

3-10-12



3-10-12

## Inhoudsopgave

Inhoudsopgave	2
1. Inleiding	4
2. Managementsamenvatting	7
3. Aandachtspunten en aanbevelingen	9

3-10-12

<b>Bijlage B: Definities</b>	<b>24</b>
<b>Bijlage C: SIS II-infrastructuur</b>	<b>25</b>
<b>Bijlage D: Controls niet in scope</b>	<b>26</b>

3-10-12

Aan het afdelingshoofd Internationaal Onderzoek van de Autoriteit Persoonsgegevens,

Voor u ligt de rapportage van het onderzoek op het Schengen Informatiesysteem II (hierna: SIS II), dat wij hebben uitgevoerd bij de Nationale Politie conform de getekende opdrachtbevestiging d.d. 16 december 2020 met kenmerk 9

De Autoriteit Persoonsgegevens (hierna: AP) is aangewezen als nationale toezichthouder op de verwerking van persoonsgegevens in het nationale deel van het SIS II (hierna: N.SIS.II) door de in Nederland bevoegde autoriteiten. Op grond van artikel 44 van de SIS II Verordening en artikel 60 van het SIS II Besluit dient de nationale toezichthoudende autoriteit ervoor zorg te dragen dat tenminste om de vier jaar een onderzoek op de gegevensverwerking van het nationale systeem wordt verricht, overeenkomstig de geldende internationale normen. 3-10-12 heeft namens de AP dit onderzoek uitgevoerd bij de ketenpartners, waaronder de Nationale Politie.

De Nationale Politie is één van de bevoegde autoriteiten voor de verwerking van persoonsgegevens in de SIS II keten. De gegevensverwerking door de Nationale Politie in het kader van SIS II, waaronder de Dienst Landelijke Informatieorganisatie (hierna: DLIO) en het SIRENE-bureau, is daarmee object van onderzoek. Het doel van dit onderzoek is:

- 1) het inventariseren van het stelsel van maatregelen en procedures (interne beheersing) gericht op de bescherming van persoonsgegevens in het N.SIS II;
- 2) het formuleren van adviezen over de verdere mogelijke verbeteringen met betrekking tot de toepassing van de eisen die zijn gesteld in de (U)AVG, Wpg, SIS II Verordening en het SIS II Besluit.

7-11-12

:

- De Nationale Politie (als N.SIS.II instantie) en Dienst Landelijke Informatie Organisatie (DLIO) en SIRENE-bureau.

7-11-12

In deze rapportage vindt u een nadere uiteenzetting van de reikwijdte en de gehanteerde aanpak voor dit onderzoek. 3-10-12

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

3-10-12

Namens deze,

9

Partner

Kenmerk: 9

-3/26-

3-10-12

# 1. Inleiding

## Achtergrond

De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Onder toezicht vallen diverse activiteiten, zoals ook dit onderzoek naar de bescherming van persoonsgegevens bij de verwerking van deze persoonsgegevens in SIS II. SIS II speelt een belangrijke rol in de uitwisseling van gegevens tussen de verschillende ketenpartners binnen de Schengenlanden, als compenserende maatregel voor het wegvallen van interne grenscontroles. Het systeem bevat gegevens over personen die:

- geen recht hebben om in het betreffende gebied te verblijven;
- gezocht worden voor (betrokkenheid bij) criminele activiteiten;
- vermiste personen, waaronder kinderen en kwetsbare individuen.

De persoonsgegevens in de SIS II infrastructuur bestaan uit gevoelige persoonsgegevens, waaronder persoonsgegevens over kwetsbare groepen. Het is daarom in het belang van alle betrokkenen dat het systeem en de procedures voldoen aan de eisen gesteld in de (U)AVG, Wpg, SIS II Verordening en het SIS II Besluit.

## Doelstelling en aanpak

Dit onderzoek betreft een inventarisatie en review van de opzet en het bestaan van het stelsel van maatregelen en procedures (interne beheersing) gericht op de bescherming van persoonsgegevens in het N.SIS II, en heeft als doel aandachtspunten te identificeren en adviezen te formuleren met betrekking tot de toepassing van de eisen die zijn gesteld in de (U)AVG, Wpg, SIS II Verordening en het SIS II Besluit. In Nederland is de Nationale Politie als bevoegde autoriteit aangewezen voor het beheer van N.SIS.II. Het onderzoek waarover gerapporteerd wordt in dit rapport, betreft het onderzoek bij de Nationale Politie, waaronder DLIO en het SIRENE-bureau.

3-10-12

## Scope

Dit onderzoek heeft als doel te inventariseren welke beheersingsmaatregelen in de SIS II keten zijn geïmplementeerd met betrekking tot de verwerking van persoonsgegevens door de lidstaat Nederland in SIS II, met inbegrip van de verzending ervan naar het centrale deel van het systeem (hierna: C.SIS.II), en adviezen te formuleren met betrekking tot de toepassing van de eisen in de relevante wetgeving. 3-10-12

. De scope van dit rapport beperkt zich tot de verantwoordelijkheden, processen en systemen beheerd door de Nationale Politie.

2-7-11-12

3-10-12

2-7-11-12

Binnen de Nationale Politie wordt op verschillende manieren en door verschillende eenheden en afdelingen gewerkt met SIS II. In grote lijnen zijn de volgende verantwoordelijkheden te onderscheiden:

1. Het SIRENE-bureau is verantwoordelijk voor het technisch beheer van het systeem en voor de communicatie over signaleringen via 7-12. Tevens voert het SIRENE-bureau integraal kwaliteitscontroles uit over elke nieuw opgevoerde signalering door de Nationale Politie en door de Koninklijke Marechaussee.
2. Binnen de Landelijke Eenheid en de Regionale Eenheden mag een beperkt aantal medewerkers signaleringen opvoeren en muteren op aanvraag van een signalerende autoriteit. De ingevoerde en/of gemuteerde signalering wordt gecontroleerd door een medewerker van het SIRENE-bureau.
3. Alle politiemedewerkers in het veld hebben via verschillende applicaties de mogelijkheid N.SIS.II te raadplegen. Indien een 'gesignaleerde' wordt geïdentificeerd, nemen zij contact op met SIRENE-bureau.
4. De Gegevensautoriteit van de Nationale Politie is verantwoordelijk voor het beleid, waaronder SIS II ook valt. De Gegevensautoriteit heeft geen toegang tot SIS II.

3-10-12

3-10-12

**Tot slot**

De inhoud van dit rapport is op 20 april 2021 afgestemd met 9 van de Nationale Politie.

De informatie in dit rapport is uitsluitend bedoeld voor de AP en de Nationale Politie en heeft uitsluitend betrekking op de door ons uitgevoerde opdracht. Zonder uitdrukkelijke en voorafgaande schriftelijke toestemming van 3-10-12 is het niet toegestaan dit rapport, dan wel delen daaruit, te gebruiken voor andere doeleinden dan overeengekomen, aan derden te verspreiden of openbaar te maken, aan het rapport te refereren of uit het rapport te citeren.

Dit rapport geeft nadrukkelijk geen assurance (zekerheid) als bedoeld in de context van een jaarrekeningcontrole of assurance-opdracht. Daarnaast bevat dit rapport nadrukkelijk geen juridisch advies. Waar wetgeving wordt aangehaald, is dit ter achtergrondinformatie.

## 2. Managementsamenvatting

3-10-12





3-10-12

### 3. Aandachtspunten en aanbevelingen

3-10-12









3-10-12



3-10-12



3-10-12







3-10-12



3-10-12



3-10-12



3-10-12







3-10-12

## Bijlage B: Definities

3-10-12



3-10-12

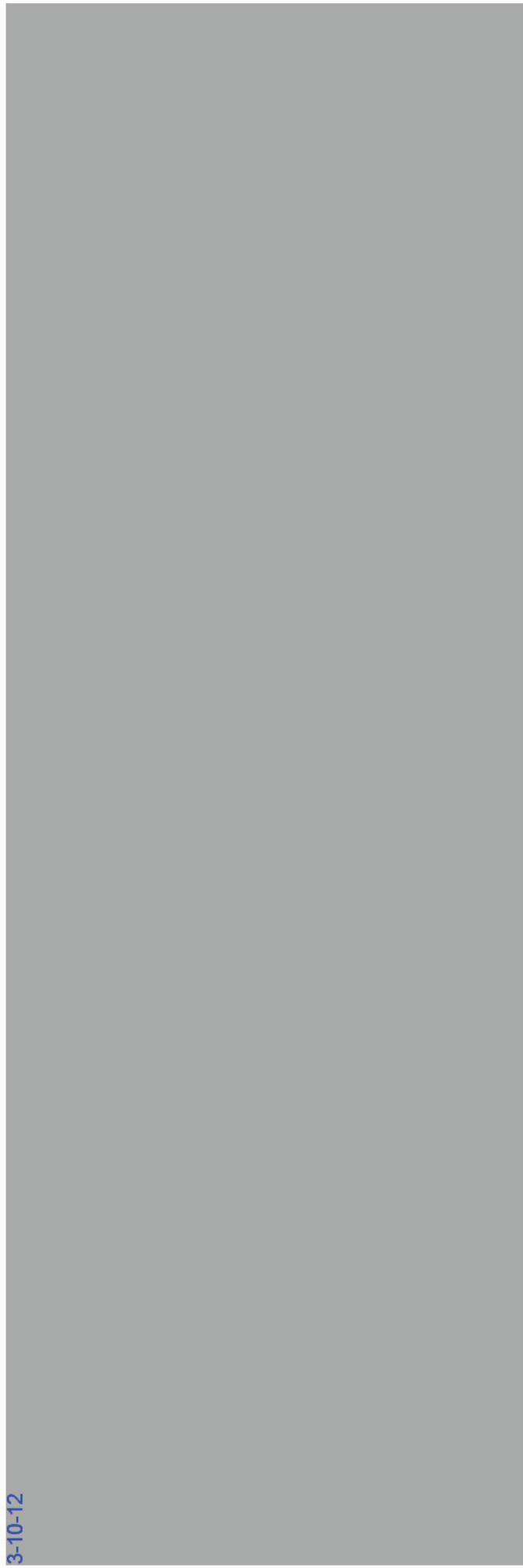
## Bijlage C: SIS II infrastructuur

3-10-12



**Bijlage D: Controls niet in scope**

3-10-12



3-10-12





## Memo

## Beantwoording vragen

**Onderwerp**  
Aankondiging onderzoek en  
verzoek om inlichtingen

**Organisatie onderdeel**  
Staf Korpsleiding  
Directie IV  
Gegevensautoriteit

**Behandeld door**

9

**Functie**  
Adviseur wet- en regelgeving

**Telefoon**

06-9

**E-mail**

9 @politie.nl

**Ons kenmerk**

2020-9

**Uw kenmerk**

9

**In afschrift aan**

Klik hier als u tekst wilt invoeren.

