

Wijziging van de Wet digitale overheid in verband met onder meer het stellen van regels over het Meldpunt Fouten in Overheidsregistraties en het Centraal Meldpunt Identiteitsfraude

(KetenID WGK11010)

Voorstel van wet

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

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om in de Wet digitale overheid regels te stellen over het Meldpunt Fouten in Overheidsregistraties en het Centraal Meldpunt Identiteitsfraude, de regeling over het toezicht op de naleving te verduidelijken en de specifieke uitkering aan provincies of gemeenten ter verbetering van de digitale dienstverlening wettelijk te verankeren;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

De Wet digitale overheid wordt als volgt gewijzigd:

A

In artikel 1. wordt in de alfabetische volgorde een begripsbepaling ingevoegd, luidende:

- overheidsregistratie: registratie die wordt gebruikt voor het uitvoeren van een publieke taak;

B

In artikel 3. wordt, onder vernummering van het vierde en vijfde lid tot vijfde onderscheidenlijk zesde lid, na het derde lid een lid ingevoegd, luidende:

4. Bij ministeriële regeling kunnen de technische instructies of opties voor het configureren van een aangewezen standaard worden gewijzigd.

C

Na artikel 16. wordt een nieuw hoofdstuk 5a ingevoegd, luidende:

HOOFDSTUK 5A. Het Meldpunt Fouten in Overheidsregistraties en het Centraal Meldpunt Identiteitsfraude

Artikel 16a. Meldpunt Fouten in Overheidsregistraties

1. Onze Minister draagt zorg voor de inrichting van een Meldpunt Fouten in Overheidsregistraties.

2. Bij het meldpunt kan melding worden gedaan van het vermoeden van de verwerking van onjuiste gegevens in een overheidsregistratie, waaronder persoonsgegevens:

- a. door of namens eenieder op wie onjuiste gegevens in een overheidsregistratie betrekking hebben;
- b. door een organisatie met een publieke taak.

3. Het meldpunt heeft de volgende taken:

a. het beoordelen van de in het tweede lid bedoelde meldingen en het naar aanleiding van een melding coördineren van het proces van het herstel van onjuiste gegevens in overheidsregistraties en de gevolgen daarvan, in het bijzonder het uitwisselen van persoonsgegevens met de verwerkingsverantwoordelijke van de in het tweede lid bedoelde overheidsregistratie;

b. het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft;

c. het analyseren van meldingen in verband met ontwikkelingen omtrent fouten in overheidsregistraties, het bijhouden van statistische beleidsinformatie en het in geanonimiseerde vorm delen hiervan met derden.

4. Gelet op artikel 9, aanhef en tweede lid, onder g, van de Algemene verordening gegevensbescherming, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien het meldpunt deze verwerkt voor zover noodzakelijk voor de uitvoering van de in het derde lid, onderdelen a en b, bedoelde taken.

5. Gelet op artikel 10 van de Algemene verordening gegevensbescherming mag het meldpunt persoonsgegevens van strafrechtelijke aard als bedoeld in dat artikel verwerken, indien de verwerking noodzakelijk is voor de uitvoering van de in het derde lid, onderdelen a en b, bedoelde taken.

6. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de gegevensverwerking door het meldpunt, waaronder het treffen van passende waarborgen ter bescherming van persoonsgegevens.

7. Bij ministeriële regeling kunnen regels worden gesteld over de wijze waarop de melding kan worden gedaan en over de procedure voor de behandeling van de melding.

Artikel 16b. Centraal Meldpunt Identiteitsfraude

1. Onze Minister draagt zorg voor de inrichting van een Centraal Meldpunt Identiteitsfraude.

2. Bij het meldpunt kan melding worden gedaan van het vermoeden van identiteitsfraude:

a. door of namens eenieder op wie het vermoeden van identiteitsfraude betrekking heeft;

b. door een organisatie met een publieke taak.

3. Het meldpunt heeft de volgende taken:

a. het beoordelen van meldingen van het vermoeden van identiteitsfraude en naar aanleiding van een melding coördineren van het proces van het herstel van identiteitsfraude en de gevolgen hiervan, in het bijzonder het uitwisselen van persoonsgegevens over de identiteitsfraude met de betrokken organisatie;

b. het begeleiden, adviseren en ondersteunen van degene op wie de melding van identiteitsfraude betrekking heeft;

c. het analyseren van meldingen in verband met ontwikkelingen omtrent identiteitsfraude, het bijhouden van statistische beleidsinformatie, en het in geanonimiseerde vorm delen hiervan met derden;

d. het adviseren van organisaties over identiteitsfraude;

e. het bijdragen aan de publieke bewustwording over identiteitsfraude;

f. het adviseren over de ontwikkeling van applicaties om identiteitsfraude te voorkomen of te stoppen.

4. Gelet op artikel 9, aanhef en tweede lid, onder g, van de Algemene verordening gegevensbescherming, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien het meldpunt deze verwerkt voor zover noodzakelijk voor de uitvoering van de in het derde lid, onderdelen a en b, bedoelde taken.

5. Gelet op artikel 10 van de Algemene verordening gegevensbescherming mag het meldpunt persoonsgegevens van strafrechtelijke aard als bedoeld in dat artikel verwerken, indien de

verwerking noodzakelijk is voor de uitvoering van de in het derde lid, onderdelen a en b, bedoelde taken.

6. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de gegevensverwerking door het meldpunt, waaronder het treffen van passende waarborgen ter bescherming van persoonsgegevens.

7. Bij ministeriële regeling kunnen regels worden gesteld de wijze waarop de melding kan worden gedaan en over de procedure voor de behandeling van de melding.

D

Artikel 17. wordt als volgt gewijzigd:

1. Het tweede lid komt te luiden:

2. Met het toezicht op de naleving van het bepaalde bij of krachtens de artikelen 3, 6, 7, 8, eerste lid, en 15 door de besturen van waterschappen en gemeenschappelijke regelingen waaraan geen bevoegdheden zijn overgedragen door de besturen van provincies of gemeenten zijn belast de bij besluit van Onze Minister aangewezen ambtenaren.

2. Het derde lid vervalt, onder vernummering van het vierde tot en met achtste lid tot derde tot en met zevende lid.

3. In het vierde lid (nieuw) wordt "het Agentschap Telecom" vervangen door "de Rijksinspectie Digitale Infrastructuur".

4. In het vijfde lid (nieuw) wordt "eerste, tweede, vierde en vijfde lid" vervangen door "eerste tot en met vierde lid".

E

In artikel 28., onderdeel b, wordt "Tijdelijk besluit digitale toegankelijkheid overheid" vervangen door "Besluit digitale toegankelijkheid overheid".

ARTIKEL II

Aan onderdeel A van Bijlage I. bedoeld in artikel 124b, eerste lid, van de Gemeentewet wordt een onderdeel toegevoegd, luidende:

9. Wet digitale overheid.

ARTIKEL III

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

MEMORIE VAN TOELICHTING

I. ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel strekt tot wijziging van de Wet digitale overheid (Wdo). Deze wet vormt een eerste tranche van wetgeving ten behoeve van de verdere digitalisering van de overheid. De Wdo is vanaf 1 juli 2023 fasegewijs in werking getreden. Met dit wetsvoorstel wordt de Wdo op verschillende punten gewijzigd.

Ten eerste wordt deze wet uitgebreid met een nieuw hoofdstuk waarin de taken van het Meldpunt Fouten in Overheidsregistraties (MFO) en het Centraal Meldpunt Identiteitsfraude (CMI) en de verwerking van persoonsgegevens door deze meldpunten wettelijk worden geregeld. Een wettelijke grondslag voor gegevensverwerking stelt de meldpunten in staat om meldingen van onjuiste gegevens in overheidsregistraties en identiteitsfraude effectiever te behandelen. Burgers en bedrijven hebben hierbij baat bij, omdat zij hierdoor betere ondersteuning krijgen bij herstel van onjuiste gegevens en identiteitsfraude in overheidsregistraties en de soms ernstige gevolgen hiervan.

Daarnaast wordt een aantal wijzigingen van meer technische aard doorgevoerd. Zo wordt de huidige regeling van het toezicht op de naleving in de Wdo aangepast om beter aan te sluiten bij het stelsel van interbestuurlijk toezicht. Verder wordt een voorziening getroffen om bij ministeriële regeling de technische instructies of opties voor het configureren van een aangewezen standaard te wijzigen.

De hoofdlijnen van het wetsvoorstel worden hieronder verder toegelicht.

2. Hoofdlijnen van het wetsvoorstel

2.1 Wettelijke regeling taken en gegevensverwerking MFO en CMI

Dit wetsvoorstel voorziet in een wettelijke regeling in de Wdo van de taken van en de gegevensverwerking door de meldpunten MFO en het CMI. Hiertoe wordt een nieuw hoofdstuk aan de Wdo toegevoegd. De taakuitoefening van het MFO en het CMI past in het streven van het kabinet naar laagdrempelige ondersteuning van burgers bij herstel van onjuiste gegevens in overheidsregistraties en identiteitsfraude en het oplossen van de daaruit voortkomende problemen. Beide meldpunten zijn ondergebracht bij de Rijksdienst voor Identiteitsgegevens (RvIG), de uitvoeringsorganisatie die onderdeel is van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Gezien het grote en stijgende aantal meldingen dat op jaarbasis wordt ontvangen voorzien de meldpunten in een duidelijke maatschappelijke behoefte. Met dit wetsvoorstel worden, conform de eisen die de Algemene verordening gegevensbescherming (AVG) stelt, rechtsgrondslagen in het nationale recht gecreëerd waarop de verwerking van persoonsgegevens door het MFO en het CMI kan worden gebaseerd.

2.1.1 Achtergrond, taken en werkwijze MFO en CMI

Overheidsregistraties bevatten gegevens van burgers en bedrijven. Deze gegevens worden door veel verschillende organisaties gebruikt, onder meer voor dienstverlening aan burgers en bedrijven, het nemen van besluiten en het uitoefenen van toezicht. Voor burgers en bedrijven is het van belang dat gegevens waarmee de overheid werkt juist zijn. In de praktijk komt het regelmatig voor dat overheidsregistraties onjuistheden bevatten waarvan burgers en bedrijven last ondervinden en die zij zelf niet of niet eenvoudig kunnen oplossen. Hieraan ligt mede ten grondslag dat onjuistheden in overheidsregistraties vaak doorwerken, niet alleen binnen andere overheidsregistraties maar ook in het maatschappelijke verkeer. Burgers en bedrijven kunnen hiervan ernstige nadelen ondervinden, zoals het niet ontvangen of stopzetten van voorzieningen,

zoals kinderopvangtoeslag, of het ontvangen van aanmaningen en boetes. Om de onjuistheden en de gevolgen hiervan ongedaan te maken moeten er meestal verschillende stappen ondernomen worden. In het uiterste geval komt het voor dat een burger of bedrijf naar de rechter moet gaan. Dat is een ongewenste situatie die zoveel mogelijk moet worden voorkomen.

In 2019 heeft de Algemene Rekenkamer geadviseerd om een apart meldpunt in het leven te roepen dat burgers en bedrijven ondersteunt bij het oplossen van problemen en het herstellen van fouten waarbij meerdere (basis)registraties zijn betrokken of die organisatie-overstijgend zijn.¹ In navolging hiervan is in 2019 de regering in de motie Van der Molen/Middendorp² verzocht om een gezaghebbend centraal meldpunt in te richten voor burgers die buiten hun schuld om in de knel komen door fouten in basisregistraties.³ In 2021 is hier met de oprichting van het MFO uitvoering aan gegeven. Bij de oprichting heeft de toenmalig staatssecretaris ingestemd met het advies van de beleidsverantwoordelijke om het meldpunt in te richten voor problemen met basisregistraties, met de opdracht voor een inventarisatie van andere registraties die in de praktijk tot problemen leiden. Naar aanleiding van de eerste ervaringen van het meldpunt hebben de beleidsverantwoordelijke en RvIG daarna – in lijn met dit advies – besloten om de taak van het meldpunt uit te breiden naar ‘overheidsregistraties in het algemeen’. De ondersteuning van het MFO zou immers ophouden als een fout geen relatie heeft tot een basisregistratie, terwijl de praktijk heeft uit gewezen dat burgers evengoed problemen met andere overheidsregistraties (dan basisregistraties) ervaren en dezelfde behoefte aan hulp hebben. Het begrip overheidsregistratie is destijds gedefinieerd als een registratie in een basisregistratie én alle andere registraties die worden gebruikt voor het uitvoeren van een publieke taak. Het gaat bijvoorbeeld om de registratie van rijbewijsgegevens bij de RDW of de registratie van een postadres bij de Belastingdienst. Het kan ook gaan om de registratie van gegevens die rechtspersonen, zoals een zorgverzekeraar, een notaris of een pensioenfonds gebruiken voor de uitvoering van een publieke taak. Door deze uitbreiding heeft het MFO ook de taak om burgers te helpen met een fout in een registratie, die buiten een basisregistratie valt, maar die wordt bijgehouden voor de uitvoering van een publieke taak.

