Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2019

248

Besluit van 1 juli 2019, houdende regels inzake het gebruik van het burgerservicenummer door de stichting Slachtofferhulp Nederland (Besluit gebruik burgerservicenummer door Slachtofferhulp Nederland)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister voor Rechtsbescherming van 10 april 2019, nr. 2563265;

Gelet op artikel 89, eerste lid, van de Grondwet;

De Afdeling advisering van de Raad van State gehoord (advies van 23 mei 2019, nr. W16.19.0096/II);

Gezien het nader rapport van Onze Minister voor Rechtsbescherming van 26 juni 2019, nr. 2636096, Directie Wetgeving en Juridische Zaken;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit wordt verstaan onder:

a. *wet:* de Wet algemene bepalingen burgerservicenummer;

b. *registratie:* een registratie als bedoeld in artikel 3, eerste lid, onderdeel d, van de wet;

c. *slachtoffer:* de persoon, bedoeld in artikel 51a, eerste lid, onderdeel a, onder 1° of 2°, van het Wetboek van Strafvordering;

d. *familielid:* een van de personen, bedoeld in artikel 51a, eerste lid, onderdeel b, van het Wetboek van Strafvordering;

e. *authenticatie:* een elektronisch proces voor de verificatie en bevestiging van de identiteit van het slachtoffer of een familielid;

f. *identificatiemiddel:* een middel dat identificatiegegevens bevat waarmee het slachtoffer of een familielid dat toegang wenst tot elektronische dienstverlening of informatieverschaffing geauthentiseerd kan worden.

Artikel 2

De stichting Slachtofferhulp Nederland gebruikt het burgerservicenummer van het slachtoffer of van een familielid bij door haar verrichte werkzaamheden ten aanzien van:

a. het bij overheidsorganen opvragen en van hen ontvangen, het vastleggen en raadplegen en het aan overheidsorganen verstrekken van persoonsgegevens van het slachtoffer of een familielid;

b. elektronische dienstverlening en informatieverschaffing aan het slachtoffer of een familielid, waarbij authenticatie plaatsvindt door middel van een identificatiemiddel dat is toegelaten bij of krachtens enig wettelijk voorschrift.

Artikel 3

De stichting Slachtofferhulp Nederland is in het kader van de werkzaamheden, bedoeld in artikel 2, bevoegd in verband met de uitvoering van artikel 12 van de wet een registratie te raadplegen om na te gaan:

a. of aan een bepaald slachtoffer of familielid reeds een burgerservicenummer is toegekend en zo ja, welk burgerservicenummer;

b. aan welk slachtoffer of familielid een bepaald burgerservicenummer is toegekend.

Artikel 4

Dit besluit berust vanaf het tijdstip dat het bij koninklijke boodschap van 15 januari 2019 ingediende voorstel van wet tot wijziging van de Penitentiaire beginselenwet, het Wetboek van Strafrecht en enige andere wetten in verband met de wijziging van de regeling inzake detentiefasering en voorwaardelijke invrijheidstelling (Wet straffen en beschermen) (Kamerstukken 35122) tot wet is verheven en in werking is getreden op artikel 51aa, vijfde lid, van het Wetboek van Strafvordering.

Artikel 5

1. Dit besluit treedt in werking met ingang van 1 oktober 2019.

2. Dit besluit vervalt met ingang van 1 oktober 2022 indien het voorstel van wet, bedoeld in artikel 4, op 1 oktober 2022 niet tot wet is verheven en in werking is getreden, tenzij voor of op die datum anderszins in een wettelijke grondslag voor dit besluit is voorzien.

Artikel 6

Dit besluit wordt aangehaald als: Besluit gebruik burgerservicenummer door Slachtofferhulp Nederland.

Het advies van de Afdeling advisering van de Raad van State wordt met de daarbij behorende stukken openbaar gemaakt door publicatie in de Staatscourant.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

's-Gravenhage, 1 juli 2019

Willem-Alexander

De Minister voor Rechtsbescherming,
S. Dekker

Uitgegeven de *negende* juli 2019

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

stb-2019-248
ISSN 0920 - 2064
's-Gravenhage 2019

NOTA VAN TOELICHTING

Algemeen deel

1.1 Inleiding

De stichting Slachtofferhulp Nederland (hierna: SHN) is een rechtspersoon met een wettelijke taak als bedoeld in artikel 1.1 van de Compatibiliteitswet 2016 (rwt).[1] Deze taak komt in de kern neer op juridische, praktische en emotionele ondersteuning van slachtoffers van vermoedelijke strafbare feiten of hun nabestaanden, dan wel bepaalde familieleden van het slachtoffer.[2] Dit is een maatschappelijk belangrijke taak, die bijdraagt aan het herstel van het leed van slachtoffers, zodat zij zo veel mogelijk weer zelf verder kunnen.

In het Regeerakkoord 2017 «Vertrouwen in de toekomst» is benadrukt dat de positie van het slachtoffer een speerpunt blijft en dat het kabinet daarnaast inzet op het wegnemen van allerhande knelpunten in de praktijk. Deze ambitie wordt nader ingevuld in de Meerjarenagenda slachtofferbeleid 2018-2021.[3] Daarin is onder meer opgenomen dat SHN in 2018 haar online dienstverlening uitbreidt (onder meer met mogelijkheden voor chats en webcare via sociale media). Op die manier kan zij vanaf 2019 (50%) meer slachtoffers bereiken. Daarnaast is in de Meerjarenagenda opgenomen dat voor slachtoffers (in 2019) een eerste versie van een ketenbreed digitaal informatieportaal beschikbaar zal zijn – het «ketenbrede slachtofferportaal» – waaraan naast SHN de Nationale Politie (hierna: de politie), het Openbaar Ministerie (hierna: het OM), het Centraal Justitieel Incassobureau (hierna: het CJIB) en het Schadefonds Geweldsmisdrijven (hierna: het Schadefonds) zullen deelnemen. Daarin zullen slachtoffers 24 uur per dag overzichtelijk en via één online ingang informatie over hun zaak kunnen vinden. Het portaal draagt bij aan de gedachte van «één overheid voor de burger» en aan de digitalisering van de dienstverlening van de overheid. Het zal eraan bijdragen dat slachtoffers goede en eenduidige informatie krijgen over het verloop van hun (straf)zaak, via één digitale ingang.

1.2 Doelen van het besluit

Deze algemene maatregel van bestuur schrijft voor dat SHN bij bepaalde, specifiek omschreven werkzaamheden gebruik maakt van het burgerservicenummer (BSN) van slachtoffers. Dit is, zoals in paragraaf 1.6 zal worden toegelicht, noodzakelijk voor een correcte en veilige uitvoering van die werkzaamheden.

Enerzijds gaat het om het gebruik van het BSN bij de (veelal elektronische) verwerking van de persoonsgegevens van slachtoffers. Daarbij moet vooral worden gedacht aan het administratief vastleggen van het BSN van het slachtoffer na ontvangst van diens gegevens. Deze gegevens worden in de meeste gevallen verstrekt door de politie of het OM (circa 80 procent). Ook komt het voor dat het slachtoffer zichzelf meldt bij SHN, bijvoorbeeld via het callcenter (circa 20 procent). Naast de administratieve

---

[1] Zie https://www.rekenkamer.nl/onderwerpen/instellingen-op-afstand-van-het-rijk/rechtspersonen-met-een-wettelijke-taak.

[2] Deze taak komt tot uitdrukking in de artikelen 6 en 7 van de Wet Justitie-subsidies en de op artikel 7 gegronde Regeling Aanwijzing rechtspersoon slachtofferhulp (Stcrt. 2008, 142). Daarnaast komt die wettelijke taak naar voren in artikel 51aa, derde lid, van het Wetboek van Strafvordering, alsmede de artikelen 1 tot en met 3 van het op die bepaling gegronde Besluit slachtoffers van strafbare feiten. Hoewel de wettelijke taak zowel op het slachtoffer als op zijn nabestaande of familieleden van het slachtoffer ziet, wordt in het algemeen deel van deze nota van toelichting omwille van de leesbaarheid steeds alleen gesproken over het slachtoffer.

[3] Kamerstukken II 2017/18, 33 552, nr. 43.

vastlegging moet worden gedacht aan het door SHN raadplegen van het BSN van het slachtoffer nadat dit in de systemen is vastgelegd en aan de verstrekking van die gegevens aan de (bovengenoemde) ketenpartners, of andere overheidsorganen, zoals (de Sociale Dienst van) gemeenten. Ook komt het voor dat SHN persoonsgegevens van slachtoffers opvraagt. Een voorbeeld daarvan betreft het opvragen van tenlasteleggingen bij het OM, waarin gegevens over slachtoffers voorkomen.

Anderzijds gaat het om de hiervoor al genoemde (voorgenomen) werkzaamheden in het kader van nieuwe elektronische online dienstverlening en informatieverschaffing door SHN. Het betreft hier ten eerste de deelname aan het genoemde ketenbrede slachtofferportaal en ten tweede het via haar eigen website aanbieden van een gepersonaliseerde «mijn-omgeving» waarop slachtoffers, na daarop met DigiD te hebben ingelogd, onder meer een voegingsformulier benadeelde partij zullen kunnen invullen, en hun digitale dossier zullen kunnen inzien.

1.3 Het vereiste van een wettelijke grondslag voor het beoogde gebruik van BSN door SHN

Ingevolge artikel 87 van de Algemene verordening gegevensbescherming (AVG) kunnen de lidstaten de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer nader vaststellen. Nederland heeft dat gedaan via de Wet algemene bepalingen burgerservicenummer (Wabb). Op dit moment mag SHN het BSN van slachtoffers niet gebruiken. Dat hangt direct samen met de context waarin het begrip «gebruiker» voorkomt in artikel 1 van de Wabb. Gebruiker in de zin van dat artikel zijn (enerzijds) «overheidsorganen» en (anderzijds) «ieder ander [...] voor zover deze werkzaamheden verricht waarbij het gebruik door hem of haar van het burgerservicenummer bij of krachtens de wet is voorgeschreven» (artikel 1, onderdeel d, van de Wabb). Gebruikers in de zin van de Wabb zijn daarmee dus, naast overheidsorganen[4], uitsluitend degenen op wie de wettelijke verplichting tot het gebruik van BSN rust.[5]

Voor het gebruik van het BSN in een andere sector dan de overheid is dus een afzonderlijke wettelijke grondslag nodig. Dat geldt ook voor de toegang tot een aantal met het BSN-stelsel samenhangende (elektronische) faciliteiten ter (verplichte) verificatie van de identiteit van de persoon wiens persoonsgegevens worden verwerkt (artikel 12 jo. 15 van de Wabb). Deze elektronische faciliteiten vormen de zogenaamde «beheervoorziening» (artikel 3 van de Wabb). Alleen gebruikers in de zin van de Wabb kunnen toegang tot die voorziening krijgen.[6]

Tot op heden is niet bij of krachtens de wet voorgeschreven dat SHN bij bepaalde werkzaamheden het BSN van slachtoffers gebruikt en dat zij (in dat kader) de genoemde beheervoorziening mag raadplegen. Dit besluit brengt daarin verandering. Het schrijft ten aanzien van de specifieke werkzaamheden van artikel 2 voor dat SHN daarbij het BSN gebruikt. Het besluit bepaalt eveneens dat SHN – in het kader van die werkzaamheden – bevoegd is om de beheervoorziening te raadplegen om na te gaan a. of aan een bepaald slachtoffer of familielid reeds een BSN is toegekend en zo ja, welk BSN, en b. aan welk slachtoffer of familielid een bepaald BSN

---

[4] Slachtofferhulp Nederland is geen overheidsorgaan, welk begrip in de Wabb wordt gehanteerd om het ruime begrip bestuursorgaan uit artikel 1:1, eerste lid, van de Algemene wet bestuursrecht (Awb), aan te duiden.

[5] De keuze om de omschrijving van deze categorie gebruikers te beperken tot degenen aan wie bij of krachtens de wet een verplichting is opgelegd tot gebruik van het BSN, hangt samen met de beheersbaarheid van het BSN-stelsel (Kamerstukken II 2005/06, 30 312, nr. 3, p. 31) en met name de toegang tot de «beheervoorziening» van artikel 3 van de Wabb.

[6] Zij vallen ook (exclusief) onder de werking van het Besluit burgerservicenummer (Stb. 2007, 443), dat kort gezegd nadere regels stelt over het gebruik van de faciliteiten van de beheervoorziening door «gebruikers» in de zin van de Wabb.

is toegekend. Dat laatste is nodig, omdat SHN als gebruiker van het BSN verplicht zal zijn de identiteit van deze personen te verifiëren (artikel 12 van de Wabb; zie nader de toelichting bij artikel 3).

Volledigheidshalve wordt in dit verband nog overwogen dat artikel 46, tweede lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) dat bepaalt dat bij algemene maatregel van bestuur [...] gevallen (kunnen) worden aangewezen waarin een daarbij aan te wijzen (identificatie)nummer [...] kan worden gebruikt, niet toereikend is voor de in paragraaf 1.2 genoemde doelen van dit besluit. Zij kan namelijk alleen worden gebruikt in gevallen waarin geen verplichting, maar «slechts» een bevoegdheid tot het gebruik van BSN wordt beoogd. Een voorbeeld is het Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht.[7] In artikel 6 van dat Besluit wordt aan beroepsmatig rechtsbijstandverleners en gemachtigden en niet-professionele gemachtigden van natuurlijke personen de bevoegdheid gegeven om het BSN van hun cliënt door te geven aan het digitale systeem van de rechterlijke instanties. Deze rechtsbijstandsverleners en gemachtigden, maar ook andere instanties aan wie op grond van artikel 46, tweede lid, van de UAVG (slechts) de bevoegdheid wordt toegekend om iemands BSN te gebruiken, worden hiermee geen gebruiker in de zin van de Wabb, omdat dit gebruik immers niet is «voorgeschreven» (artikel 1, onderdeel d, van de Wabb). Dit brengt mee dat zij geen toegang kunnen krijgen tot de met het BSN-stelsel samenhangende (elektronische) faciliteiten ter verificatie van de identiteit van de persoon wiens persoonsgegevens worden verwerkt. Voor de genoemde rechtsbijstandsverleners en gemachtigden is dat ook niet nodig; het enige wat zij moeten kunnen, is het namens hun cliënt doorgeven van het BSN aan het digitale systeem van de rechterlijke instanties. De verplichting om vervolgens de identiteit van die cliënt te verifiëren rust niet op hen, maar op de Rechtspraak als overheidsorgaan en gebruiker in de zin van de Wabb (artikel 10 jo. 12 van de Wabb). Voor SHN is dat anders. Zij heeft bij de in artikel 2 van dit Besluit genoemde werkzaamheden straks een vergelijkbare rol als de Rechtspraak in het genoemde voorbeeld. De informatie die SHN over slachtoffers verwerkt en de (online) diensten die zij aan hen ter beschikking zal stellen hebben een gevoelig en vertrouwelijk karakter, hetgeen om een strikte en veilige wijze van identificatie en authenticatie vraagt. Daarvoor is het noodzakelijk dat SHN de meergenoemde beheervoorziening kan raadplegen en dus dat zij gebruiker in de zin van de Wabb wordt. Dat kan niet via artikel 46, tweede lid, van de UAVG.[8]

1.4 Tijdelijk karakter van de grondslag van het besluit

Bij nota van wijziging (Kamerstukken II 2018/19, 35 122, nr. 7) bij het aan de Tweede Kamer voorgelegde wetsvoorstel straffen en beschermen wordt voorgesteld om in artikel 51aa van het Wetboek van Strafvordering een wettelijke grondslag op te nemen voor het bij algemene maatregel van bestuur (amvb) stellen van regels over het gebruik van het BSN door SHN en over het door haar mogen raadplegen van de «beheervoorziening» van artikel 3 van de Wabb.

---

[7] Deze amvb is overigens gegrond op de artikel 24 van de Wet bescherming persoonsgegevens. Deze bepaling is beleidsneutraal overgenomen in artikel 46 van de UAVG.

[8] Een voorbeeld van bestaande wetgeving die niet-overheidsorganen verplicht het BSN te gebruiken is de Wet gebruik burgerservicenummer in de zorg. Zorgaanbieders, indicatieorganen en zorgverzekeraars dienen het burgerservicenummer van de cliënt in hun administratie op te nemen bij het vastleggen van persoonsgegevens. Tevens dienen zij het burgerservicenummer te vermelden bij de onderlinge uitwisseling van de persoonsgegevens van hun cliënten. Het op deze wet gegronde Besluit gebruik burgerservicenummer in de zorg stelt nadere regels voor het gebruik van het BSN.

Aangezien het gebruik van het BSN onder meer belangrijk is voor het spoedig realiseren van ketenbrede digitale dienstverlening aan slachtoffers, het de bedoeling is dat het genoemde slachtofferportaal al in (de tweede helft van) 2019 in gebruik zal worden genomen en de deelname van SHN daaraan naar het oordeel van de Regering essentieel is, terwijl het niet waarschijnlijk is dat het wetsvoorstel straffen en beschermen alsdan tot wet zal zijn verheven en in werking zal zijn getreden en in casu geen andere formeelwettelijke grondslag voorhanden is, is de grondslag voor dit besluit in dit bijzondere geval vooralsnog gevonden in artikel 89, eerste lid, van de Grondwet. Nu dit besluit vanaf het moment van inwerkingtreding van de Wet straffen en beschermen op artikel 51aa, vijfde lid, van het Wetboek van Strafvordering zal worden gebaseerd (zie artikel 4) en het aldus een tijdelijke voorziening betreft, dit besluit voorts geen voorschriften geeft die door straffen dienen te worden gehandhaafd en ook geen sprake is van onderwerpen ten aanzien waarvan de Grondwet voorschrijft dat de wet deze regelt of dat bepalingen daarover bij of krachtens de wet worden vastgesteld, kan voor het vaststellen van de door dit besluit gegeven algemeen verbindende voorschriften een zelfstandige algemene maatregel van bestuur worden gebruikt (zie Aanwijzingen voor de regelgeving nr. 2.22). Het tijdelijke karakter van de in artikel 89, eerste lid, van de Grondwet gevonden grondslag wordt behalve door artikel 4 ook benadrukt door artikel 5, tweede lid, van dit besluit, dat een horizonbepaling bevat: indien de wet straffen en beschermen op 1 oktober 2022 (nog) niet in werking zal zijn getreden, vervalt dit besluit, tenzij voor of op die datum anderszins in een wettelijke grondslag voor dit besluit is voorzien.

1.5 Consultatie

Over een ontwerp van dit besluit is advies gevraagd aan de Raad voor de rechtspraak (Rvdr), het College van procureurs-generaal van het Openbaar Ministerie (OM), de Nederlandse Vereniging voor Rechtspraak (NVvR), de Nederlandse orde van advocaten (NOvA), de Autoriteit Persoonsgegevens (AP), de politie, het CJIB, SHN en het Schadefonds Geweldsmisdrijven. De Rvdr, het OM, de NVvR, de NOvA, de politie en het CJIB hebben laten weten dat het ontwerpbesluit hen geen aanleiding heeft gegeven tot het maken van opmerkingen. Het Schadefonds en SHN hebben aangegeven het ontwerpbesluit van harte te ondersteunen, vooral omdat gebruik van het BSN belangrijk is voor het realiseren van ketenbrede digitale dienstverlening aan slachtoffers.

Het (instemmende) advies van de Autoriteit Persoonsgegevens en de reacties op de internetconsultatie worden respectievelijk besproken in paragraaf 2.1 en 2.2.

1.6 Gebruik van het BSN bij de (elektronische) verwerking van de persoonsgegevens van slachtoffers

Gebruik van BSN bij het verwerken van persoonsgegevens

SHN beheert in haar administratie vertrouwelijke en gevoelige gegevens over slachtoffers en moet daarbij voldoen aan de hoogste eisen van de (Uitvoeringswet) Algemene verordening gegevensbescherming (AVG). Jaarlijks registreert SHN de persoonsgegevens van circa 250.000 personen en wisselt zij deze deels uit met ketenpartners (de politie, het OM, het CJIB, het Schadefonds) en andere overheidsorganen, zoals gemeenten. Naar verwachting neemt dit aantal de komende jaren toe. Een zorgvuldige omgang met de gegevens van burgers vormt een essentiële bouwsteen voor hun vertrouwen in de overheid, maar ook in organisaties met een publieke taak, zoals SHN. Het gebruik van BSN helpt daarbij, doordat de kans op fouten bij de administratie en het uitwisselen van

persoonsgegevens – en dus ook de kans op privacyschendingen – daardoor aanzienlijk afneemt. BSN is immers een uniek, door de overheid verstrekt nummer. Gebruik daarvan voorkomt dat het vastleggen en uitwisselen van data door SHN moet (blijven) plaatsvinden op basis van (alleen) namen en geboortedata. Dit laatste is een risicovolle werkwijze. Namen en geboortedata kunnen bijvoorbeeld dubbel voorkomen, zijn in de praktijk soms niet of op verschillende wijzen bekend, of zijn ooit eens foutief ingevoerd. Gegevensverwerking op basis van alleen namen en geboortedata is ook onpraktisch, omdat de ketenpartners met wie gegevens worden uitgewisseld allemaal overheidsorganen in de zin van de Wabb zijn en wel het BSN van het slachtoffer mogen gebruiken. Het door dit besluit voorgeschreven gebruik van het BSN door SHN stroomlijnt dus ook de tussen die ketenpartners bestaande werkprocessen voor de uitwisseling van persoonsgegevens.

Gebruik van BSN bij elektronische (online) dienstverlening en informatieverschaffing

Om burgers (en ondernemers) een uniforme en veilige wijze van inloggen te bieden en om organisaties met een publieke taak te faciliteren, biedt de rijksoverheid al jaren generieke elektronische authenticatie- en machtigingsdiensten aan voor burgers, te weten het huidige DigiD en DigiD Machtigen. Ook wordt de voorziening «MijnOverheid» aangeboden: een persoonlijk domein voor de burger voor zaken met de overheid. MijnOverheid biedt momenteel drie diensten: de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens.[9] Deze middelen hebben een adequate mate van veiligheid, door onder meer eisen die worden gesteld aan de wachtwoorden van burgers en de beschikbaarheid van een veilige infrastructuur. In het kader van de authenticatie is sprake van verwerking van het BSN.[10] Overheidsorganen, die ingevolge de Wabb van rechtswege gebruiker van het BSN zijn, kunnen (dus) elektronische (online) diensten aanbieden waarbij de genoemde authenticatie- en machtigingsmethoden worden aangeboden. Zij zijn dan «afnemer van DigiD en DigiD Machtigen» en eventueel ook «afnemer van MijnOverheid» in de zin van artikel 1 van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur (hierna: Besluit GDI). Die mogelijkheid hebben andere partijen dan overheidsorganen, zoals SHN, niet zonder meer. Ten eerste is het aanbieden van genoemde diensten alleen toegestaan aan rechtspersonen met een wettelijke taak (artikel 1 van het Besluit GDI), waarbij het aanbieden van die diensten bovendien in het teken van die wettelijke taak moet staan.[11] Daarnaast moet die rechtspersoon gelet op de met het aanbieden van DigiD, DigiD machtigen en MijnOverheid gepaard gaande verwerking van het BSN, «gebruiker» van het BSN in de zin van de Wabb zijn. Aan die laatste eis voldoet SHN zoals gezegd nog niet.

De online diensten en de informatie die SHN ter beschikking zal stellen aan slachtoffers hebben een gevoelig en vertrouwelijk karakter, hetgeen om een strikte en veilige wijze van identificatie vraagt. Aangezien het online dienstverlening betreft en medewerkers van SHN het slachtoffer daarbij niet fysiek zien, is het daarnaast essentieel dat sprake is van online authenticatie: de controle of de persoon daadwerkelijk is wie hij zegt te zijn.

---

[9] Zie het Besluit verwerking persoonsgegevens generieke digitale infrastructuur (Stb. 2016, 195).

[10] Zie de hoofdstukken 2 en 3 van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur.

[11] Voor zover die rechtspersoon – buiten die wettelijke taak – ook andere werkzaamheden uitvoert mag daarvoor dus geen gebruik worden gemaakt van DigiD en DigiD Machtigen.

Het ketenbrede slachtofferportaal is, zoals al is vermeld, een samenwerkingsverband van de politie, het OM, SHN, het CJIB en het Schadefonds. Het is essentieel dat door alle partners dezelfde sleutel voor identificatie en authenticatie wordt toegepast. Het is immers van wezenlijk belang dat in het portaal data, afkomstig van de respectieve partners, met honderd procent zekerheid in het dossier van dezelfde persoon worden getoond aan het betreffende slachtoffer. Net als bij het hiervóór genoemde uitwisselen van persoonsgegevens tussen de ketenpartners, voorkomt het gebruik van het (unieke) BSN hierbij fouten en privacyschendingen.

Alle andere partners zijn overheidsorganen die gebruik kunnen maken van het BSN. Dat door dit besluit ook SHN, voor zover het de specifieke werkzaamheden van artikel 2 betreft, gebruiker wordt van het BSN, is voor een correcte en veilige uitvoering van die werkzaamheden noodzakelijk. Het voorkomt dat de ontsluiting van zaaks- en persoonsgegevens door de partners binnen het portaal zou moeten plaatsvinden op basis van (alleen) namen en geboortedata. Dit is, zoals al aan de orde kwam, risicovol. Daarnaast voorkomt gebruik van het BSN dat een van DigiD afwijkend inlogregime zou moeten worden gehanteerd. Voor het slachtoffer, dat als burger gewend is bij overheidsinstellingen in te loggen met DigiD, zou dit onduidelijk en verwarrend zijn. Een ander inlogregime zou verder betekenen dat voor slachtoffers gebruikersnamen moesten worden uitgegeven en wachtwoordensystemen moesten worden ontwikkeld en beheerd. Naast extra kosten zou dit ook meer kwetsbaarheden opleveren: de kans dat niet-geautoriseerden toegang tot gegevens van slachtoffers krijgen (datalekken), zou aanzienlijk toenemen. Dit alles geldt evenzeer voor de overige elektronische (online) dienstverlening en informatieverschaffing die SHN zelf, naast het ketenportaal, wil aanbieden. Dit betreft zoals gezegd een gepersonaliseerde digitale omgeving op de website van SHN, waarop het slachtoffer zal kunnen inloggen. Hier zal hij bijvoorbeeld zijn digitale dossier kunnen inzien, elektronisch kunnen corresponderen met medewerkers van SHN, (juridisch) advies kunnen krijgen en een formulier kunnen invullen waarmee hij zich als benadeelde partij in een strafzaak voegt (artikel 51f en 51g Sv), dat vervolgens geautomatiseerd door SHN aan het OM wordt verzonden.

Dat SHN door dit besluit gebruiker wordt van het BSN en het daardoor mogelijk wordt DigiD te gebruiken, waarborgt en bevordert ook hier de veiligheid van de procedure, de bescherming van de persoonsgegevens van het slachtoffer en diens gebruiksgemak.

Het slachtoffer zal, nadat hij via de veilige infrastructuur van DigiD heeft ingelogd op het ketenbrede slachtofferportaal, vervolgens laagdrempelig kunnen doorklikken naar de gepersonaliseerde digitale omgeving op de website van SHN en naar de eventuele andere «mijn-omgevingen» van de ketenpartners («single sign on»).

Gelet op het voorgaande levert dit besluit voor SHN, de genoemde ketenpartners en het slachtoffer de volgende voordelen op:

1. een sterk verminderde kans op fouten bij het vastleggen en uitwisselen van persoonsgegevens en een efficiënter dataverkeer tussen de ketenpartners;
2. een goed beveiligde en voor de burger herkenbare toegang tot de gepersonaliseerde digitale omgeving op de website van SHN (en daarmee ook tot het digitale dossier) en tot het ketenbrede slachtofferportaal, waardoor sprake zal zijn van een sterke waarborg voor de privacy van het slachtoffer en een kleinere kans op datalekken;
3. een voor het slachtoffer laagdrempelig en daarnaast kostenbesparend «single sign on systeem» binnen de keten;
4. een betere naleving van de vigerende wetgeving op het gebied van bescherming van persoonsgegevens (zie nader paragrafen 1.8 en 1.9).

1.7 Lopende zaken

Het besluit heeft vanaf zijn inwerkingtreding directe werking ten aanzien van nieuwe zaken, maar ook voor lopende zaken. Dat betekent dat door SHN, indien het na inwerkingtreding in lopende zaken werkzaamheden verricht die vallen onder artikel 2, het BSN van het desbetreffende slachtoffer dient te worden gebruikt. Dit maakt het bijvoorbeeld mogelijk om het slachtoffer vanaf de datum van inwerkingtreding de gelegenheid te bieden met zijn DigiD in te loggen op het ketenbrede slachtofferportaal of op de «mijn-omgeving» op de website van SHN. En ook bij het uitwisselen van persoonsgegevens met overheidsorganen dient vanaf dat moment het BSN te worden gebruikt.

Op grond van artikel 3 van de Wabb zorgt de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de inrichting en instandhouding van een aantal faciliteiten die noodzakelijk zijn voor een goede werking van het stelsel van burgerservicenummers. Deze faciliteiten worden, zoals al aan de orde kwam, gezamenlijk aangeduid met het begrip «beheervoorziening».

SHN zal in lopende zaken het BSN van slachtoffers kunnen verkrijgen, door aan die beheervoorziening langs elektronische weg de vraag te stellen of aan een bepaald slachtoffer een BSN is toegekend en zo ja welk BSN aan die persoon is toegekend (zie nader artikel 3, onderdeel a, van dit besluit en de toelichting op dat artikel), waarna (geautomatiseerd) een antwoord van de beheervoorziening volgt. Op die manier kan op basis van (een combinatie van) reeds vastgelegde identificerende persoonskenmerken zoals naam, geboortedatum, woonplaats en geslacht, het BSN van het slachtoffer worden achterhaald.

1.8 Verwerking van persoonsgegevens door SHN

Door ten aanzien van de specifieke werkzaamheden van artikel 2 voor te schrijven dat SHN het BSN gebruikt komt zij in zoverre te vallen onder het bereik van de Wabb en het daarop gegronde Besluit burgerservicenummer[12] (Besluit BSN). Daarnaast kan zij – voor zover het de in artikel 2 genoemde elektronische dienstverlening en informatievoorziening betreft – «afnemer van DigiD en DigiD Machtigen» en «afnemer van MijnOverheid» als bedoeld in artikel 1 van het Besluit GDI worden.

Het BSN, een persoonsidentificerend nummer, is een persoonsgegeven als bedoeld in artikel 4, eerste lid, van de Algemene verordening gegevensbescherming (AVG). In algemene zin dient te worden opgemerkt dat met persoonsidentificerende nummers voorzichtig dient te worden omgegaan, onder meer omdat zij de koppeling van verschillende bestanden vergemakkelijken.

Het gebruik van BSN heeft echter geen negatieve gevolgen voor de persoonlijke levenssfeer van slachtoffers. Zoals in de memorie van toelichting bij de Wabb[13] en ook de nota van toelichting bij het Besluit BSN is vermeld, is het BSN immers een hulpmiddel om persoonsgegevens goed te kunnen opslaan, te raadplegen en (efficiënt) uit te wisselen. Het BSN zelf bevat geen informatie die de persoonlijke levenssfeer kan raken en heeft slechts betekenis in samenhang met andere gegevens over de persoon aan wie het nummer is toegekend. Het nummer is dus een administratief hulpmiddel waarvan het toegestane gebruik samenvalt met het toegestaan zijn van de registratie zelf.

---

[12] Stb. 2007, 443.

[13] Zie Kamerstukken II 2005/06, 30 312, nr. 3, paragraaf 8 (De bescherming van persoonsgegevens).

In dit verband wordt vermeld dat SHN persoonsgegevens van slachtoffers van de NP en het OM ontvangt op grond van artikel 4:2, eerste lid, onderdeel b, onder 1°, van het Besluit Politiegegevens, respectievelijk artikel 39f, eerste lid, onderdeel f, van de Wet justitiële en strafvorderlijke gegevens.

De grondslag voor het verwerken van «gewone» persoonsgegevens van slachtoffers door SHN is gelegen in de wettelijke taak van SHN (zie voetnoot 2).

Tot de verwerking van (bijzondere) gegevens over de gezondheid van slachtoffers is SHN bevoegd op grond van de uitzondering op het verbod uit artikel 9, eerste lid, van de AVG om bijzondere categorieën persoonsgegevens te verwerken, zoals opgenomen in artikel 30, derde lid, onderdeel a, en vierde lid, van de Uitvoeringswet AVG (UAVG). Persoonsgegevens van strafrechtelijke aard, tenslotte, mogen door SHN worden verwerkt op grond van artikel 33, eerste lid, onderdeel a, van de UAVG.

SHN verwerkt persoonsgegevens uitsluitend ten behoeve van de in de artikelen 4 tot en met 6 van het Privacyreglement Slachtofferhulp Nederland[14] vermelde doelen, waarvan de uitoefening van haar (wettelijke) taken vanzelfsprekend het overkoepelende doel vormt (hiernaar wordt in voetnoot 2 in dat reglement uitdrukkelijk verwezen).

Het feit dat SHN bij de in dit besluit gespecificeerde werkzaamheden gebruik kan maken van de voorzieningen van het BSN-stelsel draagt bij aan de bescherming van de persoonlijke levenssfeer van slachtoffers. Immers, het BSN-stelsel faciliteert voor gebruikers de verificatie (via de genoemde beheervoorziening van artikel 3 van de Wabb) van het BSN en de bijbehorende persoonsgegevens uit de BRP en de verificatie van de geldigheid van identiteitsdocumenten (zie met name de artikelen 12 en 14 tot en met 16 van de Wabb). Deze verificaties dragen bij aan de zorgvuldigheid waarmee gebruikers omgaan met persoonsgegevens.

Ook is het zo dat het gebruik van het BSN technische en praktische barrières bij het uitwisselen van persoonsgegevens vermindert. Ten aanzien van SHN kan hierbij in het bijzonder worden gedacht aan het uitwisselen van gegevens met ketenpartners en andere overheidsorganen en het koppelen van slachtoffergegevens binnen het ketenbrede slachtofferportaal. Het koppelen van gegevens met behulp van het BSN zorgt ervoor dat de organisaties die gegevens uitwisselen minder andere persoonsgegevens hoeven uit te wisselen om de zekerheid te krijgen dat ze met dezelfde persoon van doen hebben. Dit is in het belang van de privacy van het slachtoffer en zorgt voor een kleinere kans op fouten bij de gegevensuitwisseling en datalekken.

1.9 Gegevensbeschermingseffectbeoordeling (GBE)

Een ontwerp van dit besluit is onderworpen aan een gegevensbeschermingseffectbeoordeling (GBE).[15] Daarbij is overwogen dat het gebruik door SHN van het BSN bij de in artikel 2 omschreven werkzaamheden noodzakelijk is om op een veilige en betrouwbare manier gegevens aan een slachtoffer te verstrekken en, in het belang van het slachtoffer, zaaksgegevens met ketenpartners uit te wisselen. Het gebruik wordt proportioneel geacht. Ten aanzien van de inbreuk op de persoonlijke levenssfeer van slachtoffers wordt ten opzichte van de huidige praktijk

[14] Te vinden op https://www.slachtofferhulp.nl/over-deze-site/privacy.
[15] Ministerie van Justitie en Veiligheid, Directie Beschermen, Aanpakken en Voorkomen, 28 september 2018.

geen nadrukkelijke verandering gezien. Daarbij is van belang dat wordt ingestemd met de hierboven vermelde notie dat het BSN zelf geen informatie bevat die de persoonlijke levenssfeer kan raken, dat het in feite slechts een administratief hulpmiddel is en dat het alleen betekenis heeft in samenhang met andere gegevens over de persoon aan wie het nummer is toegekend. Een alternatief voor het voorstel en de daarmee te bereiken doelen wordt niet aanwezig geacht.

Er worden enkele vertrouwelijkheids- en integriteitsrisico's gezien. Daarbij gaat het – kort gezegd – om 1) ongeautoriseerde toegang tot BSN-gegevens van slachtoffers door medewerkers van SHN, 2) een «hack» van het Cliënt Registratie en Informatie Systeem (CRIS) van Slachtofferhulp Nederland of de online «mijn-omgeving» met als mogelijk gevolg een datalek, 3) een onjuiste registratie van een BSN met een persoonsverwisseling als mogelijk gevolg en 4) een niet toegestane registratie van het BSN van een slachtoffer. Dit laatste kan het geval zijn bij een slachtoffer dat niet onder het bereik van dit besluit valt (zie de toelichting bij artikel 1) of ten aanzien van werkzaamheden van SHN die niet zijn vermeld in artikel 2 van dit besluit.

Ten aanzien van alle risico's wordt echter geconcludeerd dat zij van dien aard zijn dat er – in de GBE nader gespecificeerde – technische, organisatorische en juridische maatregelen kunnen worden genomen die deze risico's in voldoende mate verminderen.

De GBE heeft geen aanleiding gegeven tot wijziging van het ontwerpbesluit.

2.1 Advies Autoriteit Persoonsgegevens

Over een ontwerp van dit besluit is advies gevraagd aan de Autoriteit Persoonsgegevens. Zij heeft laten weten dat het ontwerpbesluit haar geen aanleiding heeft gegeven tot het maken van opmerkingen.

2.2 Internetconsultatie

Een ontwerp van dit besluit is van 19 juli 2018 tot 31 augustus 2018 ter consultatie voorgelegd via www.internetconsultatie.nl. De volgende vragen zijn gesteld: 1) bent u het eens met het doel van het ontwerpbesluit (zie paragraaf 1.2 van de nota van toelichting) en 2) denkt u dat het ontwerpbesluit inderdaad zal zorgen voor de in paragraaf 1.2 genoemde voordelen?

Er zijn twee reacties ontvangen.

In de eerste reactie op de internetconsultatie werden enkele bezwaren tegen het besluit naar voren gebracht en daarnaast drie vragen gesteld. Deze bezwaren en vragen, voor zover van belang voor dit besluit, zien in de kern op 1) de voorgenomen online dienstverlening en de daarmee verbonden (digitale) waarborgen voor de privacy van slachtoffers en de veiligheid van zijn persoonsgegevens alsmede 2) de toegankelijkheid van de hulpverlening door SHN.

Ten aanzien van de privacy van slachtoffers en de veiligheid van zijn gegevens werd ten eerste gevraagd of wordt geregistreerd wanneer iemand inlogt op de website van SHN. Bij het gebruik van DigiD voor de afname van digitale (overheids)diensten is het altijd zo dat gedurende een inlogsessie gebruiks- en accountgegevens worden verwerkt, zoals persoonsgegevens van de gebruiker, het IP-adres van het apparaat waarmee de gebruiker inlogt en het tijdstip van begin en einde van de inlogsessie (artikel 2, onderdeel c, van het Besluit GDI). Deze gegevens worden maximaal vijf jaar bewaard (artikel 11, derde lid, Besluit GDI). Opgemerkt wordt dat de vastlegging van de genoemde gegevens is omgeven met verschillende waarborgen voor de beveiliging en de

betrouwbaarheid van de desbetreffende voorzieningen. Op dit punt wordt verwezen naar hetgeen daarover in de nota van toelichting bij het Besluit GDI is vermeld (zie met name paragraaf 6.2)

Ten tweede werd gesteld dat DigiD verschillende zwakke punten kent, die vóór de inwerkingtreding van dit besluit zouden moeten worden verbeterd. Op dit moment is DigiD het enige identificatiemiddel voor burgers in het publieke domein. Hoewel het in het verleden is voorgekomen dat DigiD tijdelijk stilgelegd moest worden omdat er kwetsbaarheden aan het licht kwamen in de gebruikte software, moet DigiD nog steeds worden beschouwd als een identificatiemiddel dat een adequate mate van veiligheid biedt, onder meer door eisen die worden gesteld aan de wachtwoorden van burgers en de beschikbaarheid van een bijzonder veilige infrastructuur. Wel is het zo dat het mede in verband met de toename van het aantal publieke diensten die digitaal van de overheid kunnen worden afgenomen noodzakelijk is maatregelen te treffen om elektronische identificatie ook in de toekomst goed te borgen. In dat verband wordt opgemerkt dat burgers na inwerkingtreding van de wet digitale overheid (*Kamerstukken 34972*) de beschikking zullen krijgen over publieke identificatiemiddelen (eID) met een hoger betrouwbaarheidsniveau dan DigiD. De afnemer bepaalt daarbij het zekerheidsniveau dat past bij de betreffende dienst.

Tenslotte werd naar voren gebracht dat de bij het ketenbrede slachtofferportaal voorziene mogelijkheid van «eenmalig inloggen», waardoor slachtoffers niet opnieuw hoeven in te loggen als ze in dezelfde browsersessie vanuit het ketenportaal naar bijvoorbeeld de «mijn-omgeving» van de politie navigeren, een bedreiging voor hun privacy meebrengt: indien bij een van de betrokken websites sprake is van een lek, zou ook informatie van SHN kunnen worden gestolen.

Zoals gezegd is DigiD een veilig en betrouwbaar identificatiemiddel voor online dienstverlening. Dat is ook zo bij het aanbieden van de functionaliteit «eenmalig inloggen». DigiD eenmalig inloggen is beveiligd door middel van een «PKIoverheid-certificaat» (waarbij PKI staat voor Public Key Infrastructure). Dit is de standaard voor het beveiligen van elektronische overheidsdiensten.

Met behulp van PKIoverheid-certificaten is de informatie die personen en organisaties over het internet sturen op een hoog niveau van betrouwbaarheid beveiligd. Sinds enkele jaren wordt gebruik gemaakt van een nieuw PKIoverheid-certificaat, op basis van het zogenaamde SHA256-algoritme, dat nog vele malen veiliger is. Dit certificaat is gebaseerd op een verbeterde en meer toekomstbestendige techniek voor het versleutelen van berichten, waardoor veilige dienstverlening ook in de toekomst gegarandeerd blijft.

Ten aanzien van de toegankelijkheid van de hulpverlening door SHN is gevraagd of de komst van de online dienstverlening ten koste zal gaan van (toegang tot) persoonlijke hulpverlening. Dat is niet het geval: het slachtoffer zal zelf de keuze mogen (blijven) maken hoe hij ondersteund wil worden: via persoonlijk contact, telefonisch of online. Het blijft ook mogelijk om anoniem hulp te krijgen, bijvoorbeeld via het online platform. Bij een dergelijk hulpverzoek is nog geen sprake van inloggen in een «mijn-omgeving».

In de tweede reactie op de internetconsultatie werd als mening naar voren gebracht dat alleen overheidsorganen toegang zouden moeten hebben tot BSN. In paragraaf 1.3 van deze nota van toelichting is echter aangegeven dat de Wabb de mogelijkheid biedt dat bij of krachtens de wet wordt bepaald dat ook anderen dan overheidsorganen het BSN

gebruiken. Daarnaast is in die paragraaf uitvoerig gemotiveerd waarom dit voor SHN zou moeten gelden.

De beide reacties op de internetconsultatie hebben niet tot aanpassing van de tekst of de toelichting van het besluit geleid.

2.3 De lasten voor de overheid, burgers en bedrijven

Bij de voorbereiding van dit voorstel is bij SHN, de politie, het OM, het CJIB en het Schadefonds nagegaan of zij verwachten dat het voorstel voor hen uitvoeringsconsequenties zal hebben. Met uitzondering van SHN hebben deze partijen aangegeven dat het besluit incidentele noch structurele gevolgen zal hebben voor hun (administratieve) werklasten en financiën. Zij voorzien slechts dat zij bestaande werkprocessen ten aanzien van de uitwisseling van persoonsgegevens moeten wijzigen, aangezien SHN straks ook het BSN van slachtoffers registreert. Dit vergt echter alleen een minimale aanpassing.

Het voorstel heeft meer gevolgen voor SHN, al zijn ook voor haar de effecten beperkt: na inwerkingtreding zal bij de registratie van nieuwe cliënten naast de huidige persoonsgegevens ook het BSN worden vastgelegd. Daarbij zal SHN op grond van artikel 12 van de Wabb in een aantal gevallen de juistheid van het BSN dienen te verifiëren en daartoe verificatievragen via de beheervoorziening stellen. Daarop zal SHN dus ook moeten worden aangesloten.

Zoals al aan de orde kwam, zal SHN na inwerkingtreding ook in lopende zaken het BSN aan de bestaande registraties van persoonsgegevens toevoegen. Dit betreft een eenmalige inhaalslag (zie ook paragraaf 1.6 van deze nota van toelichting).

Na inwerkingtreding van het besluit is gegevensuitwisseling met andere partijen mogelijk op basis van het BSN, zonder dat (ook) andere gegevens dienen te worden vermeld. Hiervan wordt een afname in administratieve lasten verwacht.

Tot slot wordt vermeld dat het besluit alleen betrekking heeft op slachtoffers van een mogelijk strafbaar feit. SHN biedt echter ook diensten aan andere categorieën slachtoffers aan, zoals verkeersslachtoffers. Werkprocessen en IV-voorzieningen moeten erop ingericht blijven dat het BSN van deze categorie slachtoffers niet wordt gebruikt. Dit is volgens SHN goed te realiseren.

Consultatie van het Adviescollege toetsing regeldruk

Over een ontwerp van dit besluit is advies gevraagd aan het Adviescollege toetsing regeldruk (ATR). Het ATR heeft laten weten dat het de analyse en conclusie dat er geen noemenswaardige gevolgen voor de regeldruk zijn, deelt.

2.4 Financiële gevolgen

In de vorige paragraaf is aangegeven dat het besluit alleen uitvoeringsconsequenties heeft voor SHN. De kosten daarvan worden betaald door SHN uit de voor haar (jaarlijks) beschikbaar gestelde middelen. Er kan onderscheid worden gemaakt tussen incidentele kosten, samenhangend met de implementatie van het besluit, en structurele kosten.

Incidentele kosten

Voor de bouw van de berichtenservice van Digid moet een koppelvlak worden ingericht. Tevens is er een koppeling nodig met de BRP. Voor de aansluiting op het applicatielandschap van Slachtofferhulp Nederland is er een aantal webservices nodig voor de CRIS (het CRM-systeem van SHN) en voor de online omgeving van SHN. Hiervoor is de inhuur van een Backend developer en een architect noodzakelijk. De verwachte ontwikkelkosten hiervoor zijn in totaal € 102.332.

Daarnaast zal het verwerken van het BSN in de primaire processen van Slachtofferhulp Nederland geïmplementeerd moeten worden. Meer dan 1500 medewerkers moeten geïnformeerd worden over de aanpassingen in hun CRM-systeem, zodat ze slachtoffers juist informeren. Dit project staat in de jaarplannen van de organisatie benoemd en hiervoor is ruimte beschikbaar gemaakt. De implementatiekosten die worden gemaakt, hebben betrekking op projectkosten waaronder een implementatiecoördinator en een projectmedewerker. Daarnaast zijn er kosten voor training en scholing van bestaande medewerkers en aanpassingen in de e-learning modules voor nieuwe medewerkers. De totale kosten voor implementatie zijn begroot op € 104.939.

De incidentele kosten worden begroot op in totaal (€ 102.332 + € 104.939 =) € 207.271

Structurele kosten vanaf 2020

Het gaat hier om bevragingen van de berichtenservice van Digid per casus. In 2018 zijn er door Slachtofferhulp Nederland 215.000 casussen aangemaakt. Per bevraging wordt een vast bedrag in rekening gebracht. Verder zijn er vaste kosten verbonden aan het aantal webservers die ontwikkeld worden: een testserver, twee applicatieservers en een load balancer.

De structurele kosten worden begroot op in totaal € 34.900.

Artikelsgewijs deel

Artikel 1

Dit artikel bevat begripsomschrijvingen. Deze spreken grotendeels voor zich.

Ten aanzien van de begrippen *authenticatie* en *identificatiemiddel* is aangesloten bij de definities van deze begrippen in artikel 1 van het wetsvoorstel digitale overheid (*Kamerstukken 34972*). Dit wetsvoorstel regelt onder meer dat publieke dienstverleners verplicht zijn om identificatiemiddelen van het betrouwbaarheidsniveau «substantieel» of «hoog» te gebruiken om toegang te geven tot online diensten waarbij de overheid deze betrouwbaarheidsniveaus nodig vindt. Burgers krijgen in de toekomst dus de beschikking over publieke identificatiemiddelen (eID) met een hoger betrouwbaarheidsniveau dan DigiD. Hiervoor gelden de relevante bepalingen uit de Europese eidas-verordening.[16]

De begrippen s*lachtoffer en familielid* geven samen de (omvang van de) kring van personen aan op wie dit besluit betrekking heeft. De verwijzing naar respectievelijk artikel 51a, eerste lid, onderdeel a, onder 1° of 2°, en

[16] Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, PB L257 van 28.8.2014, blz. 73.

onderdeel b, van het Wetboek van Strafvordering, heeft tot gevolg dat SHN bij de in artikel 2 omschreven werkzaamheden alleen het BSN van slachtoffers van vermoedelijke strafbare feiten, hun nabestaanden en de (in onderdeel b van artikel 51a, eerste lid, genoemde) familieleden van het slachtoffer gebruikt. Het gebruik wordt tot deze kring beperkt. Een bredere opvatting van het slachtofferbegrip, waardoor bijvoorbeeld ook verkeersslachtoffers of slachtoffers van een ramp (waarbij geen sprake is van een vermoedelijk strafbaar feit) onder de werking van dit besluit zouden komen te vallen, laat zich niet rijmen met de wettelijke taak van SHN (zie voetnoot 2), die immers ook niet verder reikt dan de genoemde personen. Een bredere opvatting zou ten aanzien van de voorgenomen elektronische dienstverlening ook onmogelijk zijn, omdat de «afnemer» van DigiD, DigiD Machtigen en Mijn overheid ofwel een overheidsorgaan ofwel een rechtspersoon met een wettelijke taak moet zijn (artikel 1 van het Besluit GDI). Het aanbieden van die diensten door een rechtspersoon met een wettelijke taak moet, zoals al aan de orde kwam, in het teken van die wettelijke taak staan. Anders gezegd: die diensten mogen niet worden aangeboden aan personen die niet binnen die wettelijke taak zijn te brengen. Een en ander betekent uiteraard niet dat er verschillende niveaus van dienstverlening zullen ontstaan. SHN zal andere slachtoffers dan bedoeld in artikel 1 met onverminderde inzet blijven bijstaan, ook al mag hun BSN niet worden gebruikt. Zoals al aan de orde kwam, zal SHN haar werkprocessen en IV-voorzieningen daarop inrichten.

Ten aanzien van de noodzaak om ook het BSN van familieleden van het slachtoffer te kunnen gebruiken, wordt nog het volgende overwogen. Familieleden van slachtoffers, voor zover genoemd in artikel 51a, eerste lid, onderdeel b, van het Wetboek van Strafvordering, behoren zoals gezegd tot de kring van personen ten aanzien van wie SHN een wettelijke taak heeft. Zij hebben ingevolge artikel 51aa, derde lid, van het Wetboek van Strafvordering recht op ondersteuning door een slachtofferhulporganisatie. Dit is uitgewerkt in artikel 2, derde lid, van het Besluit slachtoffers van strafbare feiten: «De familieleden van het slachtoffer hebben toegang tot slachtofferhulporganisaties, rekening houdend met hun behoeften en de mate waarin zij schade hebben geleden als gevolg van het tegen het slachtoffer gepleegde strafbare feit.» Hoewel de politie geen verwijzingsplicht heeft, kan zij familieleden wel naar SHN verwijzen (Kamerstukken II 2014/15, 34 236, nr. 3, p. 13). In die gevallen kan het dus zo zijn dat een familielid zich meldt bij SHN met een verzoek om ondersteuning. Daarnaast kunnen familieleden van slachtoffers zich sinds de inwerkingtreding van de Wet Affectieschade (Stb. 2018, 132) in bepaalde gevallen (indien het slachtoffer blijvend ernstig letsel heeft opgelopen, of bij «verplaatste schade») in het strafproces voegen als benadeelde partij.

In voorkomende gevallen verwerkt SHN dus in de praktijk ook persoonsgegevens van familieleden van slachtoffers en het is tevens wenselijk dat ook familieleden in het kader van de aan hen verstrekte hulp en ondersteuning gebruik zullen kunnen maken van de komende elektronische online dienstverlening. Voor het belang van het gebruik van het BSN daarbij wordt verwezen naar hetgeen daarover in het algemeen deel van deze nota van toelichting is vermeld.

Artikel 2

Artikel 2 bakent de werkzaamheden af waarvoor dit besluit voorschrijft dat SHN het BSN gebruikt. Dit is in overeenstemming met artikel 1, onderdeel d, onder 2°, van de Wabb, waarin is bepaald dat gebruiker in de zin van de Wabb kan zijn «ieder ander dan een overheidsorgaan [...] *voor zover* deze werkzaamheden verricht waarbij het gebruik [...] van het burgerservicenummer bij of krachtens de wet is voorgeschreven.» De

afbakening van werkzaamheden, die in het algemeen deel van deze nota van toelichting inhoudelijk al aan de orde zijn gekomen, brengt enerzijds mee dat SHN bij die werkzaamheden niet slechts bevoegd, maar verplicht is het BSN van het slachtoffer, zijn nabestaande of een familielid te gebruiken. Immers, gebruiker in de zin van de Wabb is uitsluitend degene op wie de wettelijke verplichting (daartoe) rust. De keuze om de omschrijving van deze categorie gebruikers te beperken tot degenen, aan wie bij of krachtens de wet een verplichting is opgelegd te beperken tot gebruik van het burgerservicenummer, hangt samen met de toegang tot de faciliteiten van het BSN-stelsel, en hetgeen met die toegang samenhangt. Hierbij speelt onder meer de beheersbaarheid van het stelsel een rol (Kamerstukken II 2005/06, 30 312, nr. 3, p. 31).

Anderzijds brengt die afbakening mee dat SHN bij al haar overige werkzaamheden *geen* gebruiker in de zin van de Wabb wordt en dus bij die werkzaamheden het BSN van het slachtoffer, zijn nabestaande of een familielid niet mag gebruiken.

Nader over de werkzaamheden in onderdeel a

Bij de werkzaamheden, bedoeld in onderdeel a, is gekozen voor het «bij overheidsorganen opvragen en van hen ontvangen» en het «aan overheidsorganen» verstrekken van persoonsgegevens. Hierbij wordt gedoeld op persoonsgegevens als bedoeld in de artikelen 4, eerste lid, 9, eerste lid, en 10, van de AVG.

Hoewel SHN de meeste persoonsgegevens van slachtoffers ontvangt van de NP en het OM en verstrekking meestal ook aan die partijen (en/of het CJIB of het fonds) plaatsvindt, gebeurt het in de praktijk ook regelmatig dat aan andere overheidsorganen persoonsgegevens worden verstrekt. Medewerkers van SHN (met name in het casemanagement) hebben namens slachtoffers, nabestaanden en familieleden vooral veel contacten met gemeenten (waaronder in ieder geval de Sociale Dienst) en met instanties zoals het UWV en de SVB, over inkomens- en uitkeringsgerelateerde vraagstukken. Door deze instanties wordt altijd als eerste naar een BSN gevraagd.

Nader over de werkzaamheden in onderdeel b

Bij deze werkzaamheden gaat het alleen om elektronische dienstverlening en informatieverschaffing aan het slachtoffer of een familielid, waarbij op het ketenbrede slachtofferportaal of op de website van SHN moet worden ingelogd. Het gaat niet om de nu reeds aangeboden elektronische diensten voor «chats» en «webcare». Hierbij vindt elektronisch contact met een (mogelijk) slachtoffer plaats via social media zoals facebook of twitter, op het openbare deel van de website van SHN, zonder dat daarbij identificatie en authenticatie plaatsvindt en zonder dat wordt ingelogd. SHN is in dit contact reactief en legt daarvan bovendien geen (persoons)gegevens vast. SHN kan het slachtoffer in dit contact bijvoorbeeld wel informeren over de mogelijkheden voor dienstverlening. Na inwerkingtreding van dit besluit zal ook kunnen worden verwezen naar het slachtofferportaal of de digitale «mijn-omgeving» op de website van SHN, waar een slachtoffer zal kunnen inloggen met zijn DigiD.

De voorzieningen voor identificatie en authenticatie worden in onderdeel b functioneel omschreven. De huidige middelen DigiD en DigiD Machtigen en MijnOverheid worden niet genoemd, zodat de bepaling ook de grondslag kan bieden voor opvolgers van deze voorzieningen en eventuele nieuwe voorzieningen. Deze omschrijving houdt nauw verband met het al genoemde wetsvoorstel digitale overheid. Met de formulering

«waarbij authenticatie plaatsvindt door middel van een identificatiemiddel dat is toegelaten bij of krachtens enig wettelijk voorschrift» wordt alvast aangesloten bij de terminologie van artikel 8 van genoemd wetsvoorstel.

De inwerkingtreding van de wet digitale overheid zal overigens niet betekenen dat dit besluit dan moet worden aangepast. Wel zal SHN bij besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, in overeenstemming met de Minister voor Rechtsbescherming, «voor de toepassing van die wet moeten worden aangewezen», omdat zij als niet-overheidsorgaan niet automatisch onder de toepassing van de wet zal vallen (zie nader artikel 3, vijfde lid, van het wetsvoorstel, alsmede paragraaf 3.4 van de memorie van toelichting).

Ten aanzien van de werkzaamheden, bedoeld in onderdeel b, wordt volledigheidshalve opgemerkt dat dit besluit niet (automatisch) regelt dat SHN bij de desbetreffende elektronische diensten DigiD, DigiD Machtigen en MijnOverheid mag gaan aanbieden. Hiervoor moet SHN «afnemer» van die diensten in de zin van artikel 1 van het Besluit GDI worden. Die voorzieningen zijn in beheer bij Logius, de dienst digitale overheid die valt onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. In de aansluitprocedure zal onder meer worden vastgesteld of de verzoekende organisatie inderdaad gebruiker is in de zin van de Wabb. Dit geldt overigens ook voor (het verzoek tot) het gebruik van de beheervoorziening, bedoeld in artikel 3 van de Wabb, die in het algemeen deel van deze nota van toelichting al ter sprake kwam.

Artikel 3

Op grond van artikel 3 van de Wabb zorgt de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de inrichting en instandhouding van een aantal faciliteiten die noodzakelijk zijn voor een goede werking van het stelsel van burgerservicenummers. Deze faciliteiten worden gezamenlijk aangeduid met het begrip «beheervoorziening».

Ingevolge artikel 12 van de Wabb zijn gebruikers verplicht zich er bij het verwerken van persoonsgegevens waarbij een BSN wordt gebruikt, van te vergewissen dat het BSN betrekking heeft op de persoon wiens persoonsgegevens hij verwerkt.

De vergewisplicht wordt ondersteund door het BSN-stelsel, doordat aan de genoemde beheervoorziening langs elektronische weg de vraag kan worden gesteld of aan een bepaalde persoon een BSN is toegekend en zo ja welk BSN aan die persoon is toegekend (waarna (geautomatiseerd) een antwoord van de beheervoorziening volgt). Op deze wijze kan het BSN van een bepaalde persoon worden nagetrokken. Aan de beheervoorziening kan voorts de vraag worden gesteld op welke persoon een bepaald BSN betrekking heeft. Daarmee kan gecontroleerd worden of het BSN dat een persoon opgeeft, inderdaad betrekking heeft op de persoon in kwestie, onder meer door vergelijking van de gegevens op een (Nederlands of buitenlands) identiteitsdocument. Ook kan door middel van de beheervoorziening worden nagegaan of het document, met behulp waarvan een persoon zich identificeert, een document is als bedoeld in artikel 1, eerste lid, onder 1°, 2° of 4°, van de Wet op de identificatieplicht.

Artikel 15 van de Wabb bevat de grondslag voor het verstrekken van gegevens aan gebruikers in verband met de beantwoording van de genoemde verificatievragen. Aan iedere gebruiker – dus ook niet-overheidsorganen (zoals SHN) voor wier werkzaamheden wordt voorgeschreven dat het BSN wordt gebruikt – staat de verificatievraag open die gericht is op de geldigheid van een in verband met artikel 12

overgelegd identiteitsdocument. Voor wat betreft de overige verificatievragen staat de toegang uit privacyoverwegingen voor niet-overheidsorganen slechts open voor zover aan hen bij of krachtens wet een verplichting is opgelegd of een bevoegdheid is verleend zulke verificatievragen te stellen (artikel 15, derde lid, van de Wabb).

Het onderhavige artikel verleent aan SHN de bevoegdheid om ook de in het artikel genoemde verificatievragen via de beheervoorziening te stellen. Het kan onder omstandigheden bij «back office» gegevensverwerkingen toereikend zijn om te verifiëren dat de bron of bronnen van de verwerkte gegevens voldoende betrouwbaar zijn, bijvoorbeeld omdat aan de bron een grondige verificatie heeft plaatsgevonden (Kamerstukken II 2005/06, 30 312, nr. 3, p. 36). Hierbij kan worden gedacht aan een verificatie door de NP of het OM die reeds heeft plaatsgevonden voordat de slachtoffergegevens waaronder het BSN aan SHN worden toegezonden. Er zijn echter ook situaties denkbaar waarin een slachtoffer of zijn familielid zich nog voordat hij zich tot de NP (of het OM) heeft gewend, bij SHN terechtkomt (fysiek, telefonisch, of via elektronisch inloggen). Als SHN dan werkzaamheden als bedoeld in artikel 2 verricht, dient zij op grond van artikel 12 van de Wabb de juistheid van het BSN te verifiëren. Voor dat soort gevallen dient SHN bevoegd te zijn de beheervoorziening te raadplegen. Daarop zal SHN dus ook moeten worden aangesloten: zij zal zich moeten aanmelden bij de beheerder van die beheervoorziening. Bijlage 3 bij het Besluit BSN regelt welke gegevens dan worden verstrekt.

Artikel 4

Dit artikel bevat een zogenoemde omhangbepaling, die het tijdelijke karakter van de vooralsnog in artikel 89, eerste lid, van de Grondwet gevonden grondslag voor dit besluit benadrukt. Door deze bepaling wordt de grondslag van het besluit gewijzigd zodra de Wet straffen en beschermen (Kamerstukken 35 122) in werking treedt. Vanaf dat moment zal het besluit berusten op het nieuwe vijfde lid van artikel 51aa, van het Wetboek van Strafvordering.

Artikel 5

Eerste lid

Het eerste lid van dit artikel regelt de inwerkingtreding van dit besluit met ingang van 1 oktober 2019. Dit moment hangt samen met de komst van het ketenbrede slachtofferportaal, dat volgens de huidige inschattingen eind 2019 gereed zal kunnen zijn.

Tweede lid

Het tweede lid bevat een zogenoemde horizonbepaling. Om het tijdelijke karakter van de vooralsnog in artikel 89, eerste lid, van de Grondwet gevonden grondslag van dit besluit extra te benadrukken, wordt bepaald dat het besluit op 1 oktober 2022 vervalt indien de Wet straffen en beschermen alsdan (nog) niet in werking zal zijn getreden. Mocht deze – overigens op voorhand niet te verwachten – situatie zich voordoen, dan voorkomt deze bepaling dat het (op zichzelf noodzakelijke) gebruik van het BSN door SHN te lang zou blijven plaatsvinden zonder de daarvoor vereiste formeelwettelijke basis. Omdat echter ook moet worden voorkomen dat SHN, indien die situatie zich zou voordoen, bij de in artikel

2 genoemde werkzaamheden het BSN niet meer mag gebruiken, is in deze bepaling tevens tot uitdrukking gebracht dat het besluit niet vervalt indien op 1 oktober 2022 is voorzien in een andere wettelijke grondslag.

De Minister voor Rechtsbescherming,
S. Dekker