**Datum**

19 oktober 2020

**Bijlage(n)**

0

**Pagina**

1

De vragen van de Autoriteit Persoonsgegevens zijn hieronder steeds overgenomen. De beantwoording door de politie is na iedere vraag opgenomen in een blauw gearceerd blok.

### 1. Algemene vragen

Onderstaande vragen hebben een meer algemeen karakter en dienen als doel om een goed beeld te krijgen van de huidige werkwijze omtrent het invoeren en bijhouden van artikel 36 SIS II Besluit signaleringen en de persoonsgegevens die daarbij worden verwerkt.

12-14



12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

2 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

3 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

4 van 14



12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

5 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

6 van 14



12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

7 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

8 van 14



12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

9 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

10 van 14



12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

11 van 14





12-14

**Onderwerp**

Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

12 van 14





Postbus 17107  
2502 CC Den Haag  
Nieuwe Uitleg 1  
2514 BP Den Haag  
[www.politie.nl](http://www.politie.nl)

12-14

**Onderwerp**

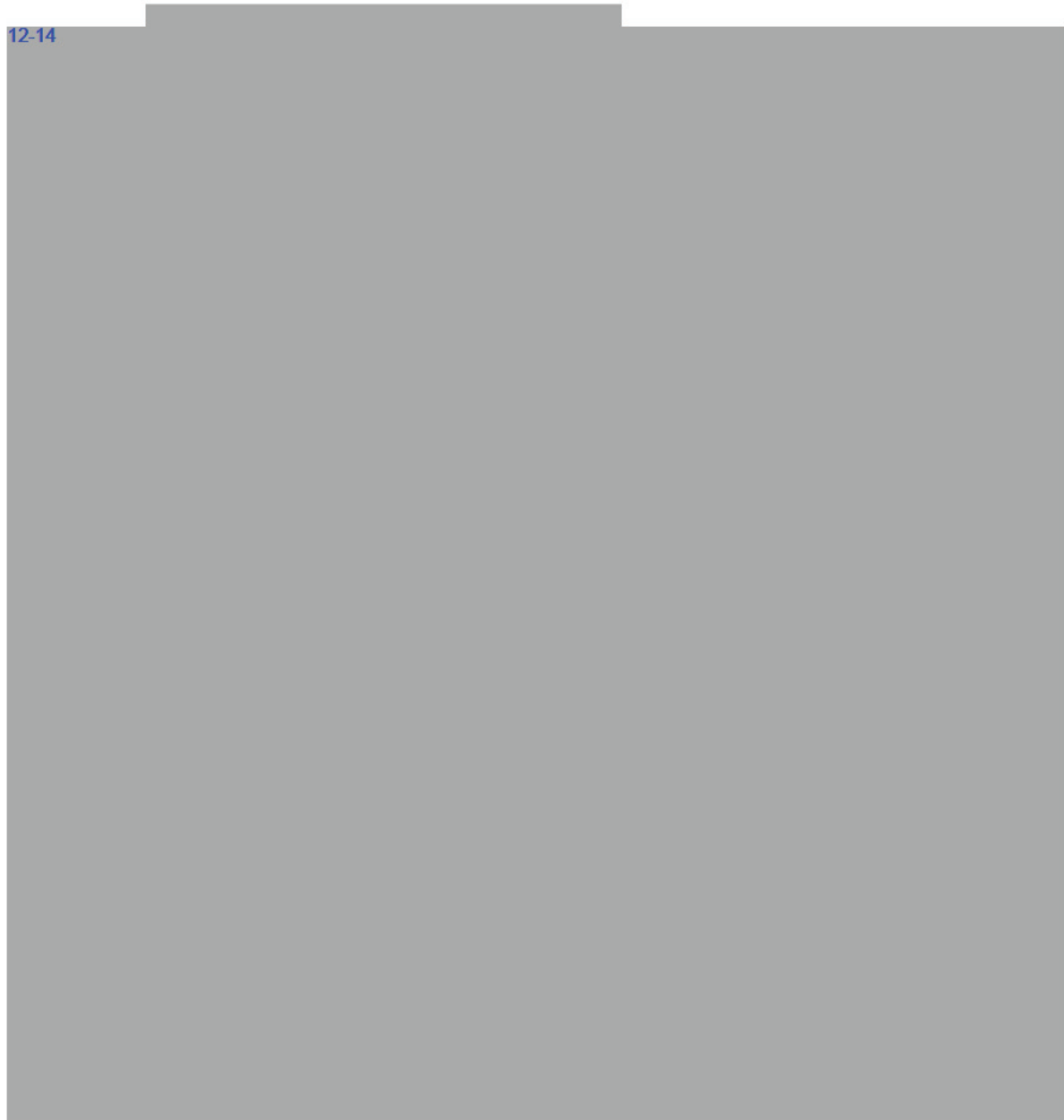
Aankondiging onderzoek en  
verzoek om inlichtingen

**Datum**

19 oktober 2020

**Pagina**

13 van 14







Ministry of Security and Justice

# Schengen Evaluation the Netherlands 2015



## Data protection

23<sup>rd</sup> September 2015





# Schengen Evaluation the Netherlands 2015

Welcome at the  
ICT Service

September 23, 2015

RESTRICTED

## Agenda

- IT figures
- Current organisation
- Delivery goals
- Questions?