Het MFO biedt ondersteuning aan eenieder die problemen ondervindt met gegevens die worden verwerkt in overheidsregistraties en het gebruik daarvan. Het MFO biedt begeleiding, ondersteuning en advies bij het herstel van onjuiste gegevens en heeft hierbij een coördinerende rol. Omdat een onjuist gegeven gevolgen kan hebben voor dienstverlening van de overheid aan burgers en bedrijven of het nemen van besluiten heeft het MFO ook een rol bij het bieden van een oplossing voor ontstane gevolgen. Het MFO fungeert hierbij als schakel tussen de burger en de betrokken organisaties. Nadat het MFO een melding heeft onderzocht, worden de organisaties waar de gevolgen zich voordoen benaderd, voorzien van informatie en wordt de casus besproken. Het MFO verstrekt daarbij persoonsgegevens aan deze organisaties, voor zover dit noodzakelijk is voor de behandeling van de melding. Ook kan aan de betrokken organisaties worden gevraagd persoonsgegevens te verstrekken aan het MFO. Degene die de melding heeft gedaan, wordt door het MFO op de hoogte gesteld van de stappen die genomen zijn naar aanleiding van de melding. De overheidsorganisaties die (basis)registraties beheren en de betrokken organisaties waar de gevolgen van de onjuiste gegevens zich voordoen worden ingelicht over de (mogelijk) onjuiste gegevens en blijven zelf verantwoordelijk voor het herstellen van onjuiste gegevens én het indien mogelijk herstellen van de gevolgen van de onjuistheid van de betreffende gegevens. Uit de evaluatie van het MFO in 2024⁴ blijkt dat het in de meeste gevallen de betrokken registratiehouders lukt de vermeende fout te laten onderzoeken en de gevolgen van een fout te herstellen. Tot slot ondersteunt het MFO overheidsorganisaties met advies en coördinerende werkzaamheden door binnengekomen meldingen te analyseren op trends. Persoonsgegevens worden hiervoor geanonimiseerd. Het ministerie van BZK kan deze gegevens gebruiken voor beleidsontwikkeling. Het MFO deelt deze trends – voor zover relevant – met overheidsorganisaties

¹ Algemene Rekenkamer, 2019, Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven, p. 16, bijlage bij Kamerstukken II 2018/19, 29362, nr. 281.

² Kamerstukken II 2018/19, 26643, nr. 630.

³ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/>

⁴ Evaluatie Meldpunt Fouten in Overheidsregistraties | Rapport | Rijksoverheid.nl, p. 34.

als input voor eventuele aanpassingen in de registratie van de gegevens.

Naast fouten in overheidsregistraties kunnen burgers te maken krijgen met misbruik van hun identiteitsgegevens als gevolg van frauduleus handelen van anderen. Regelmatig worden burgers het slachtoffer van identiteitsfraude doordat iemand wederrechtelijk gebruik maakt van hun identiteit, bijvoorbeeld door zich van hun gegevens te bedienen of van (een kopie van) hun identiteitsbewijs. De casuïstiek is zeer divers. Fraudeurs zijn inventief en regelmatig wordt in de media bericht over nieuwe oplichtingsmethodes. Het gevolg van identiteitsfraude kan zijn dat ten onrechte gegevens of dossiers worden gekoppeld aan het slachtoffer, zoals een schuld of het bezit van een telefoon of auto. Dergelijke onterechte mutaties in overheidsregistraties behoeven herstel op een wijze die de gevolgen van de identiteitsfraude zoveel als mogelijk ongedaan maakt. Voor degene die het slachtoffer is van identiteitsfraude, is het niet altijd gemakkelijk te achterhalen welke onterechte mutaties in welke (overheids)registraties zijn gedaan en hoe deze hebben doorgewerkt.

Gezien de voor de betrokkene verstrekende gevolgen van identiteitsfraude is in 2008 onder verantwoordelijkheid van het ministerie van BZK gestart met een proef met een meldpunt waar slachtoffers van identiteitsfraude terecht kunnen voor advies en ondersteuning. Deze proef heeft in 2010 geresulteerd in een definitieve voorziening, het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI).⁵ Voorbeelden van meldingen die bij het CMI kunnen worden gedaan zijn misbruik van een kopie van een identiteitsdocument (paspoort, identiteitskaart of rijbewijs), frauduleus gebruik van identiteitsgegevens door een ander bij het doen van online bestellingen of het constateren van een nepprofiel op sociale media. Hiervoor zijn meldformulieren op de site van het CMI beschikbaar. Na de ontvangst van een melding neemt het CMI contact op met de melder. Als dit nodig is schakelt het CMI met betrokken overheidsorganisaties zoals de politie, Logius, RDW of met ondernemingen en rechtspersonen zoals een telecomprovider of een bank om de gevolgen van de identiteitsfraude ongedaan te maken. Daarnaast levert het CMI een bijdrage aan bewustwording en preventie van identiteitsfraude door middel van verschillende voorlichtingsactiviteiten.

Om een melder zo goed mogelijk te kunnen ondersteunen bij een vermoeden van een fout in een overheidsregistratie of bij identiteitsfraude, hanteren het MFO en het CMI een lage drempel om een melding te kunnen doen. Via de website van de RvIG⁶ kan de melder door middel van een meldingsformulier een melding doen. Ook kan een melder een melding per post sturen of telefonisch contact opnemen.

Het meldingsformulier bevat naast gerichte vragen⁷ ook vrije velden, waarin de melder met het meldpunt informatie kan delen die door de melder van belang wordt geacht voor het beoordelen van de melding. Het toezenden van documenten die naar het oordeel van de melder relevant zijn is vormvrij. Het is voor een melder lastig om te bepalen wat wel of niet noodzakelijke gegevens zijn, hetgeen begrijpelijk is. Niet noodzakelijke gegevens zoals medische gegevens worden daarom door de meldpunten vernietigd of teruggestuurd naar de melder, indien het om per post toegestuurde stukken gaat.

Beide meldpunten voorzien in een duidelijke maatschappelijke behoefte. Sinds de oprichting van het MFO in 2021 is het aantal meldingen op jaarbasis gegroeid van 477 (2021) tot 1152 (2024). In 2024 kon het MFO bij ongeveer 30% van de meldingen vaststellen dat daadwerkelijk sprake was van een fout in een overheidsregistratie.⁸ Het aantal meldingen bij het CMI is tussen 2014 en 2024 gegroeid van 793 naar 6774.

2.1.2 Noodzaak solide rechtsgrondslagen voor de verwerking van persoonsgegevens

Vanaf hun oprichting verwerken het MFO en het CMI (persoons)gegevens in het kader van de behandeling van meldingen en het proces van herstel van onjuiste gegevens en onjuiste of

⁵ Kamerstukken II 2009/10, 29362, nr. 178.

⁶ Zie <https://www.rvig.nl/mfo-burgers> respectievelijk <https://www.rvig.nl/cmi>.

⁷ D.m.v. gerichte vragen wordt zoveel mogelijk erop aangestuurd dat de melder enkel relevante informatie deelt.

⁸ [Evaluatie Meldpunt Fouten in Overheidsregistraties | Rapport | Rijksoverheid.nl](#)

onterechte mutaties van gegevens. Hierbij wordt primair gebruik gemaakt van (persoons)gegevens die door de melder zelf in het meldingsformulier worden aangeleverd, waarbij expliciet van betrokkene toestemming is verkregen om diens persoonsgegevens te verwerken. Voor zover dat nodig is voor de behandeling van een melding en het proces van herstel, vindt gegevensuitwisseling plaats met betrokken overheidsorganisaties, andere organisaties met een publieke taak (MFO en CMI) en ondernemingen en rechtspersonen (CMI).

Op de verwerking van persoonsgegevens door het MFO en het CMI is de AVG van toepassing. Elke gegevensverwerking moet voldoen aan de in de AVG neergelegde beginselen.⁹ De verwerking moet noodzakelijk zijn voor een welbepaald en gerechtvaardigd doel en worden gebaseerd op één van de rechtsgrondslagen in de AVG.¹⁰ Naast de AVG zijn de meldpunten bij de gegevensverwerking gebonden aan de nationale wetgeving, waaronder de Wet algemene bepalingen burgerservicenummer (Wabb) en de Wet basisregistratie personen (Wet BRP). Zowel vanuit het MFO als het CMI is geconstateerd dat het, met het oog op effectieve hulpverlening door de meldpunten, noodzakelijk is om de grondslag voor de gegevensverwerking in overeenstemming met de AVG in nationale wetgeving vast te leggen. Bij de bestaande taakuitvoering lopen de meldpunten tegen verschillende beperkingen aan met betrekking tot de verwerking van persoonsgegevens, die zich als volgt laten samenvatten:

- persoonsgegevens worden verwerkt met (expliciete en geïnformeerde) toestemming van degene die melding doet. Dit kan, gelet op de verhouding burger – overheid echter niet als een bestendige grondslag volstaan voor het verwerken van de voor de behandeling van meldingen en het proces van herstel benodigde persoonsgegevens¹¹;
 - het is niet mogelijk om in het kader van een melding het burgerservicenummer (BSN) te verwerken en gegevens uit de basisregistratie personen (BRP) verstrekt te krijgen, terwijl hieraan wel behoefte is met het oog op een doelmatige behandeling van de meldingen;
 - in sommige gevallen is het nodig om ten behoeve van de behandeling een melding gegevens over gezondheid en persoonsgegevens van strafrechtelijke aard te verwerken, de hiervoor vereiste expliciete wettelijke grondslag ontbreekt echter.¹²
- Dit wordt als volgt toegelicht.

Ten eerste is sinds de oprichting van beide meldpunten de verwerking van persoonsgegevens gebaseerd geweest op de AVG-rechtsgrondslag het geven van toestemming door de betrokkene voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden. In het meldingsformulier geeft de melder toestemming om de hierin opgenomen persoonsgegevens te gebruiken voor de behandeling van de melding. Het is, in de verhouding burger – overheid, niet uitgesloten dat persoonsgegevens op basis van toestemming van de burger worden verwerkt, tenzij die verhouding het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend.¹³ Van dit laatste is geen sprake, gelet op de laagdrempelige en dienstverlenende functie van de meldpunten, die naar vrije keuze van de burger kunnen worden benaderd, en de voorhanden alternatieven, namelijk de mogelijkheid om de overheidsregistratie te benaderen waar de vermeende fout zich voordoet. Vanaf de oprichting van de meldpunten is wel beoogd om in een wettelijke grondslag voor de gegevensverwerking te voorzien. In de uitvoeringspraktijk is gebleken dat verwerking van persoonsgegevens op deze rechtsgrondslag verschillende beperkingen meebrengt voor de behandeling van meldingen door de meldpunten. Zo kunnen beide meldpunten op basis van toestemming nu uitsluitend rechtsgeldig persoonsgegevens van de melder zelf verwerken en geen persoonsgegevens van derden. Dit terwijl informatie die door de melder in het meldingsformulier wordt opgenomen over derden wel relevant

⁹ Artikel 5 van de AVG.

¹⁰ Artikel 6 van de AVG.

¹¹ Vgl. overweging (43) van de AVG: (...) Toestemming mag geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval zijn wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend.

¹² Dit gelet op het verbod op het verwerken van bijzondere categorieën persoonsgegevens in artikel 9 van de AVG en gelet op artikel 10 van de AVG.

