Besluit van (...), houdende wijziging van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking

Op de voordracht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van … 2020, nr..../CZW/SB;
Gelet op de artikelen 4 en 16 van de Wet digitale overheid en artikel 20, derde lid, van de Bekendmakingswet;
De Afdeling advisering van de Raad van State gehoord (advies van.... 2020, nr WO...);
Gezien het nader rapport van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van.... 2020 nr …/CZW/SB;
Hebben goedgevonden en verstaan:

Artikel I

Het Besluit verwerking persoonsgegevens generieke digitale infrastructuur wordt als volgt gewijzigd:

A

Artikel 1 wordt als volgt gewijzigd:

1. Het opschrift komt te luiden:

Artikel 1. Begripsbepalingen

2. De definitie "afnemer van DigiD en DigiD Machtigen" komt te luiden:

afnemer van DigiD en DigiD Machtigen: een bestuursorgaan of aangewezen organisatie die in het kader van elektronische dienstverlening gebruik maakt van DigiD respectievelijk DigiD Machtigen;

3. Na de definitie van "afnemer van DigiD en DigiD Machtigen" worden twee definities ingevoegd, luidende:

afnemer van een erkende ontsluitende dienst: een bestuursorgaan of aangewezen organisatie die in het kader van elektronische dienstverlening gebruik maakt van een erkende ontsluitende dienst, bedoeld in artikel 9, derde lid, van de wet, of artikel 13, derde lid, van de wet;

afnemer van de routeringsvoorziening: een bestuursorgaan of aangewezen organisatie die toegang wil verlenen tot elektronische diensten door middel van een toegelaten of erkend identificatiemiddel of door middel van machtiging;

4. Na de definitie van "afnemer van MijnOverheid" wordt een definitie ingevoegd, luidende:

beschikbaarheid: de mate waarin een informatiesysteem in bedrijf en toegankelijk is op het moment dat een organisatie het nodig heeft;

5. De definitie "authenticatie" vervalt.

6. De definitie "BSN-Koppelregister" komt te luiden:

BSN-Koppelregister: de voorziening, bedoeld in artikel 5, eerste lid, onder d, van de wet;

7. De definitie "DigiD" komt te luiden:

DigiD: de voorziening voor uitgifte of activatie van publieke identificatiemiddelen, waarbij onderscheiden kan worden in meerdere betrouwbaarheidsniveaus, en authenticatie;

8. Na de definitie van "DigiD Machtigen" worden twee definities ingevoegd, luidende:

eIDAS-voorziening: de voorziening, bedoeld in artikel 5, tweede lid, van de wet;

gebruiker van een bedrijfs- en organisatiemiddel: een onderneming of rechtspersoon als bedoeld in artikel 5 onderscheidenlijk 6 van de Handelsregisterwet 2007 of een op grond van artikel 8, aanhef en onderdeel a, van die wet aangewezen rechtspersoon, of een natuurlijke persoon die deze onderneming of rechtspersoon vertegenwoordigt, die een erkend bedrijfs- en organisatiemiddel heeft aangevraagd of de aanvraagprocedure voor dat middel heeft voltooid;

9. Na de definitie van "gemachtigde in MijnOverheid" worden drie definities ingevoegd, luidende:

informatiebeveiliging/informatieveiligheid: het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking en informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen, gericht op de toegang tot elektronische dienstverlening;

informatiesysteem: het geheel van gegevensverzamelingen, de daarbij behorende personen, procedures, processen en programmatuur alsmede de getroffen voorzieningen voor opslag, verwerking en communicatie ten behoeve van elektronische dienstverlening, waaronder de mobiele applicaties als onderdeel van elektronische dienstverlening;

integriteit/betrouwbaarheid: de mate waarin een organisatie zich voor zijn bedrijfs- en bestuursprocessen kan verlaten op zijn informatievoorziening;

10. De definitie "MijnOverheid" komt te luiden:

MijnOverheid: de voorziening die bereikbaar is via het webadres mijn.overheid.nl voor de dienst voor elektronisch berichtenverkeer de Berichtenbox, en de diensten voor informatieverschaffing Lopende Zaken, Persoonlijke gegevens en Algemene bekendmakingen, kennisgevingen en mededelingen;

11. De definitie "notificatie" komt te luiden:

notificatie: een attendering die met een e-mailbericht of via een ander kanaal aan de gebruiker van DigiD, DigiD Machtigen of MijnOverheid wordt verstuurd, teneinde hem te informeren over een bericht of wijziging;

12. Na de definitie van "persoonsgegevens" worden twee definities ingevoegd, luidende:

risicomanagement: het inzichtelijk en systematisch inventariseren, beoordelen en - door het treffen van maatregelen - beheersbaar maken van risico's en kansen op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes;

routeringsvoorziening: de voorziening, bedoeld in artikel 5, eerste lid, onder c, van de wet;

13. Onder vervanging van de punt door een puntkomma aan het einde van de definitie "vertegenwoordigde in mijn overheid", worden de volgende definities toegevoegd:

vertrouwelijkheid: de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden;

wet: de Wet digitale overheid.

B

Artikel 2 wordt als volgt gewijzigd:

1. In onderdeel c, onder 2°, wordt na "burgerservicenummer" ingevoegd "of een versleutelde of afgeleide vorm daarvan ter identificatie van de gebruiker van DigiD" en wordt "en gegevens met betrekking tot het paspoort of de identiteitskaart, zoals de geldigheidsdata" vervangen door "gegevens met betrekking tot het paspoort of de identiteitskaart, zoals de geldigheidsdata, en gegevens met betrekking tot het rijbewijs, zoals het documentnummer en de geldigheidsdata".