# IT figures

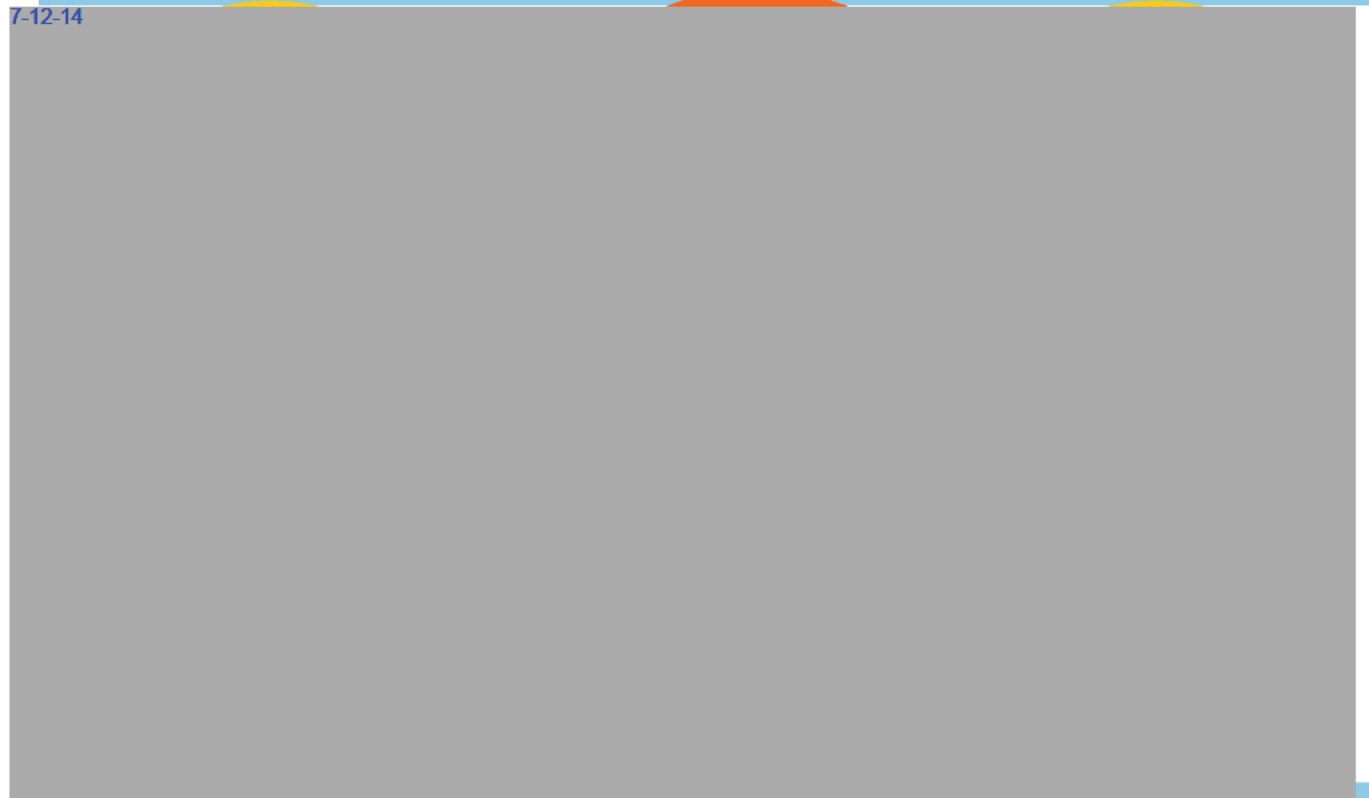
7-12-14



document13

# Current organisation

7-12-14



document13



## Delivery goals





# Questions?









Ministry of Security and Justice

# Schengen Evaluation the Netherlands 2015



Application landscape  
23 September 2015

RESTRICTED



7-12-14

RESTRICTED



7-12-14



3

RESTRI



7-12-14



4

RESTRICTED



7-12-14



7-12-14





7-12-14



7-12-14

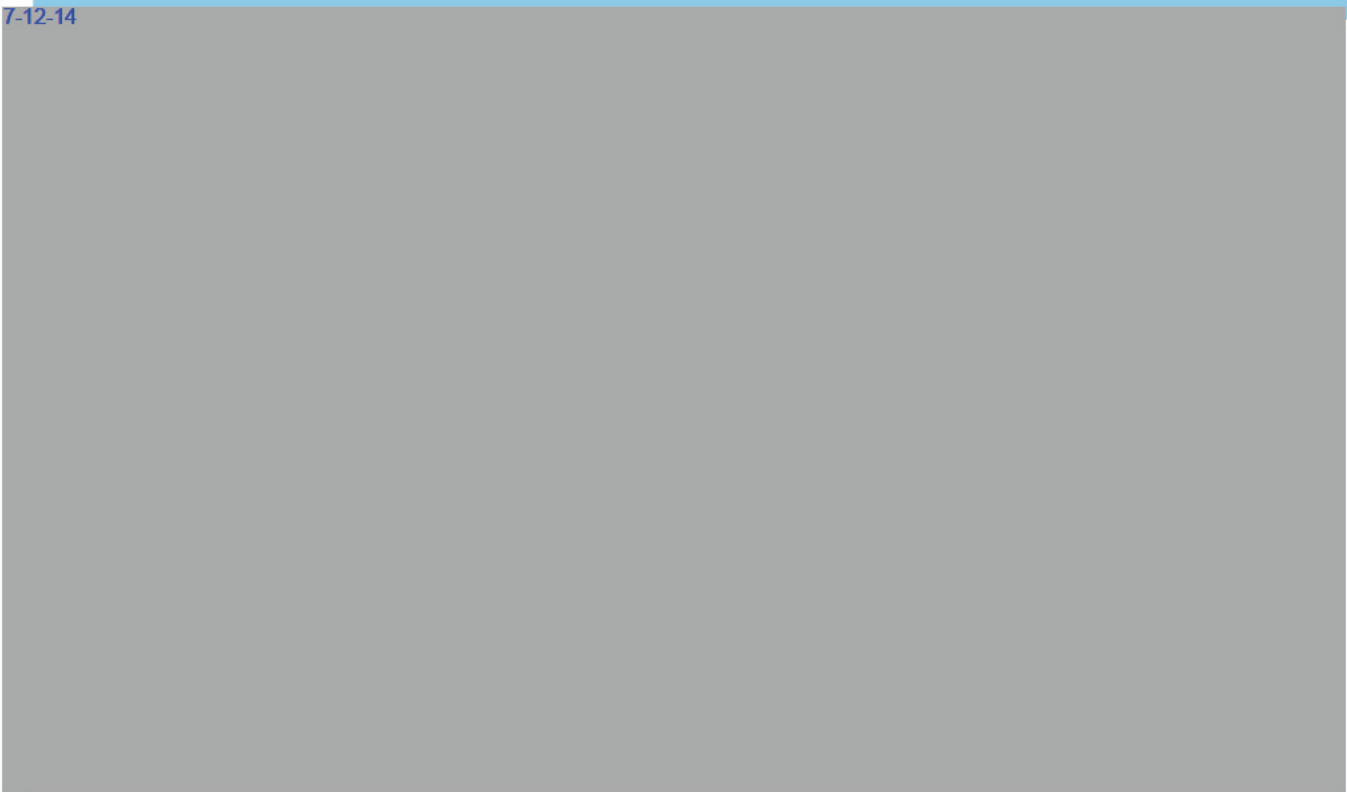




7-12-14



7-12-14





7-12-14



11

Schengen Evaluation the Netherlands 2015

RESTRICTED



7-12-14



12

Schengen Evaluation the Netherlands 2015

RESTRICTED









Ministry of Security and Justice

# Schengen Evaluation the Netherlands 2015



NL-SIS-II Architecture and Statistics  
23 September 2015

RESTRICTED



7-11-12-14

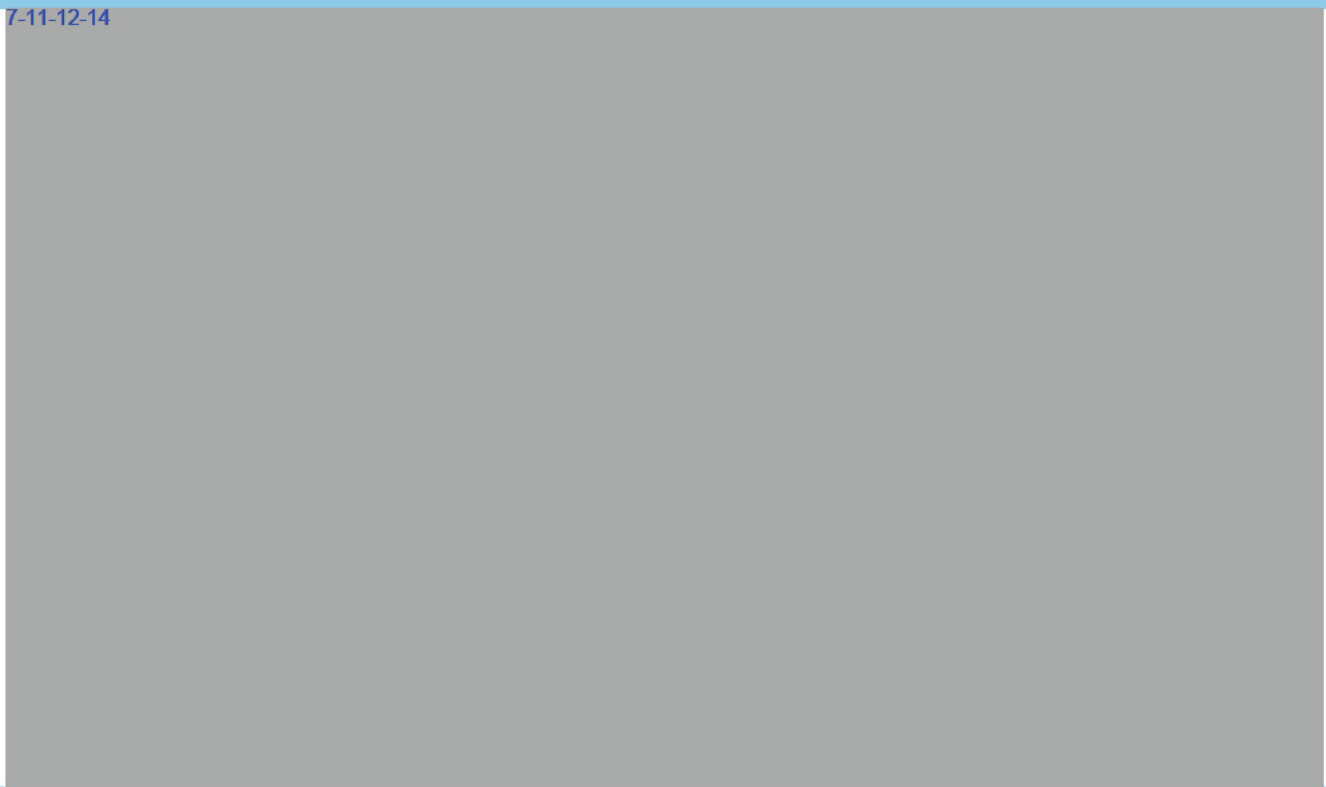
RESTRICTED



7-11-12-14



7-11-12-14

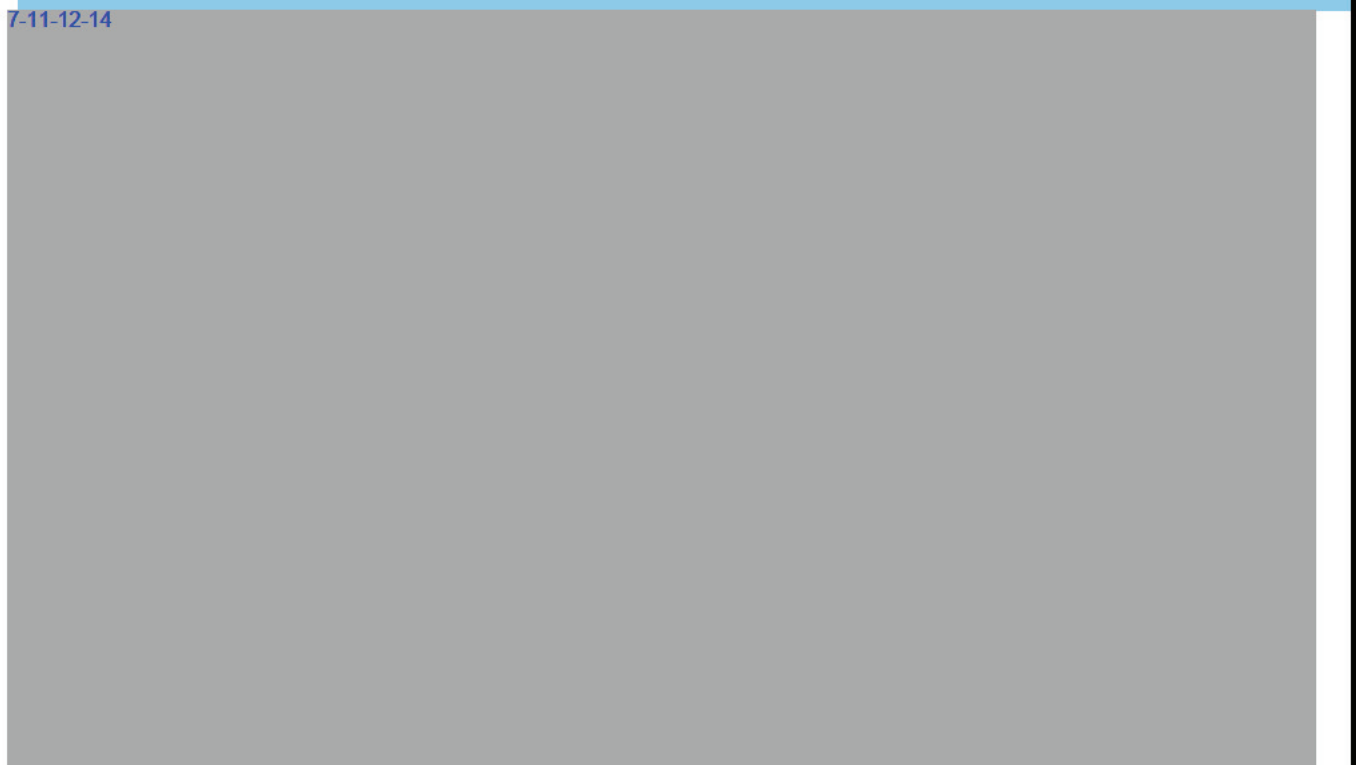




7-11-12-14



7-11-12-14





7-11-12-14



## Questions.. ?





Ministry of Security and Justice

# Schengen Evaluation the Netherlands 2015



Operations  
23 September 2015

RESTRICTED



## Agenda

- Organisation overview in numbers
- Organisation overview graphic
- Technical availability of Schengen applications
- Incident and escalation procedures
- Number of incidents of Schengen applications
- General technical setup (facility, power, backup)
- General security (physical and procedural)
- 16:00 – 17:00 Tour through CSD, OCR, ELA-A

RESTRICTED



## Organisation overview (General numbers)

- Around 65.000 employees at the Netherlands police (NP)
- [7-12-14](#)
- Around 600 physical police locations across the country

[7-11-12-14](#)



[7-12-14](#)



7-12-14

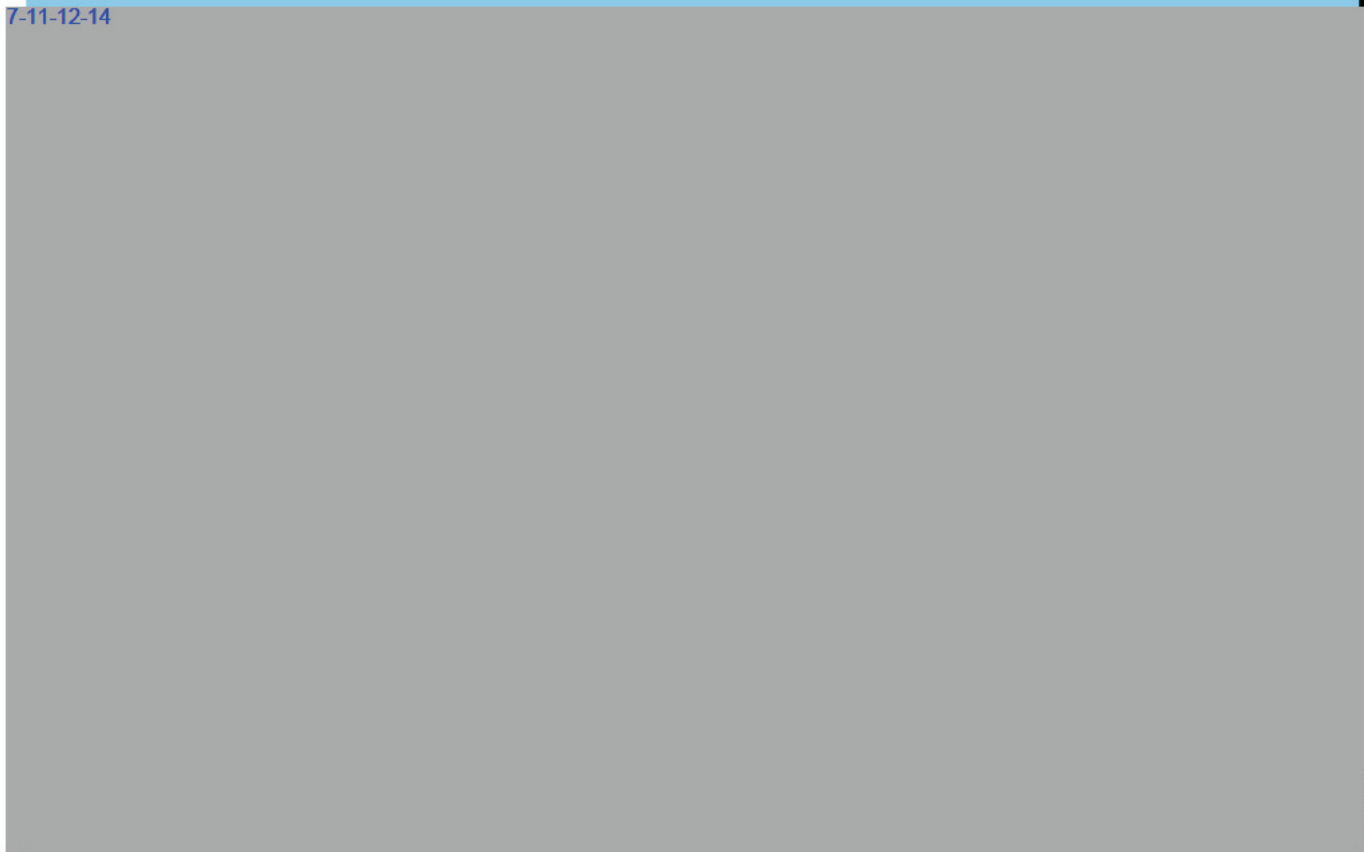


7-11-12-14





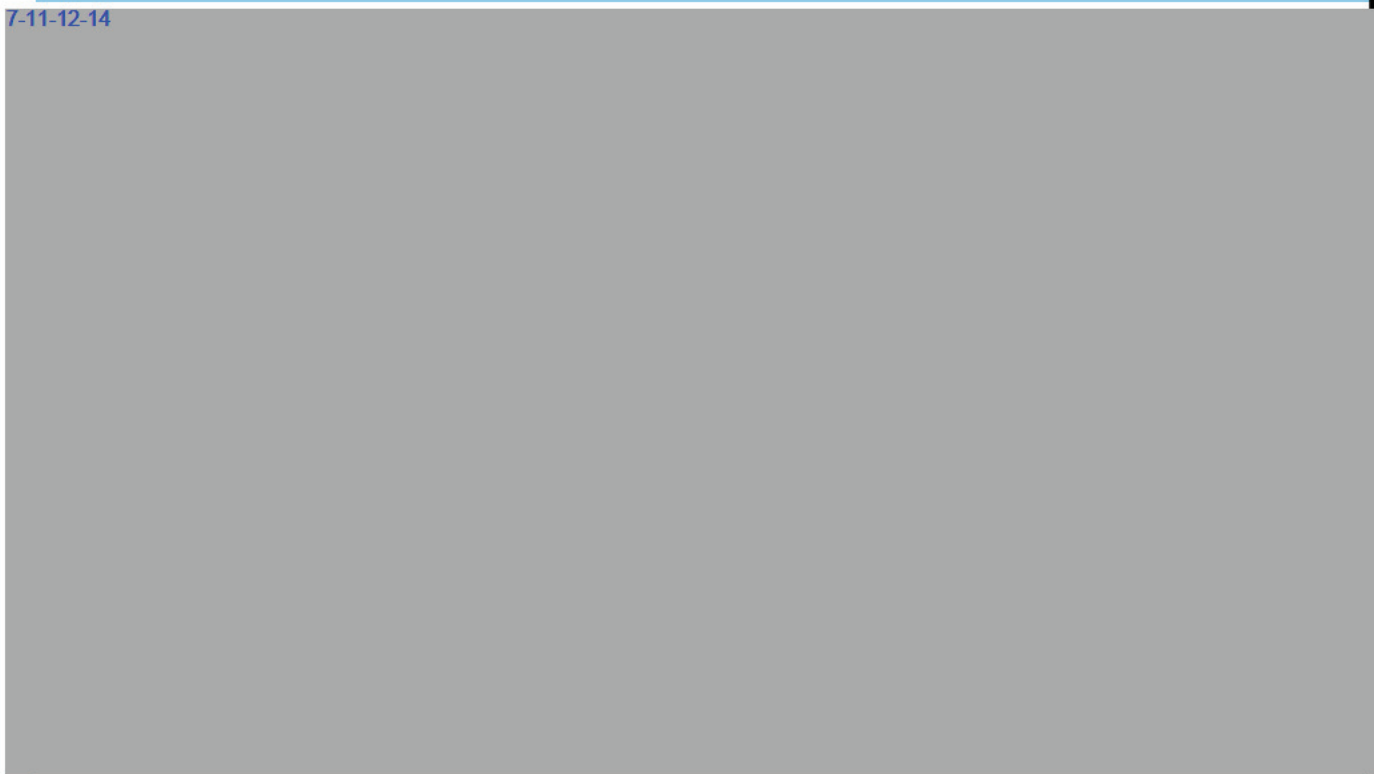
7-11-12-14



RESTRICTED



7-11-12-14



RESTRICTED





7-11-12-14



7-11-12-14





7-11-12-14



11

Schengen Evaluation the Netherlands 2015

RESTRICTED



7-11-12-14



12

Schengen Evaluation the Netherlands 2015

RESTRICTED



7-11-12-14



## Questions.. ?







# Schengen Evaluation the Netherlands 2015

Privacy by design  
23 September 2015

RESTRICTED

## Basic ICT requirements

Of the (previous) Minister of Security and Justice:



1. Ensure the continuity of IT systems
2. Make the IT systems easier to use
3. Innovation (only) if necessary

RESTRICTED

## Current system overview

7-12-14

3-10-12



Schengen Evaluation the Netherlands 2015

RESTRICTED

3-10-12



Schengen Evaluation the Netherlands 2015

RESTRICTED

7-11-12-14



Schengen Evaluation the Netherlands 2015

RESTRICTED

7-12-14



Schengen Evaluation the Netherlands 2015

RESTRICTED



7-12-14



Schengen Evaluation the Netherlands 2015

RESTRICTED



---

# *Monitoring* *N.SIS II* Stand van zaken

7 januari 2019  
2019-00039



---

# Inhoudsopgave

---

1.	Inleiding	3
2.	Systeembeschrijving	4
3.	Autorisaties	6
<hr/>		
3.1.	Scope van IAM/ATL	6
3.1.1.	IAM	6
3.1.2.	Individuele rechten toekennen (via ATL)	6
<hr/>		
3.2.	Opschoning rechten	7
3.3.	Review autorisaties	7
3.4.	Autorisaties externe samenwerkingspartners	7

---

7-11-12-14



# 1. *Inleiding*

Voor controle van inkomend en uitgaand personen- en goederenverkeer in het Schengengebied is tussen de Schengenlidstaten het Schengen informatiesysteem (hierna: SIS II) ingericht. Het SIS II bevat informatie over gesignaleerde personen en over gestolen of verloren goederen om de veiligheid bij het vrije verkeer van personen en goederen te kunnen controleren. Ieder land heeft de keuze gebruik te maken van een centrale voorziening of een eigen landelijke implementatie van SIS II. Nederland heeft gekozen voor een eigen landelijke implementatie. De Nederlandse installatie van SIS II wordt N.SIS II genoemd.

In de SIS-II Verordening van het Europees Parlement en de Raad en het SIS-II Besluit van de Raad worden voorschriften gegeven voor de werking en de beveiliging van het SIS-II systeem. De Autoriteit Persoonsgegevens (AP) is toezichthouder op het Nederlandse deel van SIS II (N.SIS II).

12-14

In dit document is in hoofdstuk 2 een systeembeschrijving opgenomen waaruit blijkt welke applicaties bevestigingen kunnen doen op de database van N.SIS II. Vervolgens zijn de acties beschreven die de politie heeft ingericht om onrechtmatige toegang (in hoofdstuk 3) en onrechtmatig gebruik (in hoofdstuk 4) van N.SIS II te voorkomen en te controleren.

In dit document wordt onder de term 'Autorisaties' begrepen de processen om toe te zien dat de juiste mensen toegang hebben en houden tot N.SIS II. Onder 'Monitoring' wordt begrepen de processen om toe te kunnen zien op het gebruik c.q. potentieel misbruik van N.SIS II.

## 2. *Systeembeschrijving*

Dit hoofdstuk geeft een beschrijving van N.SIS II en de systemen die N.SIS II kunnen benaderen. In de volgende hoofdstukken is benoemd welke van de systemen in scope vallen van het autorisatiebeheerproces en de monitoring op logging.

Hieronder is een visueel overzicht van de applicatie-architectuur opgenomen.

7-11-12



Het SIS-II-systeem bestaat uit een centraal systeem (CS-SIS II) en een nationaal informatiesysteem (N.SIS II). Omdat in alle Schengenlanden de gegevens in de database gelijk moeten zijn kan Nederland niet direct muteren in de CS-SIS-II database. Mutaties worden eerst ingevoerd in een nationaal 'wachtbestand' met behulp van de Schengen Muteer Client (SMC).

Verzoeken tot signalering worden met een signaleringsformulier aangeleverd bij het Regionaal Invoer Centrum, Sirene, het Koppelingsbureau van de IND of de meldkamer van de KMAR die de gegevens met het SMC-systeem kunnen invoeren in het wachtbestand. Voor het verzenden van deze berichten wordt gebruik gemaakt van 7-12

De nieuwe of gemuteerde gegevens in het wachtbestand worden lokaal bevestigd en gecontroleerd door het bureau Sirene van de politie en daarna geaccordeerd. Pas daarna worden de gegevens doorgestuurd naar het centrale bestand (CS-SIS-II) in Straatsburg en van daaruit worden binnen enkele seconden alle nationale (dus ook de Nederlandse) NL-SIS-II-bestanden bijgewerkt.

---

7-11-12 Daarnaast heeft de politie applicaties in beheer die bevestigingen kunnen doen op N.SIS II om gegevens te raadplegen. De volgende applicaties kunnen N.SIS II raadplegen en zijn in beheer van de politie:

7-11-12



---

### **3. *Autorisaties***

12-14



7-11-12-14



7-11-12-14



### **3.4. Autorisaties externe samenwerkingspartners**

Externe samenwerkingspartners, zoals de KMAR en de RDW, hebben de volgende applicaties in beheer die N.SIS II kunnen raadplegen:

7-11-12-14



7-11-12-14



---

## 4. *Monitoring*

12-14

A horizontal grey bar redacting content, with the text '12-14' at its top-left corner.

7-11-12-14

A large vertical grey rectangle redacting the majority of the page content, with the text '7-11-12-14' at its top-left corner.

7-11-12-14



7-11-12-14



7-11-12-14



---

7-11-12-14



AUTORITEIT  
PERSOONSGEGEVENS

# Onderzoek bij de Nationale Politie (bureau SIRENE) naar artikel 36 SIS II Besluit z2020-07040

## Rapport van voorlopige bevindingen

9 december 2021

**Over de Autoriteit Persoonsgegevens**

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.







## Inhoudsopgave

1.	Inleiding	5
1.1	Aanleiding onderzoek	5
1.2	Organisatie	5
1.3	Verloop onderzoek	6
1.4	Methodologie	8
1.5	Juridisch kader	8

5-12-14



5-12-14





5-12-14

<b>3.</b>	<b>Conclusies</b>	<b>25</b>
3.1	Hoe beoordeelt de gegevensbeschermingsautoriteit de mate van naleving bij artikel 36-signaleringen?	25
3.2	In het geval van gedeeltelijke of niet-naleving, wat zijn de redenen voor deze beoordeling?	25
3.3	Waren er klachten of verzoeken omtrent het uitoefenen van de rechten van betrokkenen in relatie tot artikel 36-signaleringen?	28
3.4	Aanbevelingen van de gegevensbeschermingsautoriteit / voorgenomen maatregelen	28
3.4.1	Aanbevelingen	28



# 1. Inleiding

## 1.1 Aanleiding onderzoek

De aanleiding om over te gaan tot een gecoördineerde inspectie van artikel 36 van het SIS II Besluit is de stijging van het aantal ingevoerde signaleringen o.g.v. artikel 36 SIS II Besluit (hierna: artikel 36 signaleringen).<sup>1</sup> In de periode van 2013 tot 2017 is het aantal signaleringen dat is ingevoerd op grond van artikel 36 SIS II Besluit met 10% gestegen binnen de EU. In 2017 bestond 15% van alle SIS II signaleringen op personen uit artikel 36-signaleringen. Deze stijgende trend is voor de Supervision Coordination Group Schengen Information System II (hierna: SCG SIS II)<sup>2</sup> aanleiding geweest om een gecoördineerde inspectie in de lidstaten op te zetten. De inspectie is tweeledig en bestaat uit het invullen van een questionnaire, die door de SCG SIS II is opgesteld, en het steekproefsgewijs controleren van artikel 36 signaleringen. De inspectie heeft ten doel om over de periode 2015-2019 steekproefsgewijs vast te stellen of de signaleringen voldoen aan de eisen uit het SIS II Besluit en de Wpg.

### *Achtergrond*

Het Schengen Informatiesysteem (SIS) is opgericht ter compensatie van de open binnengrenzen van de lidstaten van het Schengengebied. Op basis van de SIS II Verordening en het SIS II Besluit is een tweedegeneratie Schengen Informatiesysteem ingevoerd, SIS II genoemd. Dit systeem bevat signaleringen die de lidstaten van het Schengengebied hebben uitgebracht. Deze signaleringen bevatten allerlei gegevens, zoals gegevens over vreemdelingen die geen toegang hebben tot het Schengengebied en signaleringen van gezochte of vermiste personen of over gestolen voertuigen. De vreemdelingensignaleringen zijn gebaseerd op de SIS II Verordening, de overige (personen)signaleringen op het SIS II Besluit.

Lidstaten kunnen zowel signaleringen invoeren over gerichte controles als over onopvallende controles. Bij een gerichte controle wordt de gesignaleerde persoon bij een 'hit' aangesproken, gecontroleerd en indien noodzakelijk gefouilleerd. Bij een onopvallende controle wordt de gesignaleerde persoon bij een 'hit' discreet geobserveerd en wordt geen aanhouding of controle verricht. De rechtsgrondslag voor dit type signaleringen vloeit voort uit artikel 36 SIS II Besluit.

## 1.2 Organisatie

Hieronder wordt uiteengezet uit welke organisatie(onderdelen) betrokken zijn bij de verwerking van persoonsgegevens in het kader van artikel 36 signaleringen.

### *SIRENE Bureau*

Het SIRENE bureau is verantwoordelijk voor de uitwisseling van aanvullende informatie.<sup>3</sup> De taken van het SIRENE bureau bestaan uit het uitwisselen van gegevens met de EU-lidstaten over signaleringen in SIS II en het coördineren van de kwaliteitscontroles op de in SIS II opgenomen informatie.<sup>4</sup> Voor deze taken heeft het SIRENE bureau toegang tot de in SIS II verwerkte gegevens. Het SIRENE bureau van Nederland is onderdeel van de

<sup>1</sup> Dossierstuk 1

<sup>2</sup> De SCG SIS II bestaat uit de nationale toezichhoudende autoriteiten van de lidstaten en de EDPS.

<sup>3</sup> Ingevolge artikel 7, tweede lid, van de SIS II Verordening en het SIS II Besluit wijst elke lidstaat de autoriteit aan die ervoor zorgt dat alle aanvullende informatie wordt uitgewisseld ("het SIRENE-bureau"), overeenkomstig de bepalingen van het SIRENE-handboek, als bedoeld in artikel 8.

<sup>4</sup> Artikel 7 lid 2 SIS II Besluit



## AUTORITEIT PERSOONSgegevens

Nationale Politie (hierna: NP) en is ondergebracht bij het Landelijk Internationaal Rechtshulp Centrum (hierna: LIRC) te Zoetermeer.<sup>5</sup> Iedere lidstaat heeft een Bureau SIRENE dat 24 uur per dag operationeel is en als enige contactpunt fungeert voor verwerkingen in het betreffende nationale deel van het SIS II (hierna: N.SIS II). SIRENE is een acronym voor 'Supplementary Information Request at the National Entries'.<sup>6</sup>

De korpschef heeft met betrekking tot N.SIS II mandaat verleend aan de politiechef van de landelijke eenheid, die op zijn beurt mandaat heeft verleend aan het hoofd van het onderdeel Dienst Landelijke Informatie Organisatie (DLIO). Binnen DLIO staat de dagelijkse gang van zaken onder leiding van het hoofd van het LIRC. Het voorgaande neemt niet weg dat voor de juiste inhoud van de signalering elke partij zelf verantwoordelijk blijft.<sup>7</sup>

De korpschef van de NP is verwerkingsverantwoordelijke voor het verwerken van politiegegevens en daarmee ook voor de persoonsgegevens die worden verwerkt door het SIRENE bureau.<sup>8</sup>

### *N.SIS II-instantie*

In het SIS II Besluit wordt de N.SIS II-instantie aangewezen als de autoriteit die de centrale verantwoordelijkheid heeft voor zijn N.SIS II.<sup>9</sup> Deze autoriteit is verantwoordelijk voor de goede werking en beveiliging van N.SIS II, zorgt voor de toegang van de bevoegde autoriteiten tot de gegevens in SIS II en treft de nodige maatregelen ten behoeve van de naleving van de bepalingen in dit besluit.<sup>10</sup> In Nederland is de **Dienst ICT van het Politiedienstencentrum (PDC)** aangewezen als nationale N.SIS II instantie.<sup>11</sup> Dienst ICT beheert, onderhoudt en verzorgt de doorontwikkeling van N.SIS II en de daaraan gekoppelde applicaties zoals: de Schengen Muteer Client (de cliëntapplicatie waarmee signaleringen kunnen worden ingevoerd en gemuteerd in N.SIS II) en Sirene Berichten Verkeer (hierna SBV, de applicatie voor het uitwisselen van extra verzoeken en informatie rondom deze signaleringen, dit proces wordt uitgevoerd door Bureau SIRENE).

De korpschef van de NP is verwerkingsverantwoordelijke voor het verwerken van politiegegevens en daarmee ook voor de persoonsgegevens die worden verwerkt door de PDC.<sup>12</sup>

### *Samenwerking*

Bureau SIRENE werkt samen met de PDC. Zij hebben wekelijks overleg ter bevordering van de werking van N.SIS II en het daaraan gekoppelde SBV. Daarnaast heeft Bureau SIRENE toegang tot de test-omgeving van N.SIS II en SBV, om voorafgaand aan een nieuw release de systemen te testen.<sup>13</sup>

## 1.3 Verloop onderzoek

Op 4 september 2020 is per brief het onderzoek aangekondigd naar het controleren van de rechtmatigheid van de gegevensverwerkingen die plaatsvinden in het kader van artikel 36 signaleringen in N.SIS II. In dezelfde brief zijn de eerste inlichtingen verzocht. De deadline voor het indienen van de antwoorden op de vragen verliep op 14

<sup>5</sup> Lijst van N.SIS II-instanties en nationale Sirene-bureaus (2019/C 222/02).

<sup>6</sup> Dossierstuk 5, p. 3.

<sup>7</sup> Dossierstuk 5, p. 4.

<sup>8</sup> Artikel 1, eerste lid, aanhef en onder f, punt 1 Wpg

<sup>9</sup> Artikel 7 lid 1 SIS II Besluit

<sup>10</sup> Artikel 7 lid 1 SIS II Besluit

<sup>11</sup> Lijst van N.SIS II-instanties en nationale Sirene-bureaus (2019/C 222/02).

<sup>12</sup> Artikel 1, eerste lid, aanhef en onder f, punt 1 Wpg

<sup>13</sup> Dossierstuk 5, p. 3.



AUTORITEIT  
PERSOONSGEGEVENS

oktober 2020. Op 19 oktober 2020 ontving de AP de antwoorden op het verstuurd inlichtingenverzoek van 4 september 2020.

Op 21 januari 2021 heeft de AP een tweede inlichtingenverzoek verstuurd naar de NP. De deadline voor het beantwoorden van de vragen was gezet op 5 februari 2021. Na telefonisch overleg tussen de AP en de NP is door de AP uitstel verleend tot 19 februari 2021. Een bevestiging hiervan is per e-mail op 9 februari 2021 verstuurd. Op 20 februari 2021 ontving de AP de concept antwoorden. Een definitieve versie van de antwoorden ontving de AP op 12 maart 2021.

Op 22 januari 2021 heeft de AP een eerste inlichtingenverzoek verstuurd naar het Openbaar Ministerie. De antwoorden op de vragen dienden uiterlijk 5 februari 2021 in het bezit te zijn van de AP. Op 3 februari 2021 ontving de AP een verzoek om uitstel. De AP heeft per e-mail van 4 februari 2021 uitstel verleend tot 5 maart 2021. Het OM heeft op 4 maart 2021 aangegeven die deadline niet te halen. De AP heeft het OM daarop twee keer verzocht om de antwoorden alsnog te sturen. De AP ontving de antwoorden op 2 april 2021.

Op 11 maart 2021 is door de AP het onderzoek ter plaatse bij bureau SIRENE aangekondigd.

Op 17 maart 2021 ving het eerste onderzoek ter plaatse bij Bureau SIRENE aan. Tijdens het onderzoek hebben AP inspecteurs inzicht gekregen in het gehele proces van een artikel 36 signalering.

Op 22 maart 2021 heeft de AP per e-mail aanvullende informatie opgevraagd bij de NP. Op 23 maart 2021 ontving de AP de antwoorden op de vragen over de invoer door de zgn. Regionale Invoer Centra (hierna: RIC's). Deze antwoorden zijn gegeven door de "Coördinator signaleringsproces" van de Dienst Regionale Informatie Organisatie (DRIO) bij de Eenheid Amsterdam. Ook ontving de AP op dezelfde dag het aantal actieve ingevoerde signaleringen van de Koninklijke Marechaussee. Op 29 maart 2021 ontving de AP lijst met deze signaleringen.

Op 26 maart 2021 is het verslag van het Onderzoek ter Plaatsse van 17 maart 2021 voorgelegd aan de adviseur wet- en regelgeving van korpsleiding van de NP (hierna: NP). Eventuele feitelijke onjuistheden in het verslag konden tot uiterlijk 8 april 2021 naar de AP gestuurd worden. De AP heeft geen reactie ontvangen.

Het tweede onderzoek ter plaatse vond plaats op 13 april 2021. Tijdens het onderzoek hebben AP inspecteurs inzage gekregen in 21 artikel 36 signaleringen.

Na afloop van het tweede onderzoek ter plaatse heeft de AP op 16 april 2021 aanvullende informatie opgevraagd bij de NP. De deadline voor het verstrekken van deze informatie stond op 7 mei 2021. Na het verstrijken van de deadline heeft de AP nog tweemaal gevraagd om de informatie. Op 19 en 29 mei 2021 ontving de AP de aanvullende informatie per e-mail.

Op 25 april 2021 heeft de AP met betrekking tot een specifieke signalering informatie opgevraagd bij de Koninklijke Marechaussee. Deze informatie heeft de AP op 6 mei 2021 ontvangen.



## 1.4 Methodologie

3-10-12

In het onderzoek wordt verwezen naar onderzoeken ter plaatse (hierna: OTP). Tenzij anders omschreven wordt hier steeds bedoeld het onderzoek ter plaatse waarbij individuele dossierchecks hebben plaatsgevonden. Waar wordt verwezen naar 'voorbereidend otp' wordt verwezen naar het otp van 17 maart 2021.

3-10-12

## 1.5 Juridisch kader

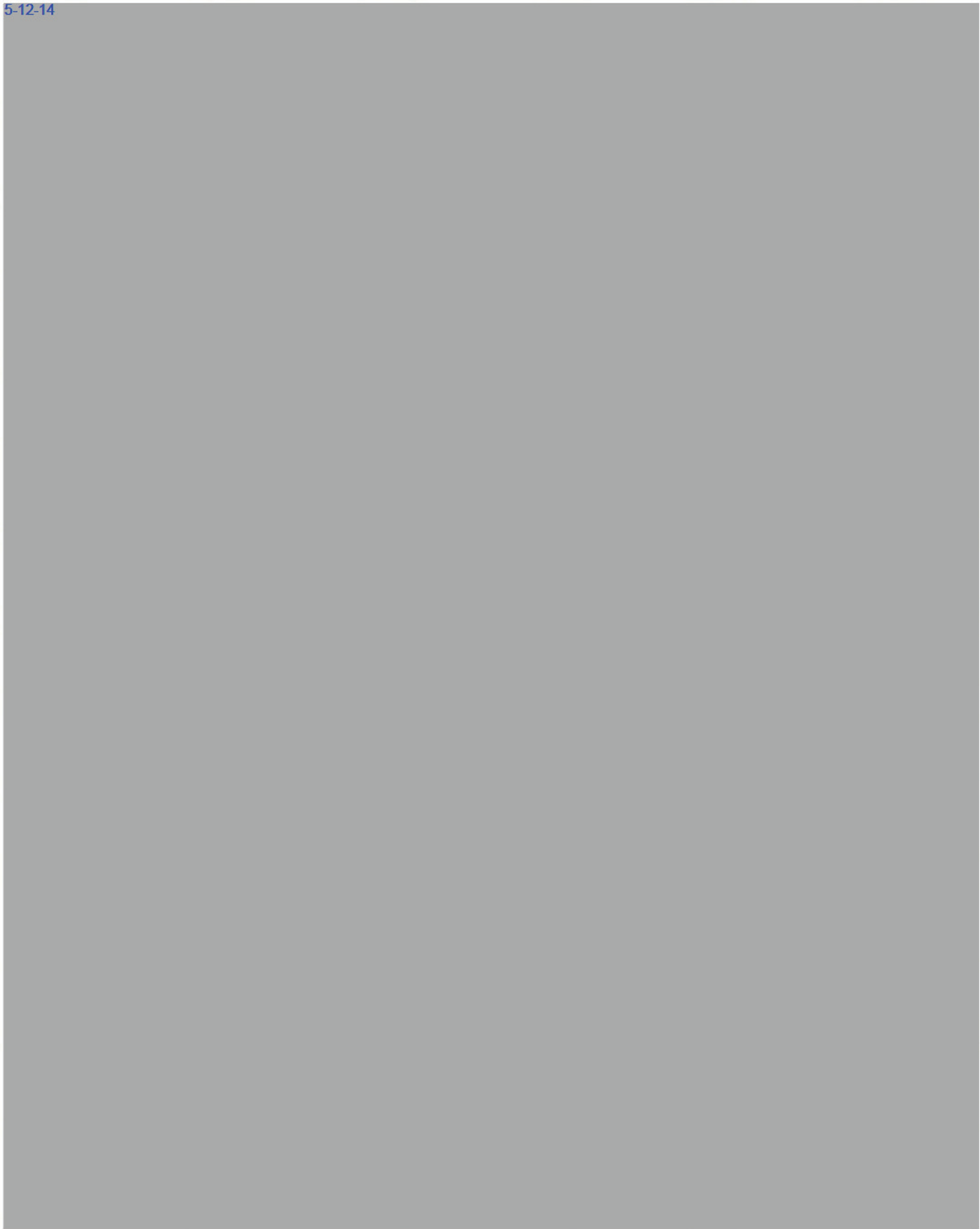
Het volledige relevante juridische kader is opgenomen in **bijlage 1** van dit rapport.

5-12-14



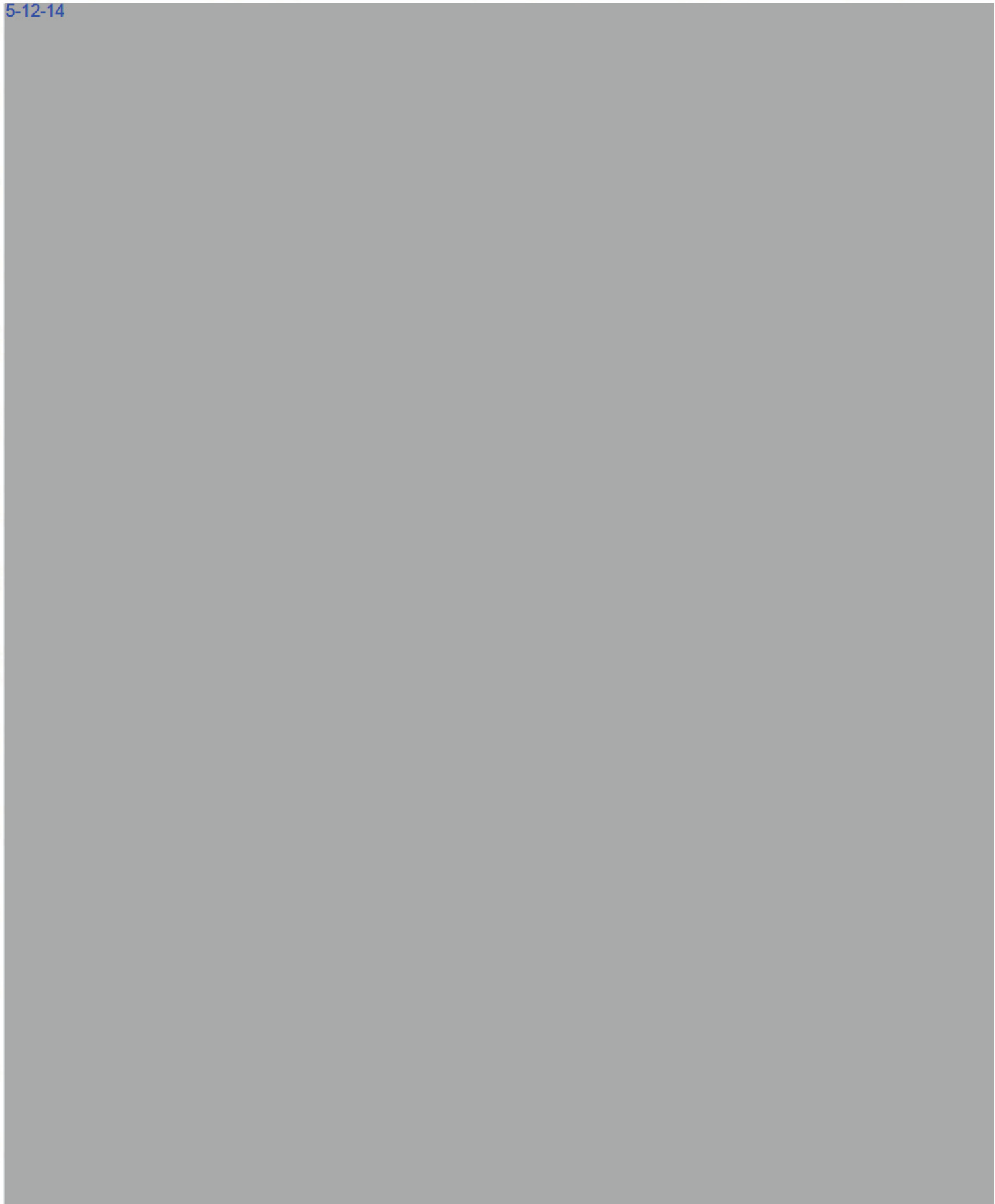


5-12-14





5-12-14





5-12-14





5-12-14



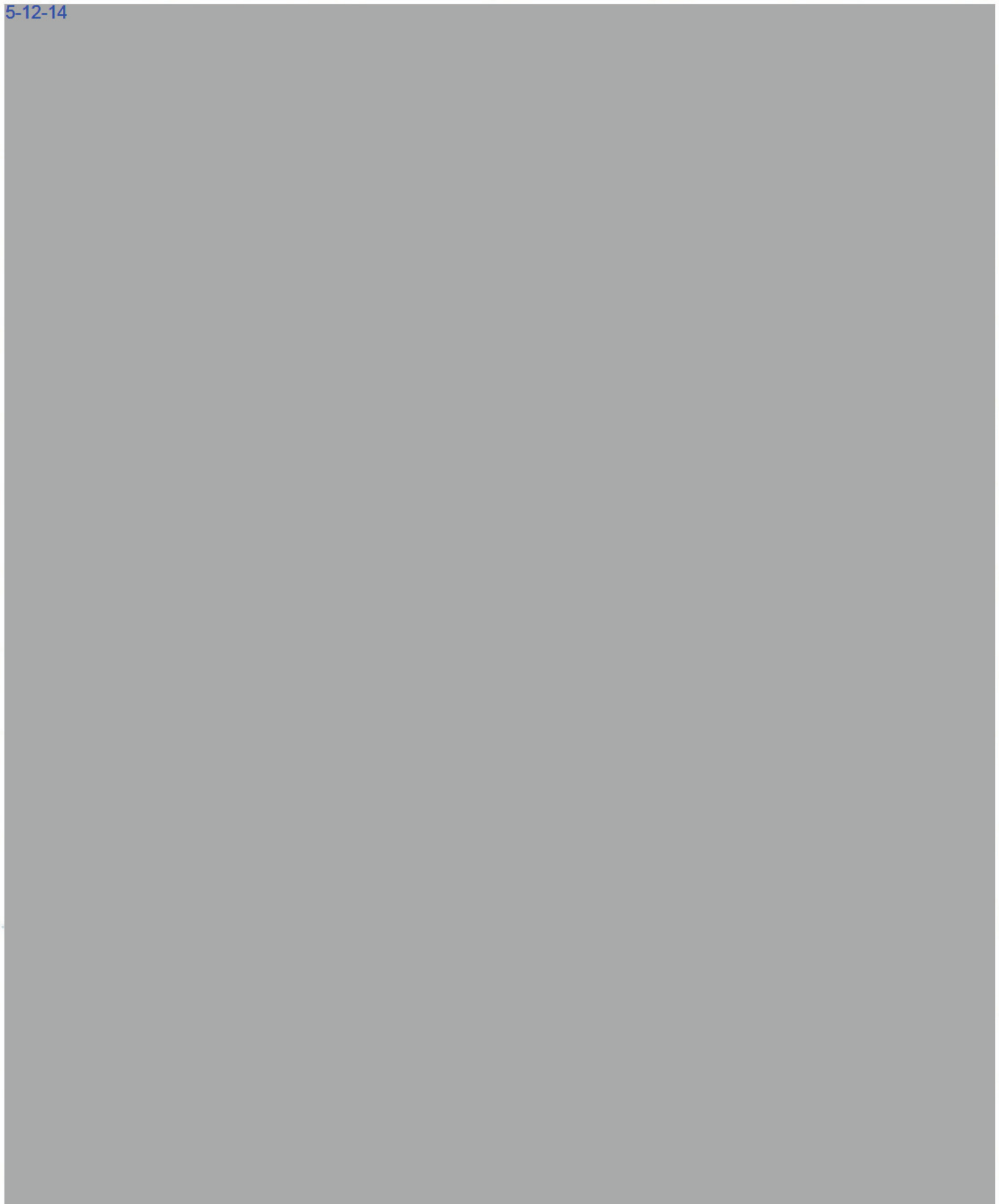


5-7-12-14





5-12-14





5-12-14





5-12-14







5-12-14

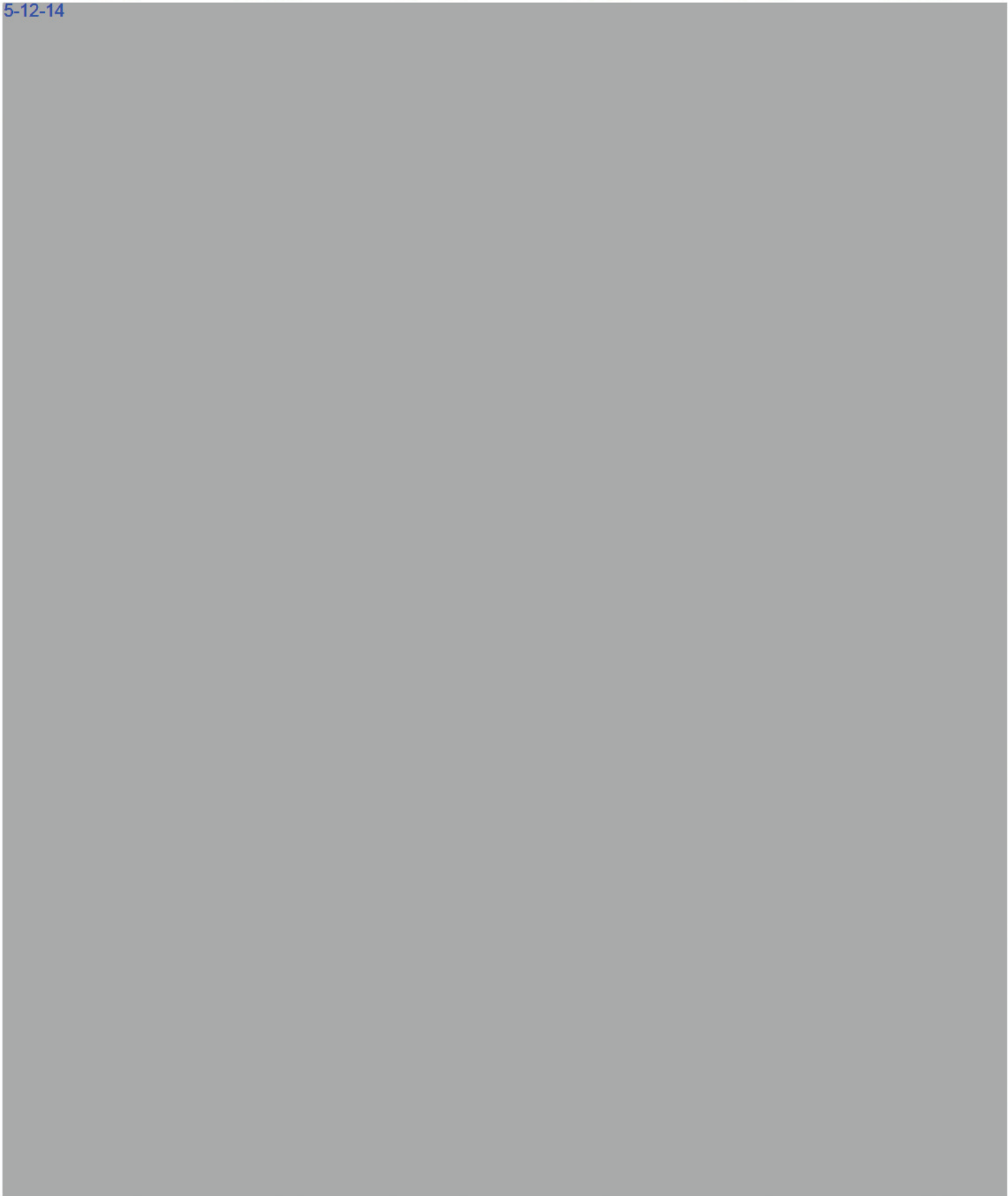


5-12-14





5-12-14



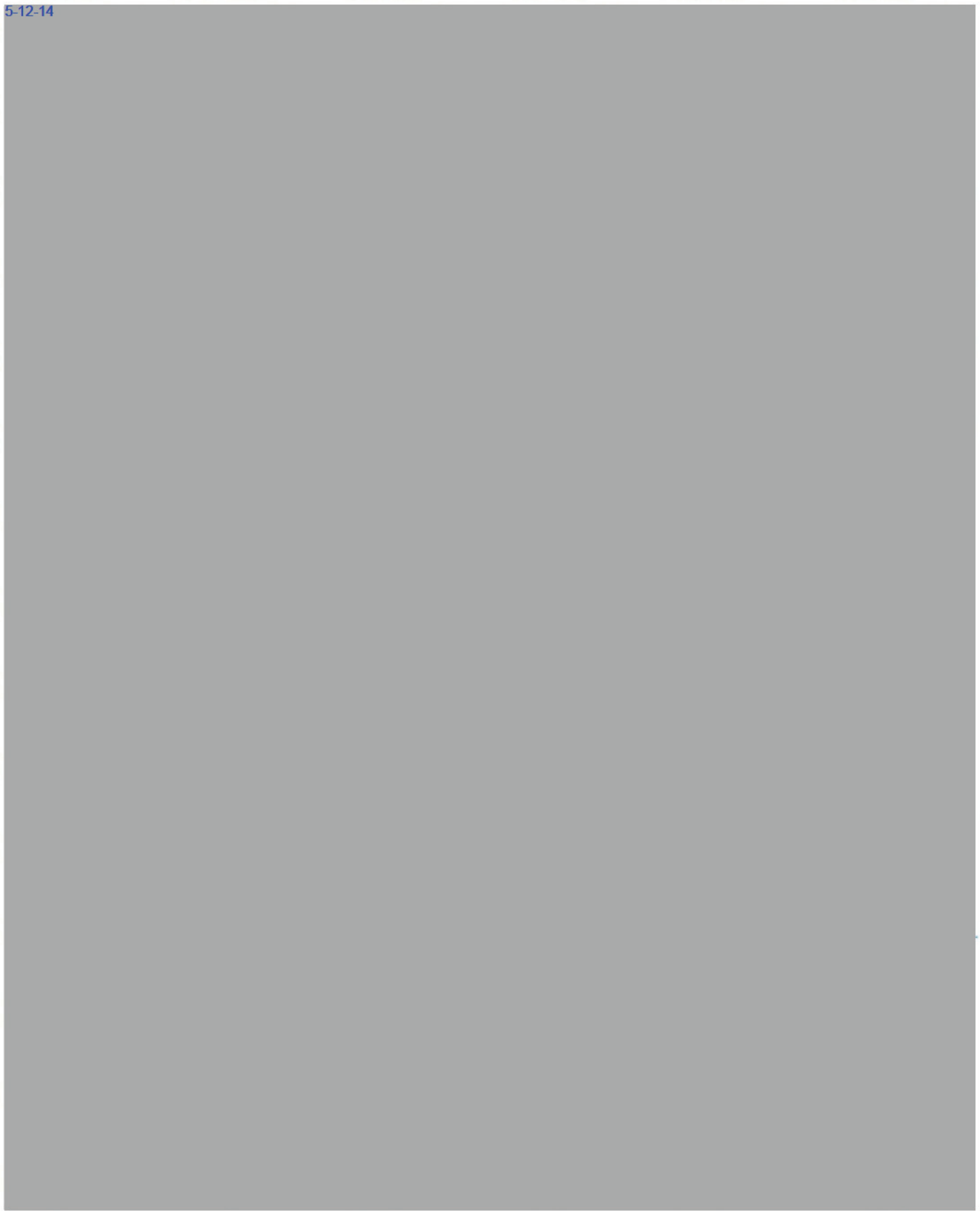


5-12-14





5-12-14





5-12-14





5-12-14





5-12-14







### 3. Conclusies

5-12-14

3.1 Hoe beoordeelt de gegevensbeschermingsautoriteit de mate van naleving bij artikel 36-signaleringen?

5-12-14

3.2 In het geval van gedeeltelijke of niet-naleving, wat zijn de redenen voor deze beoordeling?

5-12-14



AUTORITEIT  
PERSOONSGEGEVENS

5-12-14





5-12-14





5-12-14



### 3.4 Aanbevelingen van de gegevensbeschermingsautoriteit / voorgenomen maatregelen

#### 3.4.1 Aanbevelingen

5-12-14

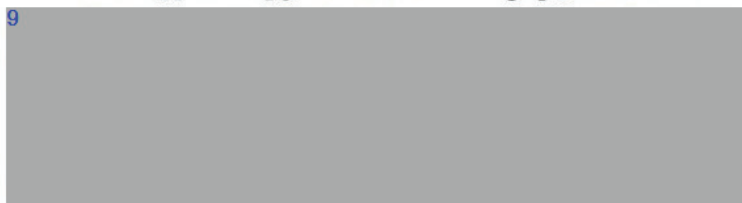




5-12-14



Dit rapport is opgemaakt te Den Haag op 9 december 2021.



Directeur Juridische Zaken en Wetgevingsadvisering



AUTORITEIT  
PERSOONSGEGEVENS

## Vragen over de Algemene verordening gegevensbescherming

Op onze website [autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl) vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.



## Bijlage 1: Juridisch kader

Bevoegdheid Autoriteit Persoonsgegevens

De bevoegdheid van de AP vloeit voort uit artikel 35 Wpg in samenhang gelezen met artikel 16 van de UAVG. Uit deze bepaling volgt dat de AP bevoegd is een last onder bestuursdwang op te leggen ter handhaving van de Wpg.

### Wet politiegegevens (Wpg)

Artikel 3 Wpg, voor zover relevant

- 1 Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden.
- 2 Politiegegevens worden slechts verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.
- 3 Politiegegevens die zijn verkregen voor een doel, als bedoeld in artikel 1, onder a, kunnen worden verwerkt voor een ander doel, bedoeld in artikel 1, onderdeel a, voor zover deze wet of Unierecht uitdrukkelijk daarin voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.
- 4 Politiegegevens kunnen voor een ander doel dan die, bedoeld in artikel 1, onderdeel a, worden verwerkt door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen.
- 5 Bij de verwerking van politiegegevens op grond van de artikelen 9, 10 en 12 worden de herkomst van deze gegevens en de wijze van verkrijging vermeld.

Artikel 4 Wpg, voor zover relevant

- 1, De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij zorgt voor het onverwijld vernietigen of rectificeren van politiegegevens als blijkt dat deze, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn. De bevoegde autoriteit controleert, voor zover praktisch uitvoerbaar, de kwaliteit van politiegegevens voordat de gegevens worden verstrekt. Voor zover mogelijk wordt bij de doorzending van politiegegevens de noodzakelijke informatie toegevoegd aan de hand waarvan de ontvangende bevoegde autoriteit de mate van juistheid, volledigheid en betrouwbaarheid van politiegegevens kan beoordelen, alsmede de mate waarin zij actueel zijn.
- 2 De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.
- 3 Voor zover mogelijk worden politiegegevens die op feiten zijn gebaseerd onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
- 4 Indien wordt vastgesteld dat onjuiste politiegegevens zijn verstrekt, of dat de politiegegevens op onrechtmatige wijze zijn verstrekt, wordt de ontvanger daarvan onverwijld in kennis gesteld. In dat geval dienen de gegevens te worden gerectificeerd of vernietigd, of wordt de verwerking beperkt, als bedoeld in artikel 28, tweede lid.

Artikel 8 Wpg, voor zover relevant

1. Politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak gedurende een periode van één jaar na de datum van de eerste verwerking.