medegedeeld dat zij de conclusies uit het onderzoeksrapport niet betwist. Bij de brief van 13 september 2016 heeft de NP een bijlage gevoegd waarin maatregelen zijn opgenomen die de NP voornemens is te treffen ten einde de geconstateerde overtredingen te doen beëindigen. Deze maatregelen hebben een implementatietermijn die loopt tot en met januari 2017. Op 9 januari 2017 heeft de NP ten aanzien hiervan mondeling toegelicht dat de NP op deze planning achterloopt en dat dit niet in januari 2017, maar in juni 2017 gerealiseerd kan worden. Gelet hierop stelt de AP ten aanzien van toekenning van autorisaties vast dat de NP nog geen formeel vastgestelde procedure heeft die betrekking heeft op autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND die in het kader van N.SIS II persoonsgegevens verwerken. De NP handelt hierdoor thans nog steeds in strijd met artikel 6, eerst lid, in samenhang met artikel 4, derde lid, van de Wpg, de NEN-norm[9], artikel 10, eerste lid, onder f, van de Verordening en artikel 10, eerste lid, onder f, van het Besluit. Ten aanzien van de (doorlopende) controle op toegekende autorisaties stelt de NP vast dat de NP geen (periodieke) controle uitvoert op de aan de functioneel beheerders van de op N.SIS II aangesloten partijen en aan de medewerkers van de IND toegekende autorisaties. De NP handelt ook in zoverre hierdoor nog steeds in strijd met artikel 6, eerst lid, in samenhang bezien met artikel 4, derde lid, van de Wpg en artikel 32, eerste lid, onder c, van de Wpg.

Ten aanzien van de beveiligingsincidenten

39. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Dit betekent gelet op artikel 3, tweede lid, onder f, van de Rip onder meer dat de NP een beleidsdocument dient vast te stellen waarin wordt neergelegd de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door politieambtenaren gemeld worden, de politieambtenaar bij wie deze inbreuken worden gemeld en de wijze waarop deze worden afgehandeld. De NEN-norm vult dit nader in, namelijk 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 directieverantwoordelijkheden en -procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.[10] Dit volgt ook uit artikel 10, eerste lid, onder d, van de Verordening en artikel 10, eerste lid, onder d, van het Besluit.

[9] NEN-ISO-IEC 27002:2013, paragraaf 9.1.1. en paragraaf 9.2.1. Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22
[10] NEN-ISO-IEC 27002:2013, paragraaf 16.1.1

40. In het onderzoeksrapport heeft de AP geconcludeerd dat de NP geen procedure heeft vastgesteld ten aanzien van het beheer van informatiebeveiligingsincidenten in het kader van N.SIS II en dat derhalve geen sprake is van een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten. Tijdens de hoorzitting van 23 maart 2016, tevens bevestigd bij brief van 13 mei 2016, heeft de NP aan de AP medegedeeld dat zij de conclusies uit het onderzoeksrapport niet betwist. Ten einde de geconstateerde overtredingen te doen beëindigen heeft de NP in de bijlage bij het verbeterplan en in de bijlage bij de brief van 13 september 2016 aangekondigd maatregelen te treffen. Bij e-mail van 3 oktober 2016 heeft de NP stukken toegezonden die zien op de procedure met betrekking tot het beleid ten aanzien van informatiebeveiligingsincidenten. Dit beleid is mondeling toegelicht tijdens een gesprek met de AP op 4 oktober 2016. Bij e-mail van 7 oktober 2016 heeft de NP nog een document toegezonden dat betrekking heeft op het beleid ten aanzien van informatiebeveiligingsincidenten. Met de toezending van deze documenten en de tijdens het gesprek van 4 oktober 2016 gegeven toelichting, waarin is verklaard dat de vastgestelde procedure met betrekking tot het beleid ten aanzien van informatiebeveiligingsincidenten ook betrekking heeft op de verwerking van gegevens in het kader van N.SIS II, stelt de AP vast dat op dit punt wordt voldaan aan artikel 4, derde lid, van de Wpg in samenhang bezien met artikel 3, tweede lid, onder f, van de Rip.

Ten aanzien van de logging en de (doorlopende) controles op het gebruik van N.SIS II

41. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Dit betekent, gelet op de invulling die de NEN-norm[11] daaraan geeft, dat logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.[12] Dit volgt ook uit artikel 10, eerste lid, onder i en k, van de Verordening en artikel 10, eerste lid, onder i en k, van het Besluit.

42. In het onderzoeksrapport heeft de AP geconcludeerd dat de NP de logbestanden niet regelmatig controleert. Vastgesteld is dat de controle op de logging slechts (achteraf) plaatsvindt in het geval sprake is van veiligheidssignalen, integriteitsonderzoeken, klachten of een technische storing. De logbestanden worden niet periodiek proactief gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van politiegegevens. Daarnaast heeft de AP geconcludeerd dat gewijzigde autorisaties in N.SIS II niet door de NP worden gelogd. Tijdens de hoorzitting van 23 maart 2016, tevens bevestigd bij brief van 13 mei 2016, heeft de NP aan de AP medegedeeld dat zij de conclusies uit het onderzoeksrapport niet betwist. Ten einde de geconstateerde overtredingen te doen beëindigen heeft de NP in de bijlage bij de brief van 13 september 2016 aangekondigd maatregelen te treffen, waarbij een implementatietermijn is genoemd die loopt tot en met april 2017. Tijdens het gesprek op 4 oktober 2016 heeft de NP toegelicht dat de controle op logbestanden nog niet proactief bij de NP kan plaatsvinden, omdat de handeling instemmingsplichtig is op grond van de Wet op de ondernemingsraden, en de ondernemingsraad hiermee nog niet heeft ingestemd.

[11] NEN-ISO-IEC 27002:2013, paragraaf 12.4.1.
[12] Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22

43. Gelet op het vorenstaande stelt de AP vast dat de NP vanwege het ontbreken van een regelmatige proactieve controle op de logbestanden en vanwege het feit dat gewijzigde of verwijderde autorisaties in N.SIS II niet door de NP worden gelogd, thans nog steeds in strijd handelt met artikel 4, derde lid, van de Wpg.

Ten aanzien van de opleidingsvoorschriften

44. Op grond van artikel 4, derde lid, van de Wpg dient de NP – samengevat – passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang. Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie beveiligen. Het bieden van een passende opleiding kan worden aangemerkt als een organisatorische maatregel en betekent, gelet op de invulling die de NEN-norm[13] daaraan geeft, dat alle werknemers van de organisatie en, voor zover relevant, contractanten een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, behoren te krijgen.[14] Het bieden van een passende opleiding volgt ook uit artikel 14 van de Verordening en artikel 14 van het Besluit.

45. Ten aanzien van de door de NP geboden opleiding heeft de AP in het onderzoeksrapport geconcludeerd dat het personeel van de NP geen specifieke en degelijke opleiding krijgt met betrekking tot de regels inzake gegevensbeveiliging en -bescherming van N.SIS II en de ter zake doende strafbare feiten en sancties en dat evenmin in de algemene opleiding aandacht wordt besteed aan N.SIS II.

46. Naar aanleiding van dit rapport heeft de NP, zowel tijdens de hoorzitting als bij brief van 6 april 2016, een nadere toelichting gegeven op het opleidingsprogramma van de NP. In dit verband is, samengevat toegelicht dat de generieke opleidingen/cursussen, die in samenspraak met de Politie Academie worden ontwikkeld, geen specifieke N.SIS II aspecten bevatten, maar dat daar waar medewerkers specifieke rechten hebben om signaleringen binnen N.SIS II aan te maken of te verwijderen, de NP gebruik maakt van een ′train de trainer concept′, waarbij gebruik wordt gemaakt het Handboek Gebruikers SMC. Daarnaast is toegelicht dat tijdens de opleidingen aandacht wordt besteed aan de ter zake doende strafbare feiten en sancties met betrekking tot het informatiebeveiligingsbeleid.

47. Gelet op hetgeen tijdens de hoorzitting naar voren is gebracht en de nadien ingediende stukken, stelt de AP in dit kader vast dat thans geen sprake meer is van een overtreding in de zin van artikel 4, derde lid, van de Wpg.

Last onder dwangsom en begunstigingstermijn

48. De AP besluit tot het opleggen van een last onder dwangsom op grond van artikel 35, tweede lid van de Wpg, in samenhang bezien met artikel 65 van de Wbp en artikel 5:32, eerste lid, van de Awb. Deze last

[13] NEN-ISO-IEC 27002:2013, paragraaf 7.2.2.
[14] Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22

onder dwangsom is gericht op het beëindigen van de geconstateerde overtredingen en het voorkomen van herhaling, zoals bedoeld in artikel 5:2, eerste lid, onder b, van de Awb.

49. De AP gelast de NP om binnen de, hierna genoemde, begunstigingstermijn maatregelen te nemen teneinde het onrechtmatige karakter van de verwerking weg te nemen. Dit houdt in dat NP binnen deze termijn ervoor dient te zorgen dat verdere overtreding van artikel 4, derde lid, van de Wpg, artikel 6, eerste lid, van de Wpg en artikel 32, eerste lid, onder c, van de Wpg achterwege blijft.

50. Concreet betekent dit dat de NP een formeel vastgestelde procedure dient te hebben die betrekking heeft op de autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND. Hierbij wijst de AP erop dat het moet gaan om een formele registratie- en afmeldingsprocedure om toewijzing van toegangsrechten mogelijk te maken.[15] Deze procedures dienen alle fasen in de levenscyclus van de gebruikerstoegang, gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben te omvatten.[16]

51. Tevens dient de NP personeelsprofielen vast te stellen waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om persoonsgegevens in N.SIS II in te zien en te verwerken.[17]

52. Voorts dient de NP ervoor zorg te dragen dat een periodieke controle wordt uitgevoerd op de autorisaties die zijn toegekend aan de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND.[18]

53. Verder is vereist dat de NP gewijzigde autorisaties in N.SIS II logt.[19]

54. Daarnaast dient de NP in het kader van N.SIS II logbestanden regelmatig te controleren op indicaties van onrechtmatige toegang of onrechtmatig gebruik van politiegegevens. Dit betekent dat niet slechts achteraf een controle (in het geval sprake is van veiligheidssignalen, integriteitsonderzoeken, klachten of een technische storing) dient plaats te vinden, maar dat de logbestanden ook regelmatig proactief moeten worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van politiegegevens.[20]

<u>Begunstigingstermijn</u>

55. Artikel 5:32a, tweede lid, van de Awb bepaalt dat een begunstigingstermijn wordt gesteld ‘gedurende welke de overtreder de last kan uitvoeren zonder dat een dwangsom wordt verbeurd’. In de Memorie van

[15] NEN-ISO-IEC 27002:2013, paragraaf 9.2.1.
[16] Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22
[17] NEN-ISO-IEC 27002:2013, paragraaf 9.1.1 en paragraaf 9.2.1.
[18] NEN-ISO-IEC 27002:2013, paragraaf 9.2.5
[19] NEN-ISO-IEC 27002:2013, paragraaf 12.4.1. Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22
[20] NEN-ISO-IEC 27002:2013, paragraaf 12.4.1. Zie ook CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, p. 22

Toelichting bij de Awb wordt benadrukt dat deze termijn zo kort mogelijk moet zijn, maar lang genoeg om de last te kunnen uitvoeren.[21]

56. De AP verbindt aan de last onder dwangsom een begunstigingstermijn van zes maanden. De AP heeft bij het vaststellen van de begunstigingstermijn rekening gehouden met de context waarbinnen de ontwikkelingen op beveiliging en de vernieuwing van informatievoorziening bij de NP plaatsvinden, zoals door de NP is toegelicht bij brief van 10 oktober 2016 en nadien mondeling namens de NP is toegelicht. Naar het oordeel van de AP is een termijn van zes maanden redelijk met het oog op het beëindigen van de geconstateerde overtredingen en het voorkomen van verdere overtreding.

57. Artikel 5:32b, derde lid, van de Awb schrijft voor dat de dwangsombedragen in redelijke verhouding staan tot de zwaarte van het geschonden belang en tot de beoogde werking van de dwangsom. Bij dat laatste is van belang dat van een dwangsom een zodanige prikkel moet uitgaan dat aan de last wordt voldaan.

58. Indien de NP niet binnen zes maanden de geconstateerde overtredingen beëindigt, verbeurt zij een dwangsom. De AP stelt de hoogte van deze dwangsom vast op € 12.500,-- voor iedere week dat de last niet (geheel) is uitgevoerd tot een maximum van € 200.000,--. Naar het oordeel van de Autoriteit staat de hoogte van deze bedragen in redelijke verhouding tot de zwaarte van het door de overtreding geschonden belang - de bescherming van politiegegevens en van de persoonlijke levenssfeer van de betrokkenen - en zijn deze (voorts) voldoende hoog om de NP te bewegen de overtredingen te beëindigen.

[21] Kamerstukken II 1993/94, 23 700, nr. 3, p.163.

Datum
6 februari 2017

Ons kenmerk
z2015-00910

Dictum

De AP legt aan de NP een last onder dwangsom op met de volgende inhoud:

De NP dient **binnen zes maanden na dagtekening van dit besluit** in het kader van de gegevensverwerking in N.SIS II maatregelen te nemen die ertoe leiden dat:

I. de NP een procedure vaststelt die betrekking heeft op autorisaties voor de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND die in het kader van N.SIS II persoonsgegevens verwerken;
II. de NP personeelsprofielen vaststelt waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om persoonsgegevens in N.SIS II in te zien en te verwerken;
III. de NP ervoor zorgdraagt dat een periodieke controle wordt uitgevoerd op de autorisaties die zijn toegekend aan de functioneel beheerders van de op N.SIS II aangesloten partijen en de medewerkers van de IND;
IV. gewijzigde autorisaties worden gelogd;
V. de logbestanden regelmatig proactief worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van politiegegevens.

Indien de NP niet uiterlijk zes maanden na datum van onderhavig dwangsombesluit de maatregelen heeft uitgevoerd, verbeurt de NP een dwangsom van € 12.500,-- (zegge: twaalfduizendvijfhonderd euro) voor iedere week dat de last niet (geheel) is uitgevoerd tot een maximum van € 200.000,-- (zegge: tweehonderdduizend euro).

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

mr. A. Wolfsen
Voorzitter

Rechtsmiddelen

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, onder vermelding van “Awb-bezwaar” op de envelop.

Datum
6 februari 2017

Ons kenmerk
z2015-00910

Bijlage 1 – wettelijk kader

Wet bescherming persoonsgegevens (Wbp)

Artikel 51, eerste lid, van de Wbp (voor zover relevant):
1. Er is een College bescherming persoonsgegevens dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Tevens houdt het College toezicht op de verwerking van persoonsgegevens in Nederland, wanneer de verwerking plaatsvindt overeenkomstig het recht van een ander land van de Europese Unie.
[…]

Artikel 60, eerste en tweede lid, van de Wbp:
1. Het College kan ambtshalve of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.
2. Het College brengt zijn voorlopige bevindingen ter kennis van de verantwoordelijke of de groep van verantwoordelijken die bij het onderzoek zijn betrokken en stelt hen in de gelegenheid hun zienswijze daarop te geven. Houden de voorlopige bevindingen verband met de uitvoering van enige wet, dan brengt het College deze tevens ter kennis van Onze Minister die het aangaat.
[…]

Artikel 61, eerste en vierde lid, van de Wbp (voor zover relevant):
1. Met het toezicht op de naleving als bedoeld in artikel 51, eerste lid zijn belast de leden en buitengewone leden van het College, de ambtenaren van het secretariaat van het College, alsmede de bij besluit van het College aangewezen personen.
[…]
4. Het College is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht, voor zover het betreft de verplichting tot het verlenen van medewerking aan een bij of krachtens het eerste lid aangewezen ambtenaar.
[…]

Artikel 65 van de Wbp:
Het College is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de bij of krachtens deze wet gestelde verplichtingen.

Algemene wet bestuursrecht (Awb)

Artikel 5:32, eerste lid, van de Awb:
1. Een bestuursorgaan dat bevoegd is een last onder bestuursdwang op te leggen, kan in plaats daarvan aan de overtreder een last onder dwangsom opleggen.

Datum
6 februari 2017

Ons kenmerk
z2015-00910

Wet politiegegevens (Wpg)

Artikel 2, eerste lid, Wpg:
1. Deze wet is van toepassing op de verwerking van politiegegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.

Artikel 4, derde lid, van de Wpg:
3. De verantwoordelijke treft passende technische en organisatorische maatregelen om politiegegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang, met name indien de verwerking verzending van gegevens via een netwerk of beschikbaarstelling via directe geautomatiseerde toegang omvat, en tegen alle andere vormen van onrechtmatige verwerking, waarbij met name rekening wordt gehouden met de risico's van de verwerking en de aard van de te beschermen gegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's van de verwerking en de aard van de politiegegevens.

Artikel 6 van de Wpg (voor zover relevant)
1. De verantwoordelijke onderhoudt een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.
2. Politiegegevens worden slechts verwerkt door ambtenaren van politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt.
3. De verantwoordelijke autoriseert de ambtenaren van politie die onder zijn beheer vallen voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast. De autorisatie bevat een duidelijke omschrijving van de verwerkingen waartoe de betreffende ambtenaar wordt geautoriseerd en de onderdelen van de politietaak ter uitvoering waarvan de verwerkingen worden gedaan.

Artikel 32, eerste lid, van de Wpg (voor zover relevant):
1. De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
[…]
c. de toekenning van de autorisaties, bedoeld in artikel 6;
[…]

Artikel 35, eerste en tweede lid, van de Wpg
1. Het College bescherming persoonsgegevens ziet toe op de verwerking van politiegegevens overeenkomstig het bij en krachtens deze wet bepaalde.
2. De artikelen 51, tweede lid, 60, 61 en 65 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.

Datum
6 februari 2017

Ons kenmerk
z2015-00910

Regeling informatiebeveiliging politie (Rip)

Artikel 2, eerste lid, van de Rip:
1. Deze regeling is van toepassing op het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Artikel 3, eerste en tweede lid, van de Rip (voor zover relevant):
1. De korpschef stelt het informatiebeveiligingsbeleid vast in een beleidsdocument en draagt dit beleid uit. Indien het informatiebeveiligingsbeleid mede betrekking heeft op informatiesystemen ten behoeve van de opsporing van strafbare feiten, stelt de korpschef dit beleidsdocument vast na overleg met de hoofdofficier van justitie.
2. Het document omvat tenminste:
[…]
f. de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door politieambtenaren gemeld worden, de politieambtenaar bij wie deze inbreuken worden gemeld en de wijze waarop deze worden afgehandeld;
[…]

Artikel 4, aanhef en onder e, van de Rip:
De korpschef draagt er zorg voor dat voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst op systematische wijze met inachtneming van de betrouwbaarheidscriteria en -normklassen, bedoeld in bijlage I, bepaald wordt welk stelsel van maatregelen uit hoofde van informatiebeveiliging getroffen dient te worden. Deze zorgplicht houdt tenminste in dat:
[…]
e. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst een informatiebeveiligingsplan wordt vastgesteld. Hierin is in elk geval opgenomen:
1. een actieplan ter implementatie van alle beveiligingsmaatregelen;
2. een calamiteitenparagraaf waarvan de effectiviteit periodiek wordt getoetst.

Politiewet 2012

Artikel 23, eerste lid, onder b, van de Politiewet 2012
1. Bij ministeriële regeling kunnen regels worden gesteld over:
a. […]
b. de informatiebeveiliging door de politie en door andere organisaties als bedoeld in onderdeel a.

Datum
6 februari 2017

Ons kenmerk
z2015-00910

Verordening (EG) Nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (hierna: de Verordening) en het Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (hierna: het Besluit)

Artikel 10, eerste lid, van het Besluit en de Verordening[22] *(voor zover relevant):*
1. Elke lidstaat neemt voor zijn N.SIS II passende maatregelen, waartoe ook een beveiligingsplan behoort, opdat:
[…]
d) onbevoegde gegevensopslag in het geheugen, alsmede onbevoegde kennisneming, wijziging of verwijdering van opgeslagen persoonsgegevens worden voorkomen (controle op de opslag);
[…]
f) degenen die bevoegd zijn om een systeem voor automatische gegevensverwerking te gebruiken, 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);
g) wordt gewaarborgd dat alle autoriteiten met toegangsrecht tot SIS II of tot faciliteiten voor gegevensverwerking, profielen opstellen waarin de taken en verantwoordelijkheden worden omschreven van personen die bevoegd zijn om persoonsgegevens in te zien, in te voeren, bij te werken, te wissen en te doorzoeken, en deze profielen desgevraagd onverwijld ter beschikking te stellen van de in artikel 60 bedoelde nationale controleautoriteiten (personeelsprofielen);
[…]
i) naderhand kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer, door wie en voor welk doel in een geautomatiseerd gegevensverwerkingssysteem zijn opgenomen (controle op de opneming);
[…]
k) de doelmatigheid van de in dit lid bedoelde beveiligingsmaatregelen doorlopend wordt gecontroleerd en met betrekking tot deze interne controle de nodige organisatorische maatregelen worden genomen om ervoor te zorgen dat de voorschriften van dit besluit worden nageleefd (interne controle).

Artikel 44 van de Verordening:
1. De in elke lidstaat aangewezen autoriteiten waaraan de bevoegdheden bedoeld in artikel 28 van Richtlijn 95/46/EG („nationale controleautoriteiten"), waken zelfstandig over de rechtmatigheid van de verwerking van SIS II-persoonsgegevens op hun grondgebied en de overdracht vanuit dat grondgebied, en de uitwisseling en verdere verwerking van aanvullende informatie.
2. De nationale controleautoriteiten zorgen ervoor dat ten minste om de vier jaar een controle van de gegevensverwerking in N. SIS II wordt verricht overeenkomstig internationale controlestandaarden.

[22] Opgemerkt moet worden dat de artikelen van het Besluit overeenkomen met die van de Verordening. Het enige verschil is dat in artikel 10, eerste lid, aanhef, van het Besluit spreekt over een *beveiligingsplan*, terwijl artikel 10, eerste lid, aanhef van de Verordening spreekt over een *veiligheidsplan*. Met deze begrippen wordt hetzelfde bedoeld.

3. De lidstaten zorgen ervoor dat de nationale controleautoriteiten voldoende middelen ter beschikking hebben om hun taken uit hoofde van deze verordening te kunnen vervullen.

Artikel 60 van het Besluit:
1. Elke lidstaat zorgt ervoor dat een onafhankelijke autoriteit („nationale controleautoriteit") zelfstandig waakt over de rechtmatigheid van de verwerking van SIS II-persoonsgegevens op en vanuit zijn grondgebied, met inbegrip van de uitwisseling en verdere verwerking van aanvullende informatie.
2. De nationale controleautoriteit zorgt ervoor dat ten minste om de vier jaar een controle van de gegevensverwerking in N.SIS II wordt verricht overeenkomstig internationale controlestandaarden.
3. De lidstaten zorgen ervoor dat de nationale controleautoriteit voldoende middelen ter beschikking heeft om haar taken uit hoofde van dit besluit te kunnen vervullen.