2. In onderdeel c, onder 3°, wordt "het versleutelde wachtwoord" vervangen door "een afgeleide vorm van het wachtwoord, een afgeleide vorm van de pincode" en wordt "het mobiele telefoonnummer" vervangen door "het mobiele of vaste telefoonnummer, de gekozen documentsoort voor elektronische

identificatie, het soort apparaat waarmee op elektronische wijze gecommuniceerd kan worden met het Nederlands paspoort, de Nederlandse identiteitskaart of het Nederlands rijbewijs, de status en het betrouwbaarheidsniveau van het identificatiemiddel".

3. In onderdeel c, onder 4°, wordt na "kenmerken van het gebruik" ingevoegd ", waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm".

4. In onderdeel c, onder 6°, wordt "ondersteuning van de gebruiker" vervangen door "ondersteuning van de gebruiker of de administratie van DigiD".

5. Aan onderdeel c worden drie subonderdelen toegevoegd, luidende:

7°. gegevens afkomstig van de chip van het Nederlandse paspoort of de Nederlandse identiteitskaart waarmee de gebruiker van DigiD heeft ingelogd ter authenticatie:

- documentcode van het paspoort of de identiteitskaart;
- uitgevende staat of organisatie van het paspoort of de identiteitskaart;
- naam van de houder;
- documentnummer van het paspoort of de identiteitskaart;
- nationaliteit van de houder;
- geboortedatum van de houder;
- geslacht van de houder;
- geldigheidsdata van het paspoort of de identiteitskaart;
- burgerservicenummer.

8°. gegevens afkomstig van de chip van het Nederlandse rijbewijs waarmee de gebruiker van DigiD heeft ingelogd ter authenticatie:

- documentcode van het rijbewijs;
- documentnummer van het rijbewijs.

9°. gegevens genoemd in artikel 5d die noodzakelijk zijn voor de elektronische identificatie ter zake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eIDAS-voorziening.

6. Er wordt een onderdeel toegevoegd, luidende:
d. over afnemers van DigiD: administratieve gegevens noodzakelijk in verband met het gebruik door de afnemer van DigiD, waaronder de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van DigiD en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

C

Artikel 3 wordt als volgt gewijzigd:

1. In onderdeel b, onder 1°, wordt "de datum van overlijden" vervangen door "de reden voor de opschorting van de persoonslijst in de basisregistratie personen".

2. In onderdeel b, onder 2°, wordt "het burgerservicenummer" vervangen door "het burgerservicenummer of een versleutelde of afgeleide vorm daarvan ter identificatie van de gebruiker van DigiD Machtigen of het door de Kamer van Koophandel, bedoeld in artikel 2 van de Wet op de Kamer van Koophandel, uniek toegekende nummer aan rechtspersoon of een onderneming die in Nederland is gevestigd en toebehoort aan een natuurlijke persoon, alsmede de authenticatieverklaring indien beschikbaar".

3. Onderdeel b, onder 4°, komt te luiden:

4°. de gebruiksgegevens, waaronder gegevens over het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van DigiD Machtigen is ingelogd op de website van DigiD Machtigen, handelingen van de gebruiker van DigiD Machtigen (inloggen, aanvragen, intrekken en activeren), de betrokken dienst, en de afnemer van DigiD Machtigen waarvoor de gebruiker van DigiD Machtigen is gemachtigd, alsmede het tijdstip waarop dit gebeurt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip,

kenmerken van het gebruik, waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;

4. In onderdeel b, onder 6°, wordt na "burgerservicenummer" ingevoegd ", notificatiegegevens waaronder het voorkeurskanaal,".

5. Er wordt een onderdeel toegevoegd, luidende:
c. over afnemers van DigiD Machtigen: administratieve gegevens noodzakelijk in verband met het gebruik door de afnemer van DigiD Machtigen, waaronder de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van DigiD Machtigen en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

D

Artikel 4 wordt als volgt gewijzigd:

1. In onderdeel b, onder 2°, wordt "het burgerservicenummer," vervangen door "het burgerservicenummer of versleutelde vorm daarvan ter identificatie van de gebruiker van MijnOverheid;".

2. In onderdeel b, onder 3°, wordt "inloghistorie" geschrapt.

3. In onderdeel b, onder 4°, wordt na "daarvan," ingevoegd "inloghistorie".

4. Onderdeel b, onder 6°, komt te luiden:

6°. gegevens noodzakelijk voor de ondersteuning bij het veilige en betrouwbare gebruik van MijnOverheid, waaronder het burgerservicenummer, gegevens in het bericht van de afnemer of in een andere functionaliteit van MijnOverheid die de afnemer afneemt en gegevens die worden verwerkt bij de ondersteuning van de gebruiker, zoals de relevante BRP-gegevens en gegevens met betrekking tot het soort apparaat waarmee op elektronische wijze gecommuniceerd kan worden;

5. In onderdeel b worden de volgende onderdelen toegevoegd:

7°. gegevens noodzakelijk voor de dienst Persoonlijke gegevens, waaronder de gegevens genoemd onder 1°, het burgerservicenummer en overige gegevens waarin inzage kan worden verleend via deze dienst;