¹³ Vgl. *Kamerstukken II* 2017/18, 34851, nr. 4, p.37.

kan zijn bij de behandeling van een melding. Te denken valt aan de situatie waarin de melder niet degene is op wie de persoonsgegevens betrekking hebben, bijvoorbeeld als een medewerker van een gemeente een melding doet bij het MFO omdat het opvalt dat een aantal burgers zich aan de gemeentebalie melden met ogenschijnlijk hetzelfde probleem met een registratie. In de context van het CMI kan als voorbeeld worden genoemd de melder die vermeend slachtoffer is van identiteitsfraude en die persoonsgegevens met het CMI wil delen van de vermoedelijke fraudeur, zoals bijvoorbeeld een marktplaatsadverteerder aan wie de melder eerder een kopie van zijn paspoort heeft gestuurd. Gelet op het vorenstaande bestaat de behoefte aan een wettelijke grondslag voor de gegevensverwerking door de meldpunten.

Een tweede beperking is dat bij de behandeling van meldingen door de meldpunten geen verwerking van het BSN plaatsvindt. Gebruik van het BSN bevordert doelmatig en efficiënt optreden van de meldpunten. Hierdoor kan de oorsprong van een mogelijke fout of de identiteitsfraude beter worden achterhaald en hersteld.

Het gebruik van het BSN wordt gereguleerd in de Wabb. Artikel 10 Wabb bevat voor overheidsorganen een grondslag om het BSN te mogen verwerken bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak. De taak van de meldpunten is op dit moment niet expliciet vastgelegd in wetgeving. Daardoor staat niet buiten twijfel dat de meldpunten het BSN mogen verwerken en aan de hand van het BSN informatie over de melder kunnen opvragen bij andere organisaties.

Een derde beperking bestaat eruit dat er op dit moment geen verstrekking van gegevens uit de BRP plaatsvindt aan de meldpunten. Op grond van artikelen 3.2 Wet BRP en 37 en 38 van het Besluit BRP kan verstrekking van BRP-gegevens plaatsvinden aan een overheidsorgaan, voor zover het overheidsorgaan aantoont dat deze gegevens noodzakelijk zijn voor een goede vervulling van zijn taak. Ook hier geldt dat de taak van de meldpunten momenteel niet expliciet is vastgelegd in wetgeving. Dit kan discussie oproepen of aan de meldpunten BRP-gegevens mogen worden verstrekt, terwijl dit voor een effectieve dienstverlening wel noodzakelijk en wenselijk is. De bijdrage die inzage in de BRP¹⁴ kan leveren aan de dienstverlening komt ook naar voren uit eerdergenoemde evaluatie van het MFO. Hieruit volgt dat de inzage het MFO in staat stelt om meldingen sneller en nauwkeuriger te beoordelen, omdat dan direct kan worden geraadpleegd of de verstrekte informatie correct is.¹⁵ Veel meldingen gaan over onjuiste gegevens die meerdere instanties in een keten delen. Het is vaak niet duidelijk bij welke schakel in de keten de oorzaak van het onjuiste gegeven ligt. De BRP fungeert vaak als centrale schakel in die keten. Het is voor het MFO in die gevallen dus noodzakelijk om in beeld te krijgen hoe het gegeven in de BRP staat geregistreerd en hoe het berichtenverkeer van en naar de BRP of BRP-V (Verstrektingsvoorziening¹⁶) is verlopen. Met inzage kan het MFO dus sneller in beeld krijgen aan welke 'kant' van de BRP het probleem zit (bij de input in de BRP of de output uit de BRP). Verder geeft inzicht in de BRP-V meer informatie over de vraag of de BRP-V een wijziging bijvoorbeeld niet heeft verstuurd of dat een afnemer een wijziging niet goed heeft verwerkt. Deze informatie is in sommige zaken noodzakelijk.

Voor het CMI geldt eveneens dat inzage in de BRP-V van belang kan zijn bij de analyse en behandeling van de melding. Het controleren van gegevens in de BRP-V en het Basisregister Reisdocumenten¹⁷ (BR) helpt het CMI om de situatie te beoordelen en, in het verlengde daarvan, om betrokken organisaties te informeren over de oorzaak, de omvang en de gevolgen van de identiteitsfraude. Het kan bijvoorbeeld van belang zijn om adresgegevens in de BRP-V te raadplegen als iemand een frauduleuze bestelling op een voormalig woonadres van de melder heeft gedaan. Of als een fraudeur of een ex-partner de melder op een ander adres heeft ingeschreven, met alle gevolgen van dien. Ook afnemers van de BRP-V zoals politie, UWV en de Belastingdienst beschikken hierdoor over onjuiste adresgegevens van de melder.

¹⁴ Door middel van een autorisatiebesluit in de zin van artikel 3.2 Wet BRP ten behoeve van de meldpunten.

¹⁵ [Evaluatie Meldpunt Fouten in Overheidsregistraties | Rapport | Rijksoverheid.nl](#), paragraaf 4.8, p. 34.

¹⁶ De BRP-Verstrektingsvoorziening (BRP-V) is de centrale component in het BRP-stelsel. Alle gegevens uit de basisregistratie personen zijn ondergebracht in één centrale landelijke database: BRP-V. BRP-afnemers krijgen gegevens aangeleverd uit de BRP-V.

¹⁷ Basisregister als bedoeld in Paragraaf 3 van de Paspoortwet.

Soms is het voor de behandeling van de melding relevant om gegevens omtrent identiteitsdocumenten te raadplegen. Bijvoorbeeld als een fraudeur zich heeft gelegitimeerd met een identiteitskaart op naam van de melder, terwijl uit de BRP-V blijkt dat de melder enkel over een paspoort beschikt. Deze informatie bevestigt de stelling van de melder dat die slachtoffer is van identiteitsfraude. Met die cruciale informatie kan het CMI een andere organisatie dus beter informeren en dat vergroot de kans dat die organisatie de gevolgen van de fraude herstelt. Inzage in de BRP-V stelt het CMI bovendien in staat om te controleren of de gevolgen van de fraude correct zijn hersteld, zoals bij een onjuiste adresinschrijving. Bovendien kunnen het CMI en het MFO de identiteit van de melder beter controleren, door in de BRP-V een controlevraag (over bijvoorbeeld de geboortedatum van de melder) te stellen. Op grond van de Wabb bestaat daarnaast de plicht voor de meldpunten om zich bij het gebruik van het BSN te vergewissen dat het BSN betrekking heeft op de melder.¹⁸ Door inzage in de BRP kan door de meldpunten aan de vergewisplicht worden voldaan.

Ten vierde bestaat er op dit moment geen expliciete wettelijke grondslag voor het CMI en het MFO om gegevens over gezondheid en persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten te verwerken bij de behandeling van meldingen, zoals vereist door de AVG. Momenteel zijn de meldpunten aangewezen op toestemming van de betrokkene voor het verwerken van diens persoonsgegevens bij de afhandeling van de melding. Zoals hiervoor uiteengezet, volstaat toestemming niet in alle gevallen als bestendige grondslag voor verwerking van persoonsgegevens in de relatie tussen burger en overheid. De meldpunten zijn hierdoor beperkt in hun mogelijkheden om meldingen te onderzoeken en passende hulp aan te bieden, waaronder het opvragen en ontvangen van informatie van andere overheidsorganisaties voor de afhandeling van een melding. In het navolgende wordt dit verder toegelicht.

Gegevens over gezondheid

Gegevens over gezondheid zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.¹⁹ Zij omvatten alle gegevens die betrekking hebben op de gezondheidstoestand van een betrokkene.²⁰ Gegevens over gezondheid zijn een bijzondere categorie van persoonsgegevens. Het verwerken ervan is verboden, tenzij de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht (artikel 9 van de AVG).

In de praktijk komt het voor dat een melder, via de vrije velden in het meldingsformulier of door het delen van documenten gegevens deelt over verleende gezondheidsdiensten, zoals het feit dat betrokkene klant is van een fysiotherapeut of een specialist, of gegevens over opname in een instelling voor gezondheidszorg. Wat betreft het CMI komt het incidenteel voor dat burgers melding doen van identiteitsfraude in de zorg. Er kan in dat geval medische informatie worden door de melder aan het CMI worden verstrekt. Na onderzoek blijkt dat zorgverleners (bijvoorbeeld) de verkeerde persoon geselecteerd hebben bij het ophalen van persoonsgegevens die uit de BRP aan de zorgverlener worden verstrekt. Voor sommige burgers is dit zelfs een repeterend probleem, als personalia erg op elkaar lijken. Als het UWV betrokken is bij een melding bij het CMI of het MFO en er is sprake van een arbeidsongeschiktheids- of ziekte-uitkering dan beschouwt het UWV dat ook als gezondheidsgegevens. Bij het MFO komt het incidenteel voor dat melders in het kader van een melding gezondheidsgegevens delen. Deze worden nu met toestemming van de melder verwerkt. Als voorbeeld kan worden genoemd dat de melder aangeeft dat zijn gegevens niet goed staan geregistreerd bij een zorgverlener dan wel instanties zoals het UWV of het CAK. Meldingen die het UWV betreffen gaan bijvoorbeeld over de onjuiste registratie van de periode dat iemand een arbeidsongeschiktheidsuitkering heeft ontvangen. Een ander voorbeeld is een melding over de onjuiste registratie van een adres, welke onder andere tot gevolg had dat de hoogte van de eigen bijdrage, die het CAK in rekening bracht voor een bepaalde vorm van zorg, onjuist was.

¹⁸ Artikel 12 van de Wabb.

¹⁹ Artikel 4, onder 15, van de AVG.

²⁰ Overweging (35) van de AVG.

In het kader van de behandeling van meldingen door het CMI en het MFO kunnen gegevens over gezondheid dus relevant zijn in het onderzoek of er mogelijk sprake is van identiteitsfraude of van een fout in een bepaalde registratie (in het gezondheidsdomein), en bij het bieden van een oplossing in het specifieke geval, zoals correctie van onjuiste gegevens of het herstel van de gevolgen. Ook kan het noodzakelijk zijn dat organisaties die door het CMI of het MFO worden bevraagd in het kader van de afhandeling van de melding gegevens over gezondheid delen met de meldpunten.

Uit het voorgaande volgt dat beide meldpunten meldingen ontvangen waarbij verwerking van gezondheidsgegevens aan de orde is dan wel kan zijn (in het laatste geval is dit niet *prima facie*, maar pas na de analyse van de melding duidelijk). Gegeven het vanuit het privacy-oogpunt gevoelige karakter van die gegevens en het feit dat deze specifieke bescherming behoeven, is het noodzakelijk dat in een expliciete wettelijke grondslag voor die verwerking wordt voorzien. Dat het momenteel slechts incidentele gevallen of meldingen (en dus verwerkingen) betreft, kan geen argument zijn om niet in die grondslag te voorzien. Burgers krijgen met de wettelijke verankering van de meldpunten een brede mogelijkheid om fouten in overheidsregistraties of identiteitsfraude te melden en om ondersteuning te krijgen. De taak van de meldpunten is om samen met de (verantwoordelijken voor) de overheidsregistraties naar een passende oplossing voor de melder te zoeken. Het ligt in de lijn der verwachting dat gegevens over de gezondheid in de meldingen zullen voorkomen. De gegevens worden verwerkt met het doel om de gevolgen van fraude en/of fouten in overheidsregistraties te De noodzaak van het verwerken van gegevens over gezondheid door het CMI en het MFO strekt niet verder dan het ontvangen ervan met het doel om de gevolgen van identiteitsfraude en/of fouten in overheidsregistraties te herstellen. Ten slotte worden de gegevens niet verwerkt met het doel om de gegevens *als zodanig*, dus voor gezondheidsdoeleinden,²¹ te verwerken.

Strafrechtelijke gegevens

Persoonsgegevens van strafrechtelijke aard zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.²² Gegevens over (gegronde) verdenkingen vallen hier ook onder.²³ Verwerking van deze gegevens is niet toegestaan zonder wettelijke grondslag, die passende waarborgen voor de rechten en vrijheden van de betrokkenen biedt (artikel 10 van de AVG).

Het MFO ontvangt momenteel, zij het sporadisch, meldingen over de registratie van strafrechtelijke gegevens in een overheidsregistratie. Meerdere organisaties registreren en delen gegevens over strafrechtelijke veroordelingen in de strafrechtketen. Het gaat bijvoorbeeld om de rechtspraak, het Openbaar Ministerie (OM), de Justitiële Informatiedienst (Justid), het Centraal Justitieel Incassobureau (CJIB) en de Dienst Justitiële inrichtingen (DJI). Door identiteitsfraude, een persoonsverwisseling, een verwerkingsfout bij een van die ketenorganisaties of door een technische fout tussen de schakels in de keten kan een onjuist gegeven, zoals een strafrechtelijke veroordeling, bij een van de ketenorganisaties in de registratie terechtkomen. Uit recent onderzoek van de Algemene Rekenkamer (AR) blijkt dat Justid sinds 2012 bij minimaal 867 zaken heeft vastgesteld dat verdachten door bijvoorbeeld identiteitsfraude of invoerfouten onder een onjuiste naam staan geregistreerd in de strafrechtketen.²⁴ Het is aannemelijk dat de door de AR geconstateerde onjuiste registraties tot meldingen bij het MFO zullen leiden. Daarom wordt voorgesteld om in een wettelijke grondslag te voorzien voor de verwerking van de strafrechtelijke gegevens door het MFO. Uiteraard zijn de hiervoor genoemde organisaties in de strafrechtsketen primair verantwoordelijk voor de juistheid van de onder hun verantwoordelijkheid vallende registraties en zijn ze een aanspreekpunt voor betrokkene. Gelet op de laagdrempeligheid van het meldpunt en de grotere naamsbekendheid die het meldpunt naar verwachting zal genereren, moet er echter rekening mee worden gehouden dat betrokkene hier diens melding zal neerleggen, en dat niet enkel in de door de AR geconstateerde gevallen. Het is aangewezen dat MFO over een

²¹ Zoals het verstrekken van gezondheidszorg en het beheer van gezondheidszorgdiensten.

²² Vgl. artikel 1 van de UAVG.

²³ Kranenburg & Verhey, *De AVG in Europees en Nederlands perspectief* (MM SBR) 2018, par. 7.4.10.

²⁴ [Resultaten verantwoordingsonderzoek 2024 ministerie van Justitie en Veiligheid](#), p. 5. [Resultaten verantwoordingsonderzoek 2024 ministerie van Justitie en Veiligheid | Rapport | Algemene Rekenkamer](#)

grondslag beschikt om de strafrechtelijke gegevens te mogen verwerken om de melding te kunnen beoordelen en om contact te kunnen leggen met de relevante registratie om de eventuele fout te herstellen.

Ook het CMI verwerkt bij de behandeling van meldingen strafrechtelijke gegevens.

De primaire taak van het CMI is het beoordelen van meldingen van een vermoeden van identiteitsfraude en het coördineren van het proces van het herstel van identiteitsfraude en de gevolgen hiervan. Identiteitsfraude is op grond van artikel 231b van het Wetboek van Strafrecht een strafbaar feit. Veel van de meldingen die het CMI ontvangt, hebben daarom naar hun aard betrekking op een vermoeden van een strafbaar feit of op feiten of omstandigheden die reeds tot een strafrechtelijk oordeel hebben geleid. In de vrije velden van het meldingsformulier vraagt het CMI de melder om:

- de datum waarop de melder de identiteitsfraude heeft ontdekt;
- een omschrijving te geven van de identiteitsfraude;
- de hoogte van de vermoedelijke schade en
- de acties die de melder al heeft ondernomen.

Het CMI vraagt de melder in het meldingsformulier ook of die aangifte heeft gedaan bij de politie. Indien dit het geval is, vraagt het CMI de melder om het proces-verbaal van aangifte mee te sturen met de melding. Het proces-verbaal van aangifte bevat ook een beschrijving van de manier waarop de identiteitsfraude volgens de melder is gepleegd. Verder staan in het proces-verbaal een proces-verbaalnummer en de namen van de verbalisanten/politieagenten die de aangifte hebben opgenomen. Het komt incidenteel voor dat een melder een proces-verbaal of een ander document, zoals een strafrechtelijk vonnis, met het CMI deelt, dat ook persoonsgegevens van strafrechtelijke aard van een ander dan de melder bevat. Samengevat kunnen de meldingen dus strafrechtelijke gegevens bevatten. Hieruit blijkt de noodzaak voor het CMI om strafrechtelijke gegevens te mogen verwerken.

Het CMI vraagt de melder om het proces-verbaal, omdat het in tegenstelling tot de omschrijving in het meldingsformulier een volledig en betrouwbaar beeld van de identiteitsfraude geeft (mogelijk is het proces-verbaal opgemaakt met betrekking tot bijvoorbeeld oplichting, computervredebreuk, diefstal, etc.). Gelet op het feit dat de melder op het politiebureau een verklaring aflegt en het strafbaar is om een valse aangifte te doen, heeft de inhoud van het proces-verbaal een hogere betrouwbaarheidsfactor dan de omschrijving in de vrije velden van het meldingsformulier. Omdat de politie de aangifte opneemt en doorvraagt, staat in het proces-verbaal ook altijd meer en betere informatie. Het proces-verbaal is hierdoor in veel gevallen noodzakelijk voor de beoordeling van de feiten, de daaruit volgende risicoanalyse en het hersteladvies.

Het proces-verbaal is om dezelfde redenen van doorslaggevend belang om een melding te kunnen voorleggen aan organisaties in de strafrechtketen, zoals de politie, Koninklijke Marechaussee en het OM.

De private partijen die het CMI nodig heeft om de identiteitsfraude te stoppen en de gevolgen te herstellen hechten bovendien meer waarde aan het proces-verbaal dan aan de omschrijving in de melding. Het CMI coördineert het contact met alle relevante partijen. Hiervoor heeft het CMI kennis en een netwerk opgebouwd, waardoor de melder zelf niet de weg hoeft te zoeken naar de partijen die verantwoordelijk zijn voor een oplossing.

Tevens geldt hier het once-only-principle: De burger is ermee gebaat dat hij het proces-verbaal met eventuele strafrechtelijke gegevens kan delen met het CMI omdat het proces-verbaal alle relevante informatie bevat en de burger dit dus niet nogmaals uiteen hoeft te zetten bij het indienen van de melding, hetgeen leidt tot administratieve lastenverlichting. Het voorgaande maakt duidelijk dat het MFO en CMI als gevolg van verschillende beperkingen bij de gegevensverwerking belemmerd worden in hun mogelijkheden om meldingen te beoordelen over onjuiste gegevens en identiteitsfraude en passende hulp te bieden. Daarmee komt de laagdrempelige ondersteuning van burgers in het gedrang en worden hun problemen niet altijd op een adequate wijze opgelost.

Hierdoor ontstaat een risico op verergering of escalatie van de problemen met mogelijke ernstige gevolgen voor de burger. Ook kunnen als gevolg hiervan hoge maatschappelijke kosten ontstaan. Om de effectiviteit van beide meldpunten te vergroten zijn solide rechtsgrondslagen voor de gegevensverwerking nodig. Dit wetsvoorstel beoogt hierin te voorzien.

2.1.3 Voorgestelde regeling met betrekking tot de taakuitoefening door het MFO en het CMI en de verwerking van persoonsgegevens

Om de in de vorige paragraaf geschetste beperkingen op te lossen wordt een nieuw hoofdstuk 5a aan de Wdo toegevoegd, getiteld Meldpunt Fouten in Overheidsregistraties en Centraal Meldpunt Identiteitsfraude (voorgestelde artikelen 16a en 16b), waarmee solide wettelijke grondslagen voor de gegevensverwerking worden gecreëerd, conform de vereisten in de AVG en in het nationale recht.

In het nieuwe hoofdstuk wordt geregeld dat de Minister van BZK zorg draagt voor de inrichting van het MFO en CMI. Bij het MFO kan melding worden gedaan over onjuiste gegevens in overheidsregistraties en het gebruik van de gegevens. Dit omvat registraties die worden gebruikt voor het uitvoeren van een publieke taak, waaronder basisregistraties²⁵. Bij het CMI kan melding worden gedaan van vermoedens van identiteitsfraude. De melding kan worden gedaan door of namens degene op wie de onjuiste gegevens of de identiteitsfraude betrekking heeft dan wel een organisatie met een publieke taak. Medewerkers van een organisatie met een publieke taak doen in verschillende situaties melding bij het CMI of het MFO. Bijvoorbeeld als een medewerker meerdere betrokken burgers met hetzelfde probleem ziet. Een medewerker van een gemeente heeft melding gedaan bij het MFO, toen meerdere burgers kort na elkaar bij hem meldden dat zij dezelfde brief van Dienst Toeslagen hadden ontvangen, waarin – naar hun mening ten onrechte – stond dat zij geen recht meer hadden op een bepaalde toeslag. Deze medewerker heeft hierover contact opgenomen met het MFO, dat vervolgens contact zocht met Dienst Toeslagen. Uiteindelijk bleek dat Dienst Toeslagen een bericht van een gemeentelijke herindeling niet goed had verwerkt, waardoor een deel van de bewoners van een gemeente in de administratie van Dienst Toeslagen ten onrechte als verhuisd stond geregistreerd. Dit had tot gevolg dat het recht van de betrokkenen op een toeslag automatisch veranderde. Medewerkers van een organisatie met een publieke taak doen ook melding bij het CMI of het MFO als een burger een fout in een overheidsregistratie of een vermoeden van identiteitsfraude bij hen meldt en de betreffende medewerker de indruk heeft dat die burger onvoldoende zelfredzaam of digitaal vaardig is om zelf een melding te doen bij het CMI of het MFO. De medewerker doet die melding vanuit het oogpunt van dienstverlening, met als doel deze burgers toch toegang te geven tot de juiste ondersteuning. Het inhoudelijke contact over de melding verloopt hierna meestal rechtstreeks met betrokkene.

Voorgesteld wordt de volgende taken voor het MFO in de wet vast te leggen:

- a. het beoordelen van meldingen van het vermoeden van verwerking van onjuiste gegevens in overheidsregistraties en het naar aanleiding van een melding coördineren van het proces van het herstel van onjuiste gegevens in overheidsregistraties en de gevolgen daarvan, in het bijzonder het uitwisselen van persoonsgegevens met de verwerkingsverantwoordelijke van de betrokken overheidsregistratie met het oog op herstel van onjuiste gegevens;
- b. het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft;
- c. het analyseren van meldingen in verband met ontwikkelingen omtrent fouten in overheidsregistraties, het bijhouden van statistische beleidsinformatie en het in geanonimiseerde vorm delen hiervan met derden.

De voorgestelde wettelijke taken van het CMI zijn:

- a. het beoordelen van een melding van het vermoeden van identiteitsfraude en het naar aanleiding van een melding coördineren van het proces van het herstel van identiteitsfraude en de gevolgen hiervan, in het bijzonder het uitwisselen van persoonsgegevens over de identiteitsfraude met de verwerkingsverantwoordelijke van de betrokken organisatie;
- b. het begeleiden, adviseren en ondersteunen van degene op wie de melding van identiteitsfraude betrekking heeft;
- c. het analyseren van meldingen in verband met ontwikkelingen omtrent identiteitsfraude, het bijhouden van statistische beleidsinformatie, en het in geanonimiseerde vorm delen hiervan met derden;
- d. het adviseren van organisaties over identiteitsfraude;
- e. het bijdragen aan de publieke bewustwording over identiteitsfraude;

²⁵ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/>

f. het adviseren over de ontwikkeling van applicaties om identiteitsfraude te voorkomen of te stoppen.

Deze taakbepalingen vormen de grondslag voor de rechtmatige verwerking van persoonsgegevens als bedoeld in artikel 6, eerste lid, onderdeel e, van de AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Met deze nieuwe taakbepalingen wordt verzekerd dat de meldpunten het BSN kunnen verwerken ingevolge artikel 10 van de Wabb, voor zover dit noodzakelijk is voor hun taakuitvoering. Verder kunnen de meldpunten op basis van de taakbepalingen op grond van de artikelen 3.2 Wet BRP en 37 en 38 van het Besluit BRP een autorisatie voor het gebruik van BRP-gegevens aanvragen, voor zover deze gegevens noodzakelijk zijn voor een goede vervulling van hun taak.

De wettelijke regeling bevat grondslagen voor de verwerking van gegevens over gezondheid en persoonsgegevens van strafrechtelijke aard door zowel het MFO als het CMI. Deze gegevensverwerking is mogelijk voor zover dit noodzakelijk is voor de uitoefening van de wettelijke taken die betrekking hebben op de behandeling van meldingen en het proces van herstel van onjuiste gegevens of identiteitsfraude en de gevolgen daarvan en het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft. Voor taken als het geven van voorlichting mogen geen gegevens over gezondheid of persoonsgegevens van strafrechtelijke aard worden verwerkt.

Waar het de verwerking van gegevens over gezondheid betreft wordt afgeweken van het in artikel 9, tweede lid, AVG opgenomen verbod op de verwerking van bijzondere persoonsgegevens, vanwege redenen van een zwaarwegend algemeen belang. Dit belang is gelegen in het (primair op initiatief van betrokkene) achterhalen van onjuiste registratie van diens persoonsgegevens in overheidsregistraties en de correctie ervan. Dit belang en doel ligt bovendien in het verlengde van het beginsel (en verplichting) van 'juistheid' van persoonsgegevens in de zin van de AVG: persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

De grondslag voor de verwerking van persoonsgegevens van strafrechtelijke aard past binnen het kader van artikel 10 AVG, dat voorschrijft dat de verwerking is toegestaan bij lidstatelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Op de verhouding met het hoger recht wordt in hoofdstuk 3 van deze memorie van toelichting ingegaan.

Tot slot bevat de wettelijke regeling grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de gegevensverwerking door de meldpunten, waaronder passende waarborgen. Bij ministeriële regeling kunnen regels worden gesteld over de wijze waarop de melding kan worden gedaan en over de procedure voor de behandeling van de melding.

2.2 Aanpassing regeling toezicht op de naleving

Dit wetsvoorstel past de regeling van het toezicht op de naleving op de Wdo aan om beter aan te sluiten bij het stelsel van interbestuurlijk toezicht. Bij brief van 23 september 2022 zijn beide Kamers over deze wijziging geïnformeerd.²⁶ De huidige toezichtbepalingsbepaling in artikel 17 van de Wdo is niet eenduidig. Volgens de memorie van toelichting bij de Wdo is het de bedoeling dat voor de bestuursorganen van provincies en gemeenten het gewone generieke interbestuurlijke toezicht geldt van de Provinciewet en de Gemeentewet.²⁷ Het specifieke toezicht in artikel 17, tweede en derde lid, van de Wdo is bedoeld voor waterschappen en bijvoorbeeld gemeenschappelijke regelingen waaraan provincies en gemeenten deelnemen. Dit blijkt echter niet zonder meer uit de huidige toezichtsbepaling, die zich ook uitstrekt tot provincies en gemeenten. Voor gemeenschappelijke regelingen waaraan bestuursorganen van provincies en gemeenten

²⁶ Zie ook Kamerstukken II 2022/23, 35868, nr. 16 en Kamerstukken II 2021/22, 35868, nr. 6.

²⁷ Kamerstukken II 2017/18, 34972, nr. 3, p. 86.

deelnemen, biedt de Wet gemeenschappelijke regelingen geldt reeds een generiek interbestuurlijk toezichtkader dat in lijn is met dat van de Provinciewet en de Gemeentewet. Specifiek toezicht in de Wdo voor dergelijke regelingen is daarom niet nodig voor deze gemeenschappelijke regelingen. Specifiek toezicht is wel nodig voor de waterschappen en voor gemeenschappelijke regelingen waaraan geen bevoegdheden van de besturen van provincies en gemeenten zijn overgedragen, omdat voor die organen het huidige toezichtkader van de Waterschapswet en de Wet gemeenschappelijke regelingen te afwijkend is van dat van de Provinciewet en Gemeentewet. Dit houdt ermee verband dat de gronden voor het uitoefenen van de bijzondere toezichtsbevoegdheden in eerstgenoemde wetten beperkter zijn en niet is voorzien in de mogelijkheid om (uiteindelijk) op rijksniveau toezichtsbevoegdheden te kunnen inzetten. Via een wijziging van artikel 17 van de Wdo wordt in dit wetsvoorstel verduidelijkt dat uitsluitend een apart toezichtsregime op grond van de Wdo geldt voor waterschappen en gemeenschappelijke regelingen waaraan geen bevoegdheden van de besturen van provincies en gemeenten zijn overgedragen. Toezicht op de naleving vindt plaats door ambtenaren die zijn aangewezen door de Minister van BZK. Verder wordt de Wdo in dit wetsvoorstel toegevoegd aan bijlage I, bedoeld in artikel 124b, eerste lid, van de Gemeentewet. Dat leidt ertoe dat de toezichtsbevoegdheden die in de artikelen 124, 124c, 124d en 124f van de Gemeentewet aan gedeputeerde staten of de commissaris van de Koning zijn toegekend (taakverwaarlozing, indeplaatsstelling) worden uitgeoefend door de minister van BZK. Daar is aanleiding toe, omdat gedeputeerde staten op het terrein van de Wdo geen taken heeft en daarom inhoudelijke expertise mist.

2.3 Wijziging van de technische instructies of opties voor het configureren van een reeds aangewezen standaard bij ministeriële regeling

Dit wetsvoorstel vereenvoudigt de regeling in de Wdo voor het wijzigen van de technische instructies of opties voor het configureren van een reeds aangewezen standaard. Op grond van artikel 3 van de Wdo zijn de in die bepaling genoemde organisaties verplicht tot de toepassing van de ingevolge het tweede lid aangewezen standaarden. Standaarden zijn afspraken over bijvoorbeeld elektronische gegevensuitwisseling, toegankelijkheid of beveiliging, vastgelegd in zogeheten specificatiedocumenten, die beschrijven hoe gegevens eruitzien, wat ze betekenen en hoe ze kunnen worden uitgewisseld. Aldus wordt het mogelijk om op efficiënte, veilige en betrouwbare wijze (administratieve) processen geautomatiseerd af te wikkelen en onafhankelijkheid van ICT-systeemleveranciers te bewerkstelligen.²⁸ Daarbij dient ook het toepassingsbereik worden omschreven, zoals voor welke organen de standaard toepasselijk is, in welke gevallen en vanaf welk moment.

Volgens de huidige Wdo kan het wijzigen van standaarden enkel bij algemene maatregel van bestuur. De praktijk wijst uit dat hiermee niet snel genoeg opvolging gegeven kan worden aan technische ontwikkelingen. Het wordt wenselijk geacht om technische instructies of opties voor het configureren van het gebruik van een al verplichte standaard voor overheidsinstanties eenvoudiger te kunnen wijzigen. Daarom voegt het wetsvoorstel een grondslag toe voor regeling van de technische instructies of opties voor het configureren van een reeds aangewezen standaard bij ministeriële regeling. Hierbij kan worden gedacht aan het aanpassen van de versie van de ICT-beveiligingsrichtlijnen waaraan een beveiligingsprotocol als Transport Layer Security moet voldoen.²⁹ Voor een nieuwe standaard of een substantiële wijziging van een al aangewezen standaard blijft gelden dat deze bij algemene maatregel van bestuur wordt aangewezen.

3. Verhouding tot hoger recht

Dit wetsvoorstel voorziet onder meer in een rechtsgrondslag voor de verwerking persoonsgegevens door het MFO en het CMI. De verwerking van persoonsgegevens betekent een inmenging in grondrechten van burgers en moet in overeenstemming zijn met geldend recht dat deze grondrechten beschermt. In dit hoofdstuk wordt de voorgestelde gegevensverwerking getoetst aan achtereenvolgens artikel 10 van de Grondwet, artikel 8 van het Europees Verdrag tot bescherming

²⁸ Kamerstukken II 2017/18, 34972, nr. 3, p. 59-60.

²⁹ Zie het Besluit beveiligde verbinding met overheidswebsites en- webapplicaties.

van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM), artikel 8 EU-Handvest en de AVG.

3.1 Artikel 10 van de Grondwet

Het verwerken van persoonsgegevens door het MFO en het CMI vormt een inbreuk op het recht op privacy, dat wordt beschermd door artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Een inmenging op dit recht kan gerechtvaardigd zijn indien wordt voldaan aan drie voorwaarden.

Artikel 10, eerste lid, van de Grondwet bepaalt dat eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. Het recht op eerbiediging van de persoonlijke levenssfeer is daarmee niet absoluut. Een inperking daarop is toegestaan, mits dit bij of krachtens een wet in formele zin gebeurt. De verwerkingen van persoonsgegevens door het MFO en het CMI vormen een beperking van genoemd grondrecht. De grondslag voor deze beperking is opgenomen in dit voorstel van formele wet, zodat voldaan is aan de eis die de Grondwet stelt. De noodzaak voor de beperking zal bij de bespreking van artikel 8 van het EVRM aan de orde komen. Artikel 10, tweede en derde lid, van de Grondwet bepalen voorts dat de wet regels dient te stellen ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op de verbetering van zodanige gegevens. Hierin wordt voor dit voorstel voorzien door de AVG en de UAVG.

3.2 Artikel 8 van het EVRM

Op grond van artikel 8, eerste lid, van het EVRM heeft eenieder recht op eerbiediging van de persoonlijke levenssfeer. Onder artikel 8, eerste lid, van het EVRM valt onder andere de verwerking van persoonsgegevens als onderdeel van het recht op eerbiediging van het privéleven. Dit recht mag alleen worden beperkt als is voldaan aan de vereisten voor beperking neergelegd in artikel 8, tweede lid, van het EVRM: de beperking van dit recht moet bij wet zijn voorzien en noodzakelijk zijn in een democratische samenleving in het belang van een of meer legitieme doelen: het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of de bescherming van de rechten en vrijheden van anderen.

Allereerst dient de inmenging bij wet voorzien te zijn. Hieraan is voldaan. In dit wetsvoorstel zijn de regels opgenomen die een grondslag vormen voor verwerking van persoonsgegevens (voorgestelde artikelen 16a en 16b van de Wdo). Geregeld wordt voor welke taak persoonsgegevens kunnen worden verwerkt door de meldpunten en onder welke voorwaarden gegevens over gezondheid en persoonsgegevens van strafrechtelijke aard mogen worden verwerkt. Voldaan is eveneens aan de eis dat de wet voldoende toegankelijk en voorzienbaar moet zijn. De toegankelijkheid van dit wetsvoorstel wordt gewaarborgd, doordat het voorstel, indien het tot wet zal worden verheven, in het Staatsblad wordt gepubliceerd. Daarnaast dient de wet voldoende specifiek te zijn, zodat de burger kan opmaken welke persoonsgegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewaard en verwerkt.³⁰ Met dit wetsvoorstel wordt voorzien in een duidelijk wettelijk kader met betrekking tot de taken waarvoor de meldpunten persoonsgegevens mogen verwerken. De nadere uitwerking van de gegevensverwerking vindt plaats op het niveau van een algemene maatregel van bestuur, hiervoor biedt de wet een grondslag.

De inmenging moet voorts noodzakelijk zijn in het belang van een legitiem doel, genoemd in artikel 8, tweede lid, van het EVRM. Het MFO en CMI verwerken persoonsgegevens voor – kort samengevat – de behandeling van meldingen over vermoedens van onjuiste gegevens in overheidsregistraties en het gebruik van die gegevens en vermoeden van identiteitsfraude en de gevolgen hiervan, en ten behoeve van het coördineren van het proces tot het herstel van fouten in

³⁰ Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:288, overweging 2.3.2.

gegevensregistraties en het herstel van gevolgen van identiteitsfraude, waaronder in kennis stellen van betrokken organisaties. Voor een uitgebreide taakomschrijving wordt verwezen naar paragraaf 2.1.3 van deze memorie van toelichting. Door de uitvoering van deze taken worden de rechten en vrijheden van burgers die te maken hebben onjuistheden in overheidsregistraties en identiteitsfraude beschermd. Daarmee is sprake van een legitiem doel.

Om aan het noodzakelijkheidsvereiste van artikel 8 EVRM te voldoen, moet verder sprake zijn van een dringende maatschappelijke behoefte (*pressing social need*), waarbij de te nemen maatregelen moeten voldoen aan de vereisten van proportionaliteit en subsidiariteit. Hierbij is sprake van een zekere beoordelingsruimte van de Staat (*margin of appreciation*). Voor een uitwerking van de dringende maatschappelijke behoefte wordt kortheidshalve verwezen naar de paragrafen 2.1.1 en 2.1.2 van deze memorie van toelichting. Daar is ingegaan op de huidige werkwijze van de meldpunten en de knelpunten met betrekking tot de gegevensverwerking. Hierdoor worden problemen van burgers niet altijd toereikend opgelost, wat grote gevolgen kan hebben. De proportionaliteitstoets behelst de vraag of het doel van de gegevensverwerking in redelijke verhouding staat tot de inmenging in de persoonlijke levenssfeer. Dat is het geval. Het gaat hier om de belangenafweging tussen enerzijds het recht van de burger om zijn persoonsgegevens niet verwerkt te zien worden door het MFO en CMI en anderzijds het belang van het bieden van hulp bij het herstellen van een onjuist gegeven in een overheidsregistratie en het gebruik daarvan en de gevolgen van identiteitsfraude. Daarmee wordt het belang van de burger gediend. Bovendien is van belang dat het onderzoek door de meldpunten (met verwerking van persoonsgegevens) primair op initiatief van de burger wordt gestart. Wat betreft de subsidiariteit kan het beoogde doel niet even doeltreffend worden bereikt op een andere wijze die de grondrechten van de betrokkenen minder aantast.

3.3 EU-Handvest en AVG

In artikel 7 van het Handvest van de grondrechten van de Europese Unie (EU-Handvest) is het recht op eerbiediging van het privéleven opgenomen. In artikel 8 van het EU-Handvest is het recht vastgelegd van eenieder op bescherming van persoonsgegevens. Artikel 16, tweede lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU) bevat een rechtsgrondslag voor het stellen van voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Deze opdracht is uitgevoerd via de AVG. De AVG vormt een nadere uitwerking van artikel 8 van het EU-Handvest en het VWEU. De voorwaarden die de AVG aan de gegevensverwerking stelt, komen deels overeen met de eisen die de Grondwet en het EVRM stellen.

De AVG is van toepassing op de verwerking van persoonsgegevens door het MFO en het CMI in het kader van de behandeling van de meldingen over vermoedens van onjuiste gegevens in overheidsregistraties en het gebruik van die gegevens en vermoedens van identiteitsfraude en de gevolgen hiervan, en ten behoeve van het coördineren van het proces tot het herstel hiervan, waaronder in kennis stellen van betrokken organisaties. Het doel van en de middelen voor de verwerkingen door het CMI en het MFO worden bepaald door de Minister van BZK, die verwerkingsverantwoordelijke is in de zin van de AVG.

In deze paragraaf wordt achtereenvolgens ingegaan op de toetsing aan de AVG-beginselen (artikel 5, eerste lid, AVG), de verwerking van gegevens over gezondheid (artikel 9 AVG), de verwerking van persoonsgegevens van strafrechtelijke aard (artikel 10 AVG) en de gegevensbeschermingseffectbeoordeling (DPIA) (artikel 35 AVG). Volledigheidshalve wordt opgemerkt dat dit wetsvoorstel geen regeling bevat met betrekking tot geautomatiseerde besluitvorming (artikel 22 AVG).

AVG-beginselen

Op grond van artikel 5 van de AVG dient de gegevensverwerking te voldoen aan de beginselen van rechtmatigheid, behoorlijkheid en transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. Het MFO en het CMI zijn namens de Minister van

BZK verantwoordelijk voor de naleving van deze beginselen en het aantonen daarvan („verantwoordingsplicht“).“

Rechtmatigheid, behoorlijkheid en transparantie

Wat betreft de rechtmatigheid wordt opgemerkt dat de taakbepalingen in de voorgestelde artikelen 16a en 16b van de Wdo voor beide meldpunten de rechtsgrondslag vormen voor de verwerking van persoonsgegevens als bedoeld in artikel 5, eerste lid, onderdeel a en 6, eerste lid, onderdeel e, van de AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. De rechtsgrondslag en daarmee de rechtmatigheid van de verwerking van persoonsgegevens die melder in het kader van de melding verstrekt, waaronder gegevens over gezondheid en persoonsgegevens van strafrechtelijke aard, is gegeven in de voorgestelde artikelen 16a en 16b van de Wdo. De noodzaak, proportionaliteit en subsidiariteit van de gegevensverwerking zijn hiervoor besproken in paragraaf 3.2.

Voorts dient de gegevensverwerking behoorlijk te zijn. Dat betekent dat de gegevensverwerking niet onverwacht of misleidend mag zijn voor de betrokkenen. Zoals hiervoor ten aanzien van het criterium ‘voorzienbaarheid’ van artikel 8 EVRM is aangegeven, is het voor betrokkene duidelijk welke gegevens worden gebruikt voor welk doel.

Het beginsel van transparantie houdt kort gezegd in dat voor betrokkenen inzichtelijk moet zijn hoe en waarom hun persoonsgegevens verwerkt worden. Wat betreft de rechten van de betrokkene gelden de rechten uit hoofdstuk 3 van de AVG en de UAVG. Op grond van de artikelen 13 en 14 AVG dienen de meldpunten de betrokkene actief te informeren en transparant te zijn over de gegevens die zij over hen hebben verwerkt en hen te wijzen op het bestaan van klacht-, bezwaar en beroepsmogelijkheden. Dat geldt ook als de melding niet door de betrokkene zelf maar door een derde is gedaan. Betrokkenen hebben op grond van de artikelen 15 tot en met 22 van de AVG verschillende rechten, zoals het recht op inzage, het recht op rectificatie en het recht om persoonsgegevens te wissen. De meldpunten kunnen alleen besluiten een verzoek te weigeren als niet voldaan is aan de voorwaarden voor een verzoek of als er sprake is van een uitzondering als bedoeld in de AVG. Deze uitzonderingen zijn uitgewerkt in artikel 41 UAVG. Er moet altijd een expliciete afweging plaatsvinden of het belang van de (tijdelijke) inperking van de rechten van betrokkene opweegt tegen de inbreuk op de rechten en vrijheden van de betrokkene.

RvIG heeft op haar website ten behoeve van de meldpunten een privacyverklaring gepubliceerd over het verwerken van persoonsgegevens door het CMI en het MFO. In die privacyverklaring geeft RvIG inzicht in welke gegevens de meldpunten verwerken, voor welk doel zij die verwerken en hoe zij dat doen. RvIG geeft in deze verklaring ook informatie over de rechten van de melder als het gaat om de verwerking van gegevens door de meldpunten: het recht op inzage, rectificatie, gegevenswissing, beperking, overdraagbaarheid en bezwaar.

Doelbinding

Het beginsel van doelbinding brengt mee dat de verwerking gebonden moet zijn aan specifieke verzameldoelen. Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Persoonsgegevens die reeds verzameld zijn voor een bepaald doel mogen alleen verder worden verwerkt voor andere doelen mits die doelen verenigbaar zijn met het oorspronkelijke verzameldoel. Aan het doelbindingsbeginsel wordt voldaan met de specifieke taakbepalingen voor de meldpunten in de artikelen 16a en 16b Wdo. De gegevensverwerking door het MFO en CMI blijft beperkt tot hetgeen voor de verwezenlijking van de hierin genoemde doelen noodzakelijk is.

Dataminimalisatie

Het beginsel van dataminimalisatie betekent dat de verwerking van persoonsgegevens toereikend dient te zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Met andere woorden: er mogen niet meer persoonsgegevens worden verwerkt

dan nodig zijn om het gestelde doel te behalen.

De behandeling van een melding door het MFO en het CMI start met (persoons)gegevens die door de melder via het meldingsformulier worden aangeleverd. Daarbij worden alleen gegevens uitgevraagd die noodzakelijk zijn voor het registreren, in behandeling nemen van de melding en voor het uitvoeren van de overige in het wetsvoorstel vastgelegde taken. De (persoons)gegevens die de melder in de vrije velden invult en die in de eventueel aangeleverde documenten staan, kunnen relevant zijn in de zoektocht naar wat er is gebeurd en naar een oplossing in het specifieke geval. Deze (persoons)gegevens worden niet actief uitgevraagd, maar kunnen wel door het MFO en CMI worden verwerkt. Daarbij wordt de gegevensverwerking zoveel mogelijk beperkt tot wat noodzakelijk is voor het herstelproces. Voor zover het nodig is voor de behandeling van de melding en het herstel van de onjuiste gegevens kan het MFO persoonsgegevens verstrekken aan betrokken (overheids)organisaties en het CMI aan betrokken organisaties, rechtspersonen en ondernemingen. Ook kunnen de meldpunten bij deze betrokken (overheids)organisaties gegevens opvragen voor de behandeling van de melding. Ook deze gegevensverwerking beperkt zich tot wat noodzakelijk is voor het herstel van een eventuele fout of identiteitsfraude.

Beide meldpunten hanteren specifieke waarborgen ter bescherming van de privacy van een melder of derde. Bij het maken van de webformulieren – waarin potentieel veel persoonsgegevens zouden kunnen worden opgenomen – is rekening gehouden met de vraag of alle gegevens nodig zijn voor de verwerking, of het doel van de verwerking in evenredige verhouding staat tot de inbreuk op de privacy (proportionaliteit) en of dit met minder ingrijpende middelen kan worden bereikt (subsidiariteit). Zo bevatten de meldingsformulieren van de beide meldpunten een zo beperkt mogelijk aantal vrije velden. Daarnaast bevat het meldingsformulier voor de melder de instructie om geen persoonsgegevens op te nemen die niet of nauwelijks met de melding te maken hebben en dus voor de beoordeling van de melding niet noodzakelijk zijn, en om terughoudend te zijn met het opnemen van persoonsgegevens van anderen.

Juistheid

Het beginsel van juistheid betekent dat de meldpunten ervoor moeten zorgen dat de gegevens juist zijn en deze moet actualiseren als dat nodig is. Voor het goed functioneren van het herstel van onjuiste gegevens en mutaties, is het van groot belang dat de gegevens die door de meldpunten bijgehouden worden correct zijn. De verwerking van het BSN en de inzage in de BRP-V dragen bij aan het eenduidig en efficiënt uitwisselen van persoonsgegevens waardoor de meldpunten kunnen beschikken over juiste en actuele gegevens van een melder.

Opslagbeperking

Het beginsel van opslagbeperking houdt in dat persoonsgegevens verwijderd dienen te worden door de meldpunten, zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld.

Het CMI bewaart de persoonsgegevens conform de selectielijst van BZK, gebaseerd op de voorschriften in de Archiefwet 1995 en het Archiefbesluit 1995, tien jaar.³¹ Het MFO-proces met bijbehorende bewaartermijn wordt opgenomen in de selectielijst van BZK. Conform de AVG bewaart het MFO persoonsgegevens thans niet langer dan noodzakelijk voor de afhandeling van de melding. Dat is in ieder geval niet langer dan een jaar nadat het MFO de behandeling van de melding heeft afgerond. Deze termijnen zijn gebaseerd op de ervaring die de meldpunten hebben met melders die na sluiting terugkomen voor een heropening van de behandeling van de melding en de termijn die daarvoor in de praktijk nodig is.

Het verschil met de bewaartermijn tussen het MFO en het CMI is verklaarbaar vanuit de noodzaak om gegevens die tot identiteitsfraude hebben geleid beschikbaar te houden, omdat de identiteitsfraude en de gevolgen daarvan zich over een langere periode kunnen uitstrekken. Als een fraudeur eenmaal beschikt over de identiteitsgegevens van de betrokkene dan kan die daar op verschillende momenten en op verschillende manieren fraude mee plegen. Ook kunnen de gevolgen van een al gepleegde vorm van fraude zich soms jaren later aan de betrokkene

³¹ https://www.nationaalarchief.nl/sites/default/files/field-file/Selectielijst_Ministerie_van_BZK_v1.0_vastgesteld.pdf, p. 43, Proces 10.6.10. Zie ook artikel 5 van de Archiefwet 1995 en artikel 5 van het Archiefbesluit 1995.

openbaren. In die situaties kan het CMI de betrokkene alleen verder helpen als het de gegevens van de melding over een langere periode bewaart. De registratie bij het CMI kan ook na een langere periode een bewijsfunctie vervullen voor de melder.

Het MFO bewaart de overige – niet tot een persoon herleidbare – gegevens in de melding maximaal tien jaar. Om aan het inzagerecht te kunnen voldoen zijn de volgende bewaartermijnen voor het MFO vastgesteld: alle binnengekomen meldingen, inclusief alle stukken en correspondentie daaromtrent een jaar, en voor de geanonimiseerde gegevens ten behoeve van de beleidsadviezen tien jaar. Als een melder wil dat zijn gegevens (eerder) verwijderd worden, kan die daartoe op ieder moment een verzoek indienen bij het MFO of het CMI. Een daartoe strekkend verzoek zal op de voet van artikel 17 van de AVG in behandeling worden genomen.

Integriteit en vertrouwelijkheid

Ingevolge artikel 5, eerste lid, onder f, van de AVG moeten de meldpunten passende technische en organisatorische maatregelen nemen, zodat een passende beveiliging van de persoonsgegevens gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De verwerkingsverantwoordelijke moet de inherente risico's beoordelen en passende maatregelen treffen, zoals bijvoorbeeld versleuteling. Het verantwoord omgaan met persoonsgegevens valt of staat met goede beveiliging van de gegevens.

Bij de beoordeling van de gegevensbeveiligingsrisico's is aandacht besteed aan risico's die zich kunnen voordoen, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de gegevens. Hierbij wordt door het CMI en het MFO aansluiting gezocht bij de voor de Rijksoverheid ter zake geldende regels, zoals onder andere de Baseline Informatiebeveiliging Overheid (BIO).

Voor de registratie van de gegevens die de melder in een meldingsformulier heeft ingevuld, gebruiken de meldpunten een beveiligd Enterprise Service Management (ESM) platform dat voor servicemanagement als ticketsysteem in gebruik is binnen RvIG.

Voor het communiceren met overheidsorganisaties maakt men gebruik van telefoon en/of e-mail, waarbij geldt dat persoonsgegevens altijd via een veilige verbinding (bijvoorbeeld Zivver of Securetransfer) worden verzonden. De meldpunten werken dus vanuit een beveiligde omgeving die enkel beschikbaar is voor de daartoe bevoegde medewerkers. Dat houdt in dat alleen daartoe geautoriseerde medewerkers van RvIG toegang hebben tot een melding en bijbehorende persoonsgegevens. Autorisaties worden verleend aan medewerkers op 'need to know' basis: alleen medewerkers die toegang tot de omgeving nodig hebben voor het uitvoeren van hun werkzaamheden ten behoeve van de taken van het CMI en het MFO krijgen de daarvoor relevante autorisaties. Deze medewerkers hebben een eed of belofte afgelegd waarbij zij een eed of belofte hebben afgelegd dat zij integer en zorgvuldig omgaan met informatie en vertrouwelijke informatie geheimhouden.

Samenvattend zijn volgende passende technische of organisatorische maatregelen in de zin van artikel 5, eerste lid, onder f, getroffen:

- De meldpunten instrueren de melder in het digitale meldingsformulier om alleen gegevens met de meldpunten te delen die van belang zijn voor de behandeling van de melding;
- De meldpunten vernietigen persoonsgegevens zoveel als mogelijk als blijkt dat die niet van belang zijn voor de behandeling van de melding;
- De meldpunten bewaren de gegevens in een beveiligde omgeving;
- De meldpunten beperken de toegang tot deze gegevens tot de medewerkers die een rol hebben bij de behandeling van MFO-meldingen en die daartoe geautoriseerd zijn;
- Voor deze medewerkers geldt als norm dat zij de gegevens alleen raadplegen als dat nodig is voor de behandeling van de betreffende melding en zij hebben een geheimhoudingsplicht;
- De meldpunten delen de gegevens van een melder alleen met andere partijen als dat nodig is voor de behandeling van de melding en maken daarbij gebruik van een beveiligde verbinding;
- De meldpunten gebruiken alleen gegevens die niet tot een persoon herleidbaar zijn voor het bijhouden van ontwikkelingen; RvIG publiceert een privacyverklaring waarin zij

informatie geeft over het gebruik van persoonsgegevens door het CMI en het MFO en over de rechten van de melder, zoals het recht op gegevenswissing.

Gegevens over gezondheid

Op grond van artikel 9, eerste lid, van de AVG is de verwerking van gegevens over gezondheid verboden. Verwerking van dergelijke gegevens is slechts toegestaan als deze kan worden geschaard onder een van de voorwaarden van artikel 9, tweede lid, van de AVG. Het tweede lid, onderdeel g, bepaalt dat het verbod om gegevens over gezondheid te verwerken niet van toepassing is als de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang en dit op grond van (Unierecht of) lidstatelijk recht wordt geregeld, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

Met dit wetsvoorstel (voorgestelde artikelen 16a en 16b, telkens vierde lid) wordt gebruik gemaakt van en invulling gegeven aan de uitzondering van artikel 9, tweede lid, onderdeel g, van de AVG om gegevens over gezondheid te verwerken. Hierbij gaat het om gegevensverwerking die noodzakelijk is voor de behandeling van meldingen in verband met onjuiste gegevens in overheidsregistraties en de doorwerking hiervan in andere overheidsregistraties of met identiteitsfraude en het proces van herstel hiervan. De mogelijkheid voor het MFO en het CMI om burgers op laagdrempelige wijze ondersteuning te bieden bij het herstel van fouten in overheidsregistraties of identiteitsfraude en de gevolgen hiervan dient een zwaarwegend algemeen belang. Dit zwaarwegend algemeen belang betreft het risico op verergering of escalatie van de problemen met mogelijk ernstige gevolgen voor de betrokkene en/of hoge maatschappelijke kosten. In paragraaf 2.1 is de noodzaak om gegevens over gezondheid te kunnen verwerken nader toegelicht. Van belang is dat de deze mogelijkheid niet ziet op alle taken van de meldpunten maar wettelijk wordt beperkt tot verwerkingen die noodzakelijke zijn voor het beoordelen van meldingen over onjuiste gegevens en identiteitsfraude en het herstelproces, respectievelijk het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft (voorgestelde artikelen 16a en 16b, derde lid, onderdelen a en b). Voor taken als publieksvoorlichting mogen deze gegevens niet worden verwerkt. Het verwerken van gegevens over gezondheid door het CMI en het MFO strekt dus niet verder dan het ontvangen ervan met het doel om de melding te onderzoeken en de gevolgen van fraude en/of fouten in overheidsregistraties te herstellen en de melder te adviseren. Het gaat niet om het verwerken van de gegevens voor gezondheidsdoeleinden. Daarmee wordt de evenredigheid van de verwerking met het nagestreefde doel (het herstel van onjuiste gegevens in overheidsregistraties respectievelijk identiteitsfraude en de gevolgen daarvan) gewaarborgd en de wezenlijke inhoud van het recht op bescherming van persoonsgegevens geëerbiedigd.

Persoonsgegevens van strafrechtelijke aard

Ten aanzien van de verwerking van persoonsgegevens van strafrechtelijke aard bepaalt artikel 10 van de AVG dat deze alleen mogen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkene bieden. Persoonsgegevens van strafrechtelijke aard zijn allereerst gegevens betreffende strafrechtelijke veroordelingen. Daarnaast zijn gegevens die een zwaardere verdenking dan een redelijk vermoeden van schuld aan een strafbaar feit opleveren óók gegevens van strafrechtelijke aard. Strafbare feiten zijn onder meer de gedragingen die in het Wetboek van Strafrecht zijn beschreven.

Met dit wetsvoorstel (voorgestelde artikelen 16a en 16b, vijfde lid) wordt voor het MFO en het CMI gebruik gemaakt van en invulling gegeven aan artikel 10 AVG om in een nationale wet de verwerking van persoonsgegevens van strafrechtelijke aard toe te staan. Hierbij gaat het om gegevensverwerking die noodzakelijk is voor de behandeling van meldingen in verband met fouten in overheidsregistraties en identiteitsfraude en de doorwerking hiervan in andere overheidsregistraties en het proces van herstel hiervan respectievelijk het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft (voorgestelde artikelen 16a en 16b, derde lid, onderdelen a en b). De meldingen die het CMI ontvangt kunnen betrekking hebben op

strafrechtelijke veroordelingen voor identiteitsfraude. Ook kunnen zij betrekking hebben op gegevens die een zwaardere verdenking dan een redelijk vermoeden van schuld aan een strafbaar feit opleveren. Wat betreft het MFO gaat het om het onderzoeken van meldingen die betrekking hebben op de registratie van een strafrechtelijk gegeven door overheidsorganisaties in de zogenaamde strafrechtketen. Door identiteitsfraude, een persoonsverwisseling, een verwerkingsfout of een technische fout kan een onjuist gegeven, zoals een veroordeling, bijvoorbeeld op iemands strafblad komen te staan. Dit is reeds toegelicht in paragraaf 2.1.2. Het wetsvoorstel bevat de nodige waarborgen ter bescherming van de grondrechten en fundamentele belangen van burgers.

Het wetsvoorstel biedt de mogelijkheid om bij of krachtens algemene maatregel van bestuur op grond van de voorgestelde artikelen 16a en 16b, telkens zesde lid, regels te stellen over passende waarborgen voor de gegevensverwerking door de meldpunten. Te denken valt aan de technische en organisatorische maatregelen ter beveiliging van de gegevens die het CMI en het MFO verwerken, verwerkingsactiviteiten en -procedures, waarborgen voor de toegang voor personeel tot (verwerkingsactiviteiten van) het CMI en het MFO en de wijze waarop het CMI en het MFO met de melder communiceren.

Gegevensbeschermingseffectbeoordeling (DPIA)

Er is een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd. Met de DPIA is de noodzaak onderzocht van de voorgenomen verwerking van persoonsgegevens en zijn op gestructureerde wijze de gevolgen en risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen van het onderhavige wetsvoorstel in kaart gebracht. De uitkomsten van de DPIA zijn, waar relevant, verwerkt in deze memorie van toelichting.

4. Uitvoering en gevolgen

4.1 Wettelijke regeling taken en gegevensverwerking MFO en CMI

De voorgestelde wettelijke regeling met betrekking tot de taken en gegevensverwerking van het MFO en het CMI in de Wdo leidt niet tot nieuwe taken voor de beide meldpunten en stelt geen nieuwe eisen aan burgers, bedrijven en professionals. Er treden daarmee geen extra regeldrukeffecten op als gevolg van het wetsvoorstel. De nieuwe wettelijke regeling zorgt wel voor een solide juridische grondslag voor de gegevensverwerking door het MFO en CMI. Door de voorgestelde grondslag voor gegevensverwerking neemt de slagkracht van de meldpunten toe en krijgen burgers, bedrijven en professionals naar verwachting betere ondersteuning bij het oplossen van hun problemen.

Burgers kunnen al op een laagdrempelige wijze een melding doen bij het MFO en het CMI over onjuiste gegevens in overheidsregistraties, het gebruik daarvan of over (het vermoeden van) identiteitsfraude. De nieuwe wettelijke regeling wijzigt dit niet. Het is belangrijk om burgers de mogelijkheid te bieden om zelf aan de bel te trekken als zij vermoeden dat hun gegevens niet kloppen of dat met hun gegevens gefraudeerd wordt. Daarvoor worden door middel van meldpunten ingangen geboden waar (gevolgen van) fouten of onjuistheden in overheidsregistraties of (gevolgen van) identiteitsfraude kunnen worden gemeld met het doel om de melder te helpen die zoveel mogelijk op te lossen. Een burger zal altijd eerst contact op moeten nemen met de organisatie die verantwoordelijk is voor de gegevens waarvan de burger vermoedt dat die niet kloppen. Indien een dergelijke melding voor de melder niet tot resultaat leidt, dan kunnen vanuit de meldpunten de noodzakelijke handelingen worden uitgevoerd gericht op het herstel van de gevolgen van identiteitsfraude of de gevolgen van het gebruik van onjuiste gegevens bij diverse overheidsorganisaties. De meldpunten vervullen hierin een coördinerende rol en hebben de procesregie over de melding. Voor de burger brengt dit mee dat hij niet zelf hoeft te achterhalen in welke registraties en bij welke organisaties het onjuiste gegeven of de fraude doorwerkt. De betreffende overheidsorganisatie heeft de verantwoordelijkheid om de problemen en de gevolgen daarvan voor de burger op te lossen.

4.2 Aanpassing regeling toezicht op de naleving

De wijziging van de regeling in artikel 17 van de Wdo inzake het toezicht op de naleving heeft geen gevolgen voor de uitvoering. Deze wijziging is slechts een verduidelijking van het toezicht zoals dat nu geregeld is.

4.3 Wijziging van de technische instructies of opties voor het configureren van een reeds aangewezen standaard bij ministeriële regeling

Het nieuwe artikel 3, vierde lid, zorgt voor een eenvoudiger procedure voor het wijzigen van de technische instructies of opties voor het configureren van een aangewezen standaard. Hierdoor kan sneller opvolging worden gegeven aan technische ontwikkelingen.

5. Toezicht en handhaving

Voor zover de bepalingen van dit wetsvoorstel de verwerking van persoonsgegevens betreffen, wordt hier toezicht op gehouden door de Autoriteit Persoonsgegevens.

6. Financiële gevolgen

Het wetsvoorstel brengt geen financiële gevolgen mee. Het MFO en CMI bestaan reeds en worden door het Ministerie van BZK gefinancierd. Dit wetsvoorstel heeft geen additionele financiële consequenties.

7. Evaluatie

PM

8. Advies en consultatie

PM AP (Privacy)

PM ATR (Regeldruk)

PM RvIG (uitvoeringstoets)

9. Overgangsrecht en inwerkingtreding

Bij het bepalen van de datum van inwerkingtreding van de wetswijzigingen (bij koninklijk besluit) zal rekening worden gehouden met het stelsel van vaste verandermomenten en minimuminvoeringstermijnen.

II. ARTIKELSGEWIJZE TOELICHTING

ARTIKEL I (Wijziging Wet digitale overheid)

Onderdeel A (wijziging artikel 1)

Dit onderdeel voegt een definitie van overheidsregistratie toe aan de begripsbepalingen in artikel 1 van de Wdo. Deze wijziging hangt samen met de wettelijke verankering van het MFO in artikelen 16a van de Wdo (zie onderdeel C). Onder overheidsregistratie wordt verstaan: registratie die wordt gebruikt voor het uitvoeren van een publieke taak. Daaronder vallen tien basisregistraties, met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken.³² Het betreft de Basisregistratie personen, Handelsregister, Basisregistratie Adressen en Gebouwen, Basisregistratie Topografie, Basisregistratie Kadaster, Basisregistratie Voertuigen (kentekenregister), Basisregistratie Inkomen, Basisregistratie Waarde Onroerende Zaken, Basisregistratie Grootschalige Topografie (voorheen GBKN), Basisregistratie Ondergrond. Daarnaast vallen onder de definitie registraties die worden gebruikt voor het uitvoeren van een publieke taak. Een publieke taak is een taak die krachtens publiekrecht in het algemeen belang of in het kader van de uitoefening van het openbaar gezag wordt uitgevoerd. Overheidsorganisaties zoals ministeries, gemeentes, agentschappen en zelfstandige bestuursorganen geven uitvoering aan een publieke taak. Rechtspersonen kunnen ook een publieke taak uitvoeren als die taak in de wet is vastgelegd. Deze rechtspersonen kunnen daarnaast ook andere (commerciële) taken verrichten. Een zorgverzekeraar verricht bijvoorbeeld een publieke taak bij de uitvoering van de Zorgverzekeringswet en een pensioenfonds bij de uitvoering van de taken uit de Pensioenwet. Een voorbeeld van een registratie die wordt gebruikt voor het uitvoeren van een publieke taak, is de verzekerdenadministratie die wordt gebruikt door de Sociale Verzekeringsbank (SVB).

Onderdeel B (wijziging artikel 3)

In artikel 3 van de Wdo wordt een nieuw vierde lid ingevoegd, op grond waarvan bij ministeriële regeling de technische instructies of opties voor het configureren van een aangewezen standaard gewijzigd kunnen worden. Deze wijziging maakt het mogelijk om wanneer er ontwikkelingen zijn in de techniek, die technische instructies of opties voor het configureren van het gebruik van een al verplichte standaard voor overheidsinstanties eenvoudiger te wijzigen. Voor een toelichting op de wijziging wordt verwezen naar het algemeen deel van de toelichting. De delegatie van regelgevende bevoegdheid op het niveau van een ministeriële regeling wordt in het nieuwe vierde lid beperkt tot uitwerking van de technische details en voorschriften die dikwijls wijziging behoeven en past daarmee in het toepasselijke kader in de Aanwijzingen voor de regelgeving (Ar 2.24). Het aanwijzen van een nieuwe standaard of een substantiële wijziging van een al aangewezen standaard blijft plaatsvinden bij algemene maatregel van bestuur (artikel 3., tweede en derde lid).

Onderdeel C (nieuw hoofdstuk 3A, artikelen 16a en 16b)

Met dit onderdeel wordt een nieuw hoofdstuk 3A in de Wdo ingevoegd, genaamd Meldpunt Fouten in Overheidsregistraties en Centraal Meldpunt Identiteitsfraude. Het hoofdstuk bevat twee artikelen die betrekking hebben op de taakuitoefening en gegevensverwerking door de meldpunten MFO en het CMI. Deze taakbepalingen vormen de grondslag voor de rechtmatige verwerking van persoonsgegevens als bedoeld in artikel 6, eerste lid, onderdeel e, van de AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Artikel 16a bepaalt dat de minister van BZK zorg draagt voor de inrichting van het MFO (eerste lid). De taken van MFO zijn ook in deze bepaling opgenomen (derde lid). In het algemeen deel van de toelichting is deze taakomschrijving toegelicht. Door of namens eenieder (daaronder alle vormen van vertegenwoordiging begrepen) kan bij het MFO melding worden gedaan van het

³² [10 basisregistraties Stelsel van basisregistraties - Digitale Overheid.](#)

vermoeden van verwerking van die persoon betreffende onjuiste gegevens in een overheidsregistratie en over het gebruik van die gegevens. De melding kan ook worden gedaan door een organisatie met een publieke taak (tweede lid). Het maatschappelijke belang van correcte gegevens in overheidsregistraties is in het laatstgenoemde geval ermee gediend dat de melding en afhandeling daarvan niet afhankelijk wordt gesteld van een melding door de betrokkene zelf. Het MFO kan een dergelijke melding in behandeling nemen, mits het de betrokkene op de hoogte stelt van de melding en de verwerking in de zin van artikel 14, eerste en tweede lid, van de AVG. De betrokkene heeft vervolgens de mogelijkheid om desgewenst op te komen tegen de verwerking van persoonsgegevens door het meldpunt.

Het vierde lid bevat een grondslag voor verwerking van gegevens over gezondheid door het MFO. Zoals in het algemeen deel van de toelichting is toegelicht is hiervoor op grond van artikel 9 van de AVG een wettelijke uitzondering op het verwerkingsverbod voor deze bijzondere categorie van persoonsgegevens vereist. De verwerking van gegevens over gezondheid is mogelijk zover dit noodzakelijk is voor de uitoefening van de wettelijke taken die betrekking hebben op de behandeling van meldingen en het proces herstel van onjuiste gegevens en de gevolgen daarvan en het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft (de uitvoering van de taken, bedoeld in artikel 16a, derde lid, onderdelen a en b).

Het vijfde lid creëert een grondslag voor de verwerking van persoonsgegevens van strafrechtelijke aard door het meldpunt conform artikel 10 van de AVG, indien de verwerking noodzakelijk is voor de uitvoering van de in het derde lid, onderdelen a en b, bedoelde taken.

Het zesde lid bevat een delegatiegrondslag voor het stellen van regels over de persoonsgegevens die worden verwerkt, waaronder het treffen van passende waarborgen voor de bescherming van persoonsgegevens. Deze regels kunnen worden toegevoegd aan het Besluit digitale overheid. Op grond van het zesde lid kunnen bij ministeriële regeling regels worden gesteld over wijze waarop een melding van een fout in een overheidsregistratie gedaan kan worden. Hierbij kan worden gedacht aan de locatie of website waar een melding gedaan kan worden. Ook kunnen bij ministeriële regeling regels worden gesteld over de procedure voor de behandeling van de melding, zoals de terugkoppeling aan de melder over het resultaat van de afhandeling van de melding.

Artikel 16b bepaalt dat de minister van BZK zorg draagt voor de inrichting het CMI (eerste lid). Door of namens eenieder die het betreft kan bij het CMI melding gedaan worden van het vermoeden van identiteitsfraude (tweede lid).

De taken van het CMI zijn opgenomen in het derde lid. Deze taakomschrijving is in het algemeen deel van de toelichting toegelicht. Het vierde lid bevat een grondslag voor verwerking van gegevens over gezondheid door het CMI. Zoals in het algemeen deel van de toelichting is toegelicht is hiervoor op grond van artikel 9 van de AVG een wettelijke uitzondering op het verwerkingsverbod voor bijzondere persoonsgegevens vereist. De verwerking van gegevens over gezondheid is mogelijk zover dit noodzakelijk is voor de uitoefening van de wettelijke taken bedoeld in artikel 16b, derde lid, onderdelen a en b. Dit zijn taken die betrekking hebben op de behandeling van meldingen en het proces herstel van onjuiste gegevens en de gevolgen daarvan en het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft. Het vijfde lid bevat een grondslag voor verwerking van persoonsgegevens van strafrechtelijke aard door het CMI. Zoals in het algemeen deel van de toelichting is toegelicht is hiervoor op grond van artikel 10 van de AVG een wettelijke grondslag in het nationale recht vereist. De verwerking van persoonsgegevens van strafrechtelijke aard is mogelijk voor zover dit – evenals bij het MFO – noodzakelijk is voor de uitoefening van de wettelijke taken van het CMI die betrekking hebben op de behandeling van meldingen van identiteitsfraude en de gevolgen daarvan en het begeleiden, adviseren en ondersteunen van degene op wie de melding betrekking heeft (de uitvoering van de taken, bedoeld in artikel 16b., derde lid, onderdelen a en b). Zoals ook in artikel 16a. geregeld, bevatten het zesde en zevende lid delegatiegrondslagen voor het stellen van regels over de verwerking van persoonsgegevens, waaronder het treffen van passende waarborgen voor de bescherming van persoonsgegevens (bij algemene maatregel van bestuur) en de behandeling van meldingen (bij ministeriële regeling).

Onderdeel D (wijziging artikel 17)

De wijziging van artikel 17 strekt tot aanpassing van de regeling van het toezicht op de naleving in de Wdo. In het algemeen deel van de toelichting is deze aanpassing toegelicht. Voorgesteld wordt

om, onder vernummering van het huidige vierde tot en met achtste lid, huidige derde lid van artikel 17 te laten vervallen en het tweede lid aan te passen. In het tweede lid (nieuw) wordt geregeld dat toezicht op de naleving van het bepaalde bij of krachtens de artikelen 3, 6, 7, 8, eerste lid, en 15 door de besturen van waterschappen en gemeenschappelijke regelingen waaraan geen bevoegdheden zijn overgedragen door de besturen van provincies of gemeenten plaatsvindt door de Minister van BZK aan te wijzen ambtenaren.

Daarmee wordt verduidelijkt dat er uitsluitend een apart toezichtsregime is voor waterschappen en voornoemde gemeenschappelijke regelingen. Verder wordt het toezicht op de naleving niet langer uitgeoefend door de provincies, maar door de Minister van BZK aan te wijzen ambtenaren. Met deze wijziging wordt tevens voor provincies en gemeenten buiten twijfel gesteld dat het generieke interbestuurlijk toezicht van toepassing is zoals dat geldt op grond van de Provinciewet en Gemeentewet.

Onderdeel E (wijziging artikel 28)

Deze wijziging is redactioneel van aard en hangt samen met een (aanstaande) wijziging van de citeertitel van het Tijdelijk Besluit digitale toegankelijkheid overheid (in Besluit digitale toegankelijkheid overheid).

ARTIKEL II (Wijziging bijlage I Gemeentewet)

In artikel II wordt voorgesteld om de Wdo te plaatsen op onderdeel A van Bijlage I. bedoeld in artikel 124b, eerste lid, van de Gemeentewet. Daarmee wordt bereikt dat de toezichtsbevoegdheden die in de artikelen 124, 124c, 124d en 124f aan gedeputeerde staten of de commissaris van de Koning zijn toegekend voor het interbestuurlijk toezicht op gemeenten, worden uitgeoefend door Onze Minister wie het aangaat. In dit geval is dat de minister van BZK. In het algemeen deel van de toelichting is deze wijziging toegelicht.

ARTIKEL III (Inwerkingtreding)

Bij het bepalen van de datum van inwerkingtreding (bij koninklijk besluit) zal rekening worden gehouden met het stelsel van vaste verandermomenten en minimuminvoeringstermijnen. Met het oog op een flexibele inwerkingtreding bepaalt de inwerkingtredingsbepaling dat de datum voor inwerkingtreding voor de verschillende artikelen of onderdelen verschillend kan worden vastgesteld.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,