Schengeninformatiesysteem II – Een gids voor de uitoefening van het recht van toegang
Samenvatting

Personen van wie persoonsgegevens worden verzameld, bewaard of anderszins worden verwerkt in het Schengeninformatiesysteem van de tweede generatie (hierna "SIS II" genoemd), hebben het recht van toegang, het recht van verbetering van onjuiste gegevens en het recht van verwijdering van onrechtmatig opgenomen gegevens[1]. In deze gids worden de modaliteiten voor de uitoefening van deze rechten beschreven.

I. Inleiding bij het Schengeninformatiesysteem van de tweede generatie (SIS II)

SIS II is een grootschalig IT-systeem dat is opgezet als compenserende maatregel voor de afschaffing van de interne grenscontroles en dat als doel heeft om een hoog niveau van veiligheid te garanderen binnen een ruimte van vrijheid, veiligheid en recht van de Europese Unie, onder meer door handhaving van de openbare orde en veiligheid en vrijwaring van de veiligheid op het grondgebied van de lidstaten. SIS II wordt ten uitvoer gelegd in alle EU-lidstaten, met uitzondering van Cyprus, Kroatië en Ierland[2], en in vier geassocieerde staten: IJsland, Noorwegen, Zwitserland en Liechtenstein.

SIS II is een informatiesysteem dat nationale rechtshandhavings-, justitiële en administratieve autoriteiten in staat stelt specifieke taken te verrichten door relevante gegevens te delen. Ook de Europese agentschappen Europol en Eurojust hebben beperkte toegangsvoorrechten tot dit systeem.

Categorieën van verwerkte informatie

SIS II centraliseert twee brede categorieën van informatie, die de vorm aannemen van signaleringen van, ten eerste, *personen* – die worden gezocht met het oog op aanhouding, vermissing, een gerechtelijke procedure of onopvallende of gerichte controles, of omdat ze onderdaan van een derde land zijn aan wie de toegang tot of het verblijf in het Schengengebied is geweigerd, en ten tweede, *voorwerpen* – zoals voertuigen, reisdocumenten of creditcards, met het oog op inbeslagneming of gebruik in strafrechtelijke procedures of voor onopvallende of specifieke controles.

Rechtsgrondslag

Afhankelijk van het type signalering, wordt SIS II gereguleerd door ofwel 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), te weten met betrekking tot signaleringsprocedures die vallen onder titel IV van het Verdrag tot oprichting van de Europese Gemeenschap – de voormalige eerste pijler (hierna de "SIS II-verordening" genoemd), ofwel door 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), met betrekking tot procedures die vallen onder titel VI van het Verdrag betreffende de Europese Unie – de voormalige derde pijler (hierna het "SIS II-besluit" genoemd).

[1] Deze rechten worden verleend door artikel 41 van Verordening (EG) nr. 1987/2006 van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) en artikel 58 van 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).

[2] Informatie d.d. juli 2015. Hoewel zij het SIS ten uitvoer hebben gelegd, verrichten Bulgarije en Roemenië nog interne grenscontroles. Het Verenigd Koninkrijk heeft toegang tot het SIS, behalve tot signaleringen ter fine van weigering van toegang tot het Schengengrondgebied.

Categorieën van verwerkte persoonsgegevens

Wanneer een signalering een persoon betreft, moet de informatie altijd de voor- en achternaam alsmede eventuele aliassen, het geslacht, een verwijzing naar de aan een signalering ten grondslag liggende beslissing en de te nemen maatregel omvatten. Indien beschikbaar, kan de signalering ook informatie omvatten zoals specifieke, objectieve fysieke kenmerken die niet aan verandering onderhevig zijn, de geboorteplaats en -datum, foto's, vingerafdrukken, nationaliteit(en), of de betrokkene gewapend of gewelddadig is of is ontsnapt, de reden van de signalering, de signalerende autoriteit, en koppeling(en) met andere SIS II-signaleringen in overeenstemming met artikel 37 van de SIS II-verordening of artikel 52 van het SIS II-besluit.

Architectuur van het systeem

SIS II bestaat uit 1) een centraal systeem (het "centrale SIS II"), 2) een nationaal systeem (het "N.SIS II") in elke lidstaat, dat in verbinding staat met het centrale SIS II, en 3) een communicatie-infrastructuur tussen het centrale systeem en de nationale systemen waarmee een versleuteld virtueel netwerk tot stand wordt gebracht dat specifiek voor SIS II-gegevens bestemd is, en gegevens worden uitgewisseld tussen de Sirene-bureaus[3].

II. Rechten van natuurlijke personen van wie gegevens worden verwerkt in SIS II

In overeenstemming met de gegevensverwerkingsbeginselen verlenen de SIS II-verordening en het SIS II-besluit specifieke rechten aan natuurlijke personen van wie gegevens worden verwerkt in SIS II[4], welke rechten hieronder nader worden geanalyseerd. Eenieder die een van deze rechten wil uitoefenen, kan zich wenden tot de bevoegde autoriteiten in de lidstaat van zijn of haar keuze waar SIS II wordt gebruikt. Deze optie is mogelijk omdat alle nationale databanken (N.SIS II) identiek zijn aan de databank van het centrale systeem[5]. Deze rechten kunnen derhalve worden uitgeoefend in alle landen die SIS II gebruiken, ongeacht de lidstaat die de signalering heeft doen uitgaan.

Wanneer een natuurlijke persoon zijn of haar recht van toegang, verbetering van onjuiste gegevens of verwijdering van onrechtmatig opgenomen gegevens uitoefent, moeten de bevoegde autoriteiten binnen strikte termijnen antwoorden. De betrokkene wordt zo spoedig mogelijk en uiterlijk zestig dagen na de datum waarop hij of zij om toegang heeft verzocht, geïnformeerd, of eerder indien het nationale recht in een kortere termijn voorziet[6]. Ook wordt de betrokkene zo spoedig mogelijk op de hoogte gesteld van het gevolg dat wordt gegeven aan de uitoefening van zijn of haar recht van verbetering of verwijdering van gegevens, en in elk geval binnen drie maanden vanaf de datum waarop hij of zij om verbetering of

[3] De SIS II-gegevens worden ingevoerd, geactualiseerd, verwijderd en opgehaald via de verschillende nationale systemen. Het centrale systeem, dat technische toezicht- en administratieve functies verricht, bevindt zich in Straatsburg (Frankrijk). Dit systeem levert de diensten voor de invoering en verwerking van SIS II-gegevens. Een centraal back-upsysteem, dat in staat is alle functionaliteiten van het centrale hoofdsysteem in stand te houden als het centrale systeem uitvalt, is gevestigd bij Salzburg (Oostenrijk). Elke lidstaat is verantwoordelijk voor het opzetten, doen functioneren en onderhouden van zijn eigen nationale systeem en voor de verbinding van het nationale systeem met het centrale systeem. Elke lidstaat wijst een autoriteit aan, de nationale SIS II-instantie (N.SIS II-instantie), die de centrale verantwoordelijkheid heeft voor zijn SIS II-project. Deze autoriteit is verantwoordelijk voor de goede werking en beveiliging van het nationale systeem.

[4] Zie in het bijzonder artikel 41 van de SIS II-verordening en artikel 58 van het SIS II-besluit.

[5] Zie artikel 4, lid 1, onder b), van de SIS II-verordening en het SIS II-besluit.

[6] Zie 41, lid 6, van de SIS II-verordening en artikel 58, lid 6, van het SIS II-besluit.

verwijdering heeft verzocht, of binnen een kortere termijn indien het nationaal recht daarin voorziet[7].

Recht van toegang

Het recht van toegang biedt de mogelijkheid aan eenieder die daartoe een verzoek heeft ingediend, om te weten te komen welke informatie over hem of haar is opgeslagen in een gegevensbestand als bedoeld in het nationaal recht. Dit is een fundamenteel beginsel van gegevensbescherming dat betrokkenen in staat stelt controle uit te oefenen over door derden bewaarde persoonsgegevens. In dit recht wordt uitdrukkelijk voorzien in artikel 41 van de SIS II-verordening en artikel 58 van het SIS II-besluit.

Het recht van toegang wordt uitgeoefend in overeenstemming met het recht van de lidstaat waar het verzoek wordt ingediend. De procedures lopen uiteen tussen de landen, evenals de regels voor het meedelen van gegevens aan de verzoeker. Wanneer een lidstaat een verzoek om toegang tot een signalering die niet door hemzelf is doen uitgegaan, ontvangt, moet die staat de signalerende lidstaat de gelegenheid bieden om zijn standpunt over de bekendmaking van de gegevens aan de verzoeker kenbaar te maken[8]. Deze informatie wordt niet aan de betrokkene meegedeeld als dit onontbeerlijk is voor een rechtmatige, uit de signalering voortvloeiende taakuitoefening of ter bescherming van de rechten en vrijheden van andere personen.

Momenteel zijn er twee typen systemen die van toepassing zijn op het recht van toegang tot door rechtshandhavingsinstanties verwerkte gegevens, en derhalve ook op SIS-gegevens. In sommige lidstaten is het recht van toegang direct, in andere indirect.

In geval van **directe toegang** dient de betrokkene een verzoek rechtstreeks in bij de autoriteit die de gegevens gebruikt (politie, *gendarmerie*, douane, enz.). Indien het nationale recht dit toestaat, kan de op de verzoeker betrekking hebbende informatie aan hem of haar worden toegezonden.

In geval van **indirecte** toegang zendt de betrokkene zijn of haar verzoek om toegang aan de nationale gegevensbeschermingsautoriteit van de staat waar het verzoek wordt ingediend. De gegevensbeschermingsautoriteit verricht de nodige verificaties bij het afhandelen van het verzoek en antwoordt de verzoeker.

Recht van verbetering en verwijdering van gegevens

Het recht van toegang wordt aangevuld met het recht om persoonsgegevens te doen verbeteren wanneer deze feitelijk onjuist of onvolledig zijn, en het recht om te vragen om verwijdering van persoonsgegevens die onrechtmatig zijn opgenomen (artikel 41, lid 5, van de SIS II-verordening en artikel 58, lid 5, van het SIS II-besluit).

Krachtens het wettelijk kader van Schengen kan alleen de staat die een signalering in SIS II heeft doen uitgaan, deze signalering wijzigen of verwijderen (zie artikel 34, lid 2, van de SIS II-verordening en artikel 49, lid 2, van het SIS II-besluit). Als het verzoek wordt ingediend in een lidstaat waarvan de signalering niet is uitgegaan, werken de bevoegde autoriteiten van de betrokken lidstaten samen bij de afhandeling van de zaak door informatie uit te wisselen en de nodige verificaties te verrichten. De verzoeker moet de gronden van het verzoek om verbetering of verwijdering van de gegevens verstrekken en alle relevante informatie verzamelen die het verzoek ondersteunt.

[7] Zie artikel 41, lid 7, van de SIS II-verordening en artikel 58, lid 7, van het SIS II-besluit.
[8] Zie artikel 41, lid 3, van de SIS II-verordening en artikel 58, lid 3, van het SIS II-besluit.

Rechtsmiddelen: het recht om een klacht in te dienen bij de gegevensbeschermingsautoriteit of een procedure aanhangig te maken bij de rechtbank

Artikel 43 van de SIS II-verordening en artikel 59 van het SIS II-besluit voorzien in rechtsmiddelen waarvan natuurlijke personen gebruik kunnen maken indien hun verzoek niet is ingewilligd. Eenieder kan bij de rechtbanken of de volgens het recht van de lidstaat bevoegde instantie een procedure initiëren wegens een hem of haar betreffende signalering teneinde toegang te krijgen tot de opgenomen informatie of deze te doen verbeteren, te doen verwijderen of te verkrijgen of om schadevergoeding te verkrijgen.

In geval van een klacht met een grensoverschrijdend element moeten de nationale gegevensbeschermingsautoriteiten met elkaar samenwerken om de rechten van de betrokkene te garanderen.