8°. gegevens noodzakelijk voor de dienst Algemene bekendmakingen, kennisgevingen en mededelingen, waaronder het burgerservicenummer, de geboortedatum, het actuele adres van de gebruiker en het e-mailadres;

6. In onderdeel c, wordt onder wijziging van de punt aan het eind van onderdeel c in een puntkomma, een onderdeel toegevoegd, luidende:

5°. gegevens noodzakelijk voor de ondersteuning bij het veilige en betrouwbare gebruik van MijnOverheid, waaronder het burgerservicenummer, gegevens in het bericht van de afnemer of in een andere functionaliteit van MijnOverheid die de afnemer afneemt en gegevens die worden verwerkt bij de ondersteuning van de gebruiker;

7. Er wordt een onderdeel toegevoegd, luidende:
d. over afnemers van MijnOverheid: administratieve gegevens noodzakelijk in verband met het gebruik door de afnemer van MijnOverheid, waaronder, indien van toepassing, de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van MijnOverheid en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

E

Artikel 5 komt te luiden:

Artikel 5. Persoonsgegevens BSN-Koppelregister

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van het BSN-Koppelregister de volgende persoonsgegevens:

a. over de gebruiker van een toegelaten privaat of publiek identificatiemiddel, erkend bedrijfs- of organisatiemiddel of machtiging die elektronische diensten wil afnemen:
1°. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum en de datum van overlijden;
2°. het burgerservicenummer of een versleutelde of afgeleide vorm daarvan ter identificatie van de gebruiker van een toegelaten privaat of publiek identificatiemiddel, bedrijfs- of organisatiemiddel of machtiging of het uniek identificerend nummer of een afgeleide vorm daarvan ingeval van authenticatie buiten Nederland en binnen de EU;
3°. de datum van totstandkoming en het niet langer gebruiken van de koppeling tussen het toegelaten private of publieke identificatiemiddel, bedrijfs- of organisatiemiddel of machtiging en de afgeleide vorm van het burgerservicenummer of het uniek identificerend nummer ter identificatie van de gebruiker;
4°. statusgegevens van de aan de gebruiker gekoppelde middelen;
b. over afnemers van het BSN-Koppelregister: administratieve gegevens noodzakelijk in verband met het gebruik van het BSN-Koppelregister, waaronder, indien van toepassing, de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van het BSN-koppelregister en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

F

Na artikel 5 worden zes artikelen ingevoegd, luidende:

Artikel 5a. Persoonsgegevens routeringsvoorziening

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking en betrouwbaarheid van de routeringsvoorziening de volgende persoonsgegevens over:
a. de gebruiker van een toegelaten publiek of privaat identificatiemiddel of erkend bedrijfs- of organisatiemiddel, die dit middel wil gebruiken in het kader van elektronische dienstverlening:
1°. de voornaam, achternaam, geboortedatum, geboortenaam, geboorteplaats, actueel adres en geslacht, in voorkomend geval in versleutelde vorm;
2°. een nummer dat ter identificatie van een persoon kan worden gebruikt of tot een persoon kan worden herleid, waaronder het burgerservicenummer of een versleutelde of afgeleide vorm daarvan en het afgeleide uniek identificerend nummer in geval van authenticatie buiten Nederland en binnen de EU;
3°. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker is ingelogd, handelingen van de gebruiker, het door de gebruiker gebruikte identificatiemiddel en betrouwbaarheidsniveau, de website van de organisatie waar de gebruiker een middel aanvraagt of vanuit welke de gebruiker inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;
b. de vertegenwoordigde in het geval van machtiging: een nummer dat ter identificatie van de vertegenwoordigde kan worden gebruikt of tot de vertegenwoordigde kan worden herleid, waaronder het burgerservicenummer of een versleutelde of afgeleide vorm daarvan;
c. afnemers van de routeringsvoorziening: administratieve gegevens noodzakelijk in verband met het gebruik door de afnemer van de routeringsvoorziening, waaronder, indien van toepassing, de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van de routeringsvoorziening en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

Artikel 5b. Persoonsgegevens privaat identificatiemiddel en - diensten

De aanbieder van een toegelaten privaat identificatiemiddel als bedoeld in artikel 9, tweede lid, van de wet, of een erkende ontsluitende dienst als bedoeld in artikel 9, derde lid van de wet, verwerkt voor de werking van het private identificatiemiddel en goede en veilige toegang met dat middel tot elektronische dienstverlening de volgende persoonsgegevens over gebruikers van het middel:
a. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden en het adres;
b. een nummer dat ter identificatie van een persoon kan worden gebruikt, waaronder het burgerservicenummer;
c. de accountgegevens, waaronder het mobiele telefoonnummer, het e-mailadres, de gebruikersnaam,

een afgeleide vorm van het wachtwoord, en overige gegevens die bij het account horen;
d. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van het middel is ingelogd, handelingen van de gebruiker, het door de gebruiker gekozen authenticatieniveau, de website van de instelling waar de gebruiker een toegelaten privaat authenticatiemiddel aanvraagt of vanuit welke de gebruiker van het toegelaten private identificatiemiddel met het middel inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;
e. gegevens die relevant zijn voor de adequate werking van het middel, waaronder in ieder geval de kenmerken van de door de gebruiker gebruikte software en hardware;
f. gegevens noodzakelijk voor de ondersteuning van de gebruiker, waaronder het burgerservicenummer en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker.

Artikel 5c. Persoonsgegevens bedrijfs- en organisatiemiddel en - diensten

Een erkende middelenuitgever, een erkende authenticatiedienst, een erkende ontsluitende dienst, een erkende machtigingsdienst of een attributendienst als bedoeld in artikel 12, derde lid, van de wet, verwerkt voor de werking van het bedrijfs- en organisatiemiddel en goede en veilige toegang met dat middel tot elektronische dienstverlening de volgende persoonsgegevens:
a. over gebruikers van een erkend bedrijfs- en organisatiemiddel:
1°. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de geboorteplaats, de nationaliteit, het actuele adres, het e-mailadres, het telefoonnummer, de foto en het type identiteitsbewijs, een gekwalificeerd certificaat dat wordt gebruikt als elektronische handtekening en bedrijfsgegevens;
2°. een nummer dat ter identificatie van een persoon kan worden gebruikt of tot een persoon kan worden herleid, waaronder het burgerservicenummer of een versleutelde of afgeleide vorm daarvan, het uniek identificerend nummer in geval van authenticatie buiten Nederland in afgeleide vorm, het nummer van een rijbewijs, het nummer van de Kamer van Koophandel;
3°. gebruikersgegevens noodzakelijk voor de registratie van een machtiging, waaronder de identiteit van de gemachtigde en machtigingsverlener, de dienst ter afname waarvan de machtiging is verleend, de looptijd en status van de machtiging en gegevens betreffende uitgevoerde verificaties en validaties;
4°. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van een bedrijfs- en organisatiemiddel is ingelogd, gegevens afkomstig van het authenticatiemiddel van de gebruiker, waarmee hij heeft ingelogd ter authenticatie, handelingen van de gebruiker, het door de gebruiker van een bedrijfs- en organisatiemiddel gebruikte authenticatieniveau, gegevens over ondertekende en ontvangen ondertekende berichten over een gebruiker die tussen de diensten worden uitgewisseld, de website van de instelling waar de gebruiker een bedrijfs- en organisatiemiddel aanvraagt of vanuit welke de gebruiker van het bedrijfs- en organisatiemiddel met het bedrijfs- en organisatiemiddel inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;
e. gegevens die relevant zijn voor de adequate werking van de voorziening, bedoeld in
5°. gegevens bedoeld in artikel 5d die noodzakelijk zijn voor de elektronische identificatie ter zake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eIDAS-voorziening;
6°. gegevens die relevant zijn voor de adequate werking van de toegang tot elektronische dienstverlening, waaronder in ieder geval de kenmerken van de door de gebruiker gebruikte software en hardware;
7°. gegevens noodzakelijk voor de ondersteuning van de gebruiker, waaronder gegevens die ter identificatie van de gebruiker kunnen worden gebruikt en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker van een bedrijfs- en organisatiemiddel.
b. over afnemers van een erkende ontsluitende dienst als bedoeld in artikel 12, derde lid, van de wet: administratieve gegevens noodzakelijk in verband met het gebruik door de gebruiker van een bedrijfs- en organisatiemiddel, waaronder, indien van toepassing, de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van een erkende ontsluitende dienst en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

Artikel 5d. Persoonsgegevens eIDAS-voorziening

1. Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de eIDAS-voorziening de volgende persoonsgegevens over de gebruiker van een toegelaten of erkend identificatiemiddel die dit middel wil gebruiken in het kader van elektronische dienstverlening:
a. naam en de noodzakelijke gegevens om deze correct weer te geven;
b. geboortedatum;
c. uniek identificerend nummer of een afgeleide vorm daarvan;
d. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van een toegelaten of erkend identificatiemiddel is ingelogd, handelingen van de gebruiker, het door de gebruiker gekozen authenticatieniveau, de website vanuit welke de gebruiker inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;
e. gegevens die relevant zijn voor de adequate werking van de voorziening, waaronder in ieder geval de EU-landkeuze van de gebruiker en de status van de koppeling tussen het burgerservicenummer en het uniek identificerend nummer;
f. burgerservicenummer of een versleutelde of afgeleide vorm daarvan.
2. Indien geen zekerheid omtrent uniciteit kan worden verkregen, verwerkt Onze Minister tevens de volgende gegevens:
a. geboortenaam en de noodzakelijke gegevens om deze correct weer te geven;
b. geboorteplaats;
c. geslacht;
d. adres.

Artikel 5e. Doelbinding

De gegevens als bedoeld in de artikelen 2, 3 en 5 tot en met 5d worden niet gebruikt voor andere doeleinden dan de goede werking van identificatiemiddelen en de goede en veilige toegang met die middelen of via machtiging tot elektronische dienstverlening.

Artikel 5f. Persoonsgegevens misbruik en oneigenlijk gebruik

Onze Minister kan de volgende gegevens verwerken, indien dit noodzakelijk is voor het waarborgen van de veilige toegang tot en de werking van de elektronische dienstverlening en het voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening:
a. de gegevens, bedoeld in de artikelen 2 tot en met 5d, die verwerkt worden voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de voorzieningen van de generieke digitale infrastructuur;
b. de gegevens en inlichtingen, bedoeld in artikel 19 van de wet, die verstrekt worden door de bestuursorganen en aangewezen organisaties, aanbieders van een toegelaten identificatiemiddel en op grond van artikel 11 van de wet erkende middelenuitgevers en diensten;
c. de uit onderzoek voortgekomen persoonsgegevens, met inbegrip van openbaar toegankelijke persoonsgegevens en persoonsgegevens die door derden aan Onze Minister verstrekt zijn.

G

Artikel 6 wordt als volgt gewijzigd:

1. De aanhef komt te luiden: Onze Minister verstrekt aan de afnemers van DigiD, aan de eIDAS-voorziening en aan een routeringsvoorziening:

2. In onderdeel a. wordt “het burgerservicenummer” vervangen door “het burgerservicenummer, of een versleutelde of afgeleide vorm daarvan ter identificatie van de gebruiker van DigiD,”.

3. Er wordt een onderdeel toegevoegd, luidende:
c. de naam en de noodzakelijke gegevens om deze correct weer te geven, het uniek identificerend

nummer ingeval van authenticatie buiten Nederland en de geboortedatum van de gebruiker van DigiD ten behoeve van de elektronische identificatie ter zake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eIDAS-voorziening.

H

Artikel 8 wordt als volgt gewijzigd:

1. Onderdeel a. komt te luiden:

a. het burgerservicenummer, waar van toepassing de status van de toepasselijke berichtenvoorkeur van de gebruiker van MijnOverheid, voorafgaand aan het aanleveren en ter bevestiging van het afleveren van berichten en gegevens, of het falen daarvan, ten behoeve van de werking van de diensten van MijnOverheid, en op verzoek van een afnemer informatie over het openen van een bericht door de gebruiker van MijnOverheid, teneinde de gebruiker te attenderen op een eerder aan hem gezonden bericht;

2. Er wordt een onderdeel toegevoegd, luidende:

c. op verzoek van een afnemer inlichtingen die benodigd zijn om aflevering van een bericht te kunnen bevestigen.

I

Artikel 9 komt te luiden:

Artikel 9. Verstrekkingen in verband met het BSN-Koppelregister

Onze Minister verstrekt:
a. het burgerservicenummer in versleutelde of afgeleide vorm van de gebruiker van een toegelaten privaat of publiek identificatiemiddel of een erkend bedrijfs- of organisatiemiddel die dit nummer wil gebruiken in het kader van elektronische dienstverlening door bestuursorganen of aangewezen organisaties aan de routeringsvoorziening, de erkende middelenuitgever of authenticatiedienst, of de erkende machtigingsdienst;
b. het uniek identificerend nummer in afgeleide vorm aan de eIDAS-voorziening.

J

Artikel 10 wordt vervangen door vijf artikelen, luidende:

Artikel 9a. Verstrekkingen in verband met de routeringsvoorziening

Onze Minister verstrekt de voornaam, achternaam, geboortedatum, het burgerservicenummer, een afgeleide vorm van het uniek identificerend nummer in geval van authenticatie buiten Nederland, geboortenaam, geboorteplaats, actueel adres en geslacht en het gebruikte betrouwbaarheidsniveau van de gebruiker van een toegelaten privaat of publiek identificatiemiddel die dit middel gebruikt in het kader van elektronische dienstverlening door bestuursorganen of aangewezen organisaties, en het burgerservicenummer van de vertegenwoordigde zo mogelijk in versleutelde of afgeleide vorm aan de bedoelde bestuursorganen of aangewezen organisaties.

Artikel 9b. Verstrekkingen in verband met een privaat identificatiemiddel

De aanbieder van een toegelaten privaat identificatiemiddel als bedoeld in artikel 9, tweede lid, van de wet, verstrekt aan bestuursorganen en aangewezen organisaties en aan een routeringsvoorziening:
a. het burgerservicenummer of een versleutelde of afgeleide vorm daarvan ten behoeve van de vaststelling van de identiteit van de gebruiker;
b. het door de gebruiker gekozen betrouwbaarheidsniveau van het identificatiemiddel.

Artikel 9c. Verstrekkingen in verband met een bedrijfs- en organisatiemiddel

1. Een erkende middelenuitgever, een erkende authenticatiedienst, een erkende ontsluitende dienst, een routeringsvoorziening, een erkende machtigingsdienst of een attributendienst, bedoeld in artikel 12, derde lid, van de wet, verstrekken aan elkaar: de gegevens, bedoeld in artikel 5c, onderdeel a, onder 1°, 2°, 3° en 4°, voor zover noodzakelijk voor de werking van het bedrijfs- en organisatiemiddel.
2. Een erkende authenticatiedienst verstrekt de gegevens bedoeld in artikel 5c, onderdeel a, onder 5°, in versleutelde of afgeleide vorm via een erkende ontsluitende dienst of een routeringsvoorziening aan de eIDAS-voorziening.
3. Een erkende machtigingsdienst verstrekt de naam en de geboortedatum van de gebruiker en de gegevens, bedoeld in artikel 5c, onderdeel a, onder 2°, aan het BSN-Koppelregister.
4. Een erkende ontsluitende dienst of een routeringsvoorziening verstrekt aan afnemers in verband met hun elektronische dienstverlening aan de gebruikers van een bedrijfs- en organisatiemiddel:
a. het burgerservicenummer in versleutelde of afgeleide vorm, ten behoeve van de vaststelling van de identiteit van de gebruiker van een bedrijfs- en organisatiemiddel;
b. het door de gebruiker van een bedrijfs- en organisatiemiddel gekozen authenticatieniveau.

Artikel 9d. Verstrekkingen in verband met de eIDAS-voorziening

Onze Minister verstrekt:
a. aan het BSN-Koppelregister van de gebruiker van een toegelaten of erkend identificatiemiddel die dit middel wil gebruiken in het kader van elektronische dienstverlening het burgerservicenummer en de afgeleide vorm hiervan, en aan een routeringsvoorziening en de erkende ontsluitende dienst in de zin van artikel 1 van de wet het burgerservicenummer in versleutelde vorm en het uniek identificerend nummer in afgeleide vorm;
b. aan een erkende ontsluitende dienst of een routeringsvoorziening ten behoeve van bestuursorganen of aangewezen organisaties: de naam en de noodzakelijke gegevens om deze correct weer te geven, geboortedatum, geboorteplaats, adres en geslacht in versleutelde vorm van de gebruiker van een toegelaten of erkend identificatiemiddel die dit middel wil gebruiken in het kader van elektronische dienstverlening;
c. bij grensoverschrijdende authenticatie het uniek identificerend nummer en indien beschikbaar het burgerservicenummer aan het BSN-Koppelregister en een afgeleide vorm daarvan aan bestuursorganen of aangewezen organisaties in het kader van elektronische dienstverlening.
d. bij grensoverschrijdende authenticatie het van het burgerservicenummer afgeleide uniek identificerend nummer, de naam en de noodzakelijke gegevens om deze correct weer te geven, geboortedatum, geboorteplaats, adres en geslacht aan de betreffende andere lidstaat.

Artikel 10. Overige verstrekkingen

Onverminderd het bepaalde in de artikelen 6 tot en met 9d, verstrekt Onze Minister geen gegevens over een bezoeker of gebruiker van de in de artikelen 2 tot en met 5d genoemde voorzieningen en middelen of de uit onderzoek voortgekomen gegevens, bedoeld in artikel 5f, onderdeel c, aan anderen dan de bezoeker of de gebruiker zelf zonder voorafgaande toestemming van de bezoeker of de gebruiker, tenzij:
a. het een verstrekking betreft aan een overheidsorgaan of rechtspersoon met een wettelijke taak die noodzakelijk is voor de borging van de beveiliging en betrouwbaarheid van de betreffende voorziening, of
b. hij daartoe gerechtigd is op grond van een wettelijke bepaling.

K

Artikel 11 wordt als volgt gewijzigd:

1. Het vijfde lid komt te luiden:

5. De accountgegevens, bedoeld in artikel 2, onderdeel c, onder 3°, die nodig zijn voor het actuele gebruik van DigiD, zoals het actuele en historische mobiele of vaste telefoonnummer en e-mailadres, de actuele gebruikersnaam, het actuele wachtwoord, het account-ID, de status van het account, de gekozen documentsoort voor elektronische identificatie en het soort apparaat waarmee op

elektronische wijze gecommuniceerd kan worden met het Nederlands paspoort, de Nederlandse identiteitskaart of het Nederlands rijbewijs, de status van het identificatiemiddel worden bewaard zo lang het bijbehorende DigiD geldig is, en zodra dat niet meer het geval is maximaal 5 jaar.

2. Het achtste lid komt te luiden:

8. De gegevens noodzakelijk voor de ondersteuning van de gebruiker en de administratie van DigiD, bedoeld in artikel 2, onderdeel c, onder 6°, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.

3. Er worden vier leden toegevoegd, luidende:

9. De gegevens afkomstig van de chip van het Nederlands paspoort, het Nederlandse identiteitsbewijs of het Nederlandse rijbewijs, bedoeld in artikel 2, onderdeel c, onder 7° en 8°, worden bewaard zolang de sessie duurt.
10. De eIDAS gegevens, bedoeld in artikel 2, onderdeel c, onder 9°, worden maximaal 2 jaar bewaard, met uitzondering van uniek identificerende nummers, burgerservicenummers en de versleutelde vormen daarvan, welke maximaal vijf jaar worden bewaard.
11. De gegevens over afnemers van DigiD, bedoeld in artikel 2, onderdeel d, worden bewaard voor de duur van het gebruik door de afnemer van DigiD, en daarna maximaal vijf jaar.
12. Een reservekopie van alle in dit artikel genoemde gegevens wordt maximaal vier maanden bewaard nadat de bewaartermijnen bedoeld in de andere leden van dit artikel zijn verlopen.

L

Artikel 12 wordt als volgt gewijzigd:

1. In het tweede lid wordt “de datum van overlijden” vervangen door “de reden voor de opschorting van de persoonslijst in de basisregistratie personen”.

2. In het vierde lid wordt “Het burgerservicenummer” vervangen door “het burgerservicenummer of het door de Kamer van Koophandel, genoemd in artikel 2 van de Wet op de Kamer van Koophandel, uniek toegekende nummer aan een onderneming die in Nederland is gevestigd en toebehoort aan een natuurlijke persoon”.

3. Er worden twee leden toegevoegd, luidende:
7. De gegevens over afnemers van DigiD Machtigen, bedoeld in artikel 3, onderdeel c, worden bewaard voor de duur van het gebruik door de afnemer van DigiD Machtigen, en daarna maximaal vijf jaar.
8. Een reservekopie van alle in dit artikel genoemde gegevens wordt maximaal vier maanden bewaard.

M

Artikel 13 wordt als volgt gewijzigd:

1. In het tweede lid wordt “bedoeld in bedoeld in artikel 4” vervangen door “bedoeld in artikel 4”.

2. In het derde lid vervalt “de nationaliteit, de geboortedatum, de datum van overlijden en”.

3. Onder vernummering van de leden 5 en 6 tot 6 en 7 komt lid 5 te luiden:
5. De gegevens over een gebruiker van MijnOverheid en zijn MijnOverheid-account, bedoeld in artikel 4, onderdeel b, onder 7° en 8° worden bewaard zolang het bijbehorende MijnOverheid-account bestaat, en zodra het account is opgeheven maximaal 1 jaar.

4. In het zesde lid wordt een onderdeel toegevoegd, luidende:

d. de gegevens, bedoeld onder 5°, blijven bewaard zo lang het MijnOverheid-account bestaat, en zodra dat account is opgeheven maximaal 1 jaar.

5. Er worden twee leden toegevoegd, luidende:
8. De gegevens over afnemers van MijnOverheid, bedoeld in artikel 4, onderdeel d, worden bewaard voor de duur van het gebruik door de afnemer van MijnOverheid, en daarna maximaal vijf jaar.

9. Een reservekopie van alle in dit artikel genoemde gegevens wordt maximaal vier maanden bewaard.

N

Artikel 14 komt te luiden:

Artikel 14. Bewaartermijnen in verband met het BSN-Koppelregister

De bewaartermijn van de gegevens, bedoeld in artikel 5, is als volgt:
a. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden, het uniek identificerend nummer en het burgerservicenummer en de versleutelde vorm daarvan worden niet langer bewaard dan nodig is om de gegevens op juistheid te controleren;
b. het burgerservicenummer in afgeleide vorm en het uniek identificerend nummer in afgeleide vorm ingeval van authenticatie buiten Nederland en binnen de EU, en de gegevens, bedoeld in artikel 5, onderdeel a, onder 3° en 4°, worden bewaard zo lang als de koppeling tussen het toegelaten private of publieke identificatiemiddel of erkende bedrijfs- of organisatiemiddel bestaat en zodra dat niet meer het geval is, maximaal 5 jaar;
c. de gegevens over afnemers van de BSN-Koppelregister, bedoeld in artikel 5, onderdeel b, worden bewaard voor de duur van het gebruik van het BSN-Koppelregister en daarna maximaal vijf jaar.

O

Na artikel 14 worden vijf artikelen ingevoegd, luidende:

Artikel 14a. Bewaartermijnen in verband met de routeringsvoorziening

De bewaartermijn van de gegevens, bedoeld in artikel 5a, is als volgt:
a. de gegevens, bedoeld in artikel 5a, onderdeel a, onder 1°, worden bewaard zolang de gebruiker het identificatiemiddel gebruikt;
b. een nummer dat ter identificatie kan worden gebruikt als bedoeld in artikel 5a, onderdeel a, onder 2°, of onderdeel b, wordt maximaal 18 maanden na afloop van het authenticatieproces bewaard;
c. de gebruiksgegevens, bedoeld in artikel 5a, onderdeel a, onder 3°, worden maximaal vijf jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker;
d. de gegevens over afnemers van de routeringsvoorziening, bedoeld in artikel 5a, onderdeel c, worden bewaard voor de duur van het gebruik ervan door de routeringsvoorziening en daarna maximaal vijf jaar.

Artikel 14b. Bewaartermijnen in verband met het privaat identificatiemiddel

1. De naam van de gebruiker en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum, de datum van overlijden en het adres, bedoeld in artikel 5b, onderdeel a, worden maximaal 6 weken bewaard.
2. De gebruiksgegevens, bedoeld in artikel 5b, onderdeel d, worden maximaal 5 jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker.
3. Een nummer dat ter identificatie van een persoon kan worden gebruikt als bedoeld in artikel 5b, onderdeel b, wordt bewaard:
a. gedurende het aanvraagproces maximaal 18 maanden; of
b. zo lang het bijbehorende identificatiemiddel geldig is, en zodra dat niet meer het geval is maximaal 5 jaar.
4. De accountgegevens, bedoeld in artikel 5b, onderdeel c, die nodig zijn voor het actuele gebruik van de voorziening voor de uitgifte en authenticatie van een toegelaten privaat identificatiemiddel, zoals het actuele en historische mobiele of vaste telefoonnummer en e-mailadres, de actuele gebruikersnaam, het actuele wachtwoord, het account-ID en de status van het account worden bewaard zo lang het bijbehorende identificatiemiddel geldig is, en zodra dat niet meer het geval is maximaal 5 jaar.

5. De overige accountgegevens, bedoeld in artikel 5b, onderdeel c, worden maximaal 18 maanden bewaard.
6. De gegevens die relevant zijn voor de adequate werking van de voorziening, bedoeld in artikel 5b, onderdeel e, worden bewaard zo lang de gebruiker van de voorziening is ingelogd.
7. De gegevens noodzakelijk voor de ondersteuning van de gebruiker, bedoeld in artikel 5b, onderdeel f, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.

Artikel 14c. Bewaartermijnen in verband met het bedrijfs- en organisatiemiddel

1. De gegevens, bedoeld in artikel 5c, onderdeel a, onder 1° tot en met 3°, worden bewaard zolang de gebruiker het bedrijfs-en organisatiemiddel of de machtiging gebruikt en zodra dat niet meer het geval is maximaal 18 maanden.
2. De gegevens, bedoeld in artikel 5c, onderdeel a, onder 4° en 6°, worden maximaal 5 jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker.
3. De eIDAS-gegevens, bedoeld in artikel 5c, onderdeel a, onder 5°, worden bewaard zolang de gebruiker het bedrijfs-en organisatiemiddel of de machtiging gebruikt en zodra dat niet meer het geval is maximaal 5 jaar.
4. De gegevens noodzakelijk voor de ondersteuning van de gebruiker, bedoeld in artikel 9c, onderdeel a, onder 7°, worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden.
5. De gegevens, bedoeld in artikel 5c, onderdeel b, worden maximaal 5 jaar bewaard.

Artikel 14d. Bewaartermijnen in verband met de eIDAS-voorziening

1. De gegevens, bedoeld in artikel 5d, eerste lid, onderdelen a en b, en tweede lid, worden bewaard zolang de gebruiker het identificatiemiddel gebruikt.
2. Een nummer dat ter identificatie kan worden gebruikt bedoeld in artikel 5d, eerste lid, onderdelen c en f, worden maximaal 5 jaar bewaard na het laatste gebruik.
3. De gebruiksgegevens, bedoeld in artikel 5d, eerste lid, onderdelen d en e, worden maximaal 5 jaar bewaard na het laatste gebruik, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker.

Artikel 14e Bewaartermijnen in verband met misbruik en oneigenlijk gebruik generieke digitale infrastructuur

De bewaartermijn van de gegevens, bedoeld in artikel 5f, onderdeel c, is maximaal 5 jaar na afloop van de in de artikelen 11 tot en met 14d genoemde bewaartermijnen.

P

Na artikel 15 wordt een artikel ingevoegd, luidende:

Artikel 15a. Beveiliging van persoonsgegevens

Teneinde de te verwerken persoonsgegevens te beveiligen en deze te beschermen tegen ongeoorloofde of onrechtmatige verwerking en opzettelijk verlies, vernietiging of beschadiging, neemt de in de artikelen 2 tot en met 15 bedoelde verwerker passende technische, organisatorische en personele maatregelen, waaronder inzake de juiste en veilige bediening en gebruik van informatiesystemen, de toegang tot en de beschikbaarheid en integriteit van informatiesystemen en het herkennen en herstellen van beveiligingsinbreuken.

Q

Het opschrift van hoofdstuk 5 komt te luiden:

Hoofdstuk 6. Slotbepalingen

R

Onder vernummering van de artikelen 16 en 17 tot 25 en 26 wordt een nieuw hoofdstuk 5 ingevoegd, luidende:

Hoofdstuk 5. Informatieveiligheid ten aanzien van de toegang tot elektronische dienstverlening

§ 5.1 Bedrijfsvoering

Artikel 16. Informatieveiligheidsbeleid

1. Bestuursorganen en aangewezen organisaties stellen beleid op voor de informatieveiligheid van de toegang tot hun elektronische dienstverlening, waaronder een veiligheidsplan dat is gebaseerd op een risico-identificatie en risico-afweging.
2. Het in het eerste lid bepaalde laat de toepasselijkheid van de eisen inzake het elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon, onderneming of rechtspersoon, zoals bedoeld in de wet, onverlet.
3. Het informatieveiligheidsbeleid behelst een continue proces, dat integraal deel uitmaakt van de reguliere bedrijfsvoeringscyclus en jaarlijks wordt beoordeeld en zo nodig bijgesteld.
4. Onverminderd de toepasselijkheid van de bepalingen in hoofdstuk 5 van dit besluit, kan Onze Minister nadere regels stellen met betrekking tot de werking en beveiliging van de toegang tot elektronische dienstverlening.

Artikel 17. Organisatie en beheer

1. Bestuursorganen en aangewezen organisaties beleggen taken, verantwoordelijkheden en coördinatie ter zake van informatieveiligheid van de toegang tot hun elektronische dienstverlening.
2. Bestuursorganen en aangewezen organisaties nemen passende beheersmaatregelen, waaronder inzake het gebruik van bedrijfsmiddelen en de classificatie en verwerking van informatie.

Artikel 18. Personele en fysieke beveiliging

1. Bestuursorganen en aangewezen organisaties rusten hun personeel toe om het informatieveiligheidsbeleid ter zake van de toegang tot elektronische dienstverlening uit te voeren.
2. Bestuursorganen en aangewezen organisaties beschermen hun terreinen, ruimten en apparatuur fysiek.

Artikel 19. ICT-voorzieningen en informatiesystemen

1. Bestuursorganen en aangewezen organisaties waarborgen juiste en veilige bediening en gebruik van ICT-voorzieningen en informatiesystemen, door onder meer de toepassing van functiescheiding.
2. Bestuursorganen en aangewezen organisaties waarborgen de beschikbaarheid en integriteit van ICT-voorzieningen en informatiesystemen, door onder meer de toepassing van systeemplanning, bescherming tegen kwaadaardige software, het maken van reservekopieën en netwerkbeheer.
3. Bestuursorganen en aangewezen organisaties reglementeren en beschermen de uitwisseling van informatie binnen de eigen organisatie en met externen, door onder meer cryptografische versleuteling en het gebruik van digitale certificaten of maatregelen die aantoonbaar een tenminste gelijkwaardig beveiligingsniveau bieden.
4. Bestuursorganen en aangewezen organisaties nemen beheersmaatregelen inzake de toegang tot informatie en informatiesystemen, waaronder netwerken en besturingssystemen.
5. Bestuursorganen en aangewezen organisaties nemen bij het beveiligingsniveau passende maatregelen ter beveiliging van ontwerp, ontwikkeling, onderhoud, ondersteuning en werking van ICT-voorzieningen en informatiesystemen.
6. Bestuursorganen en aangewezen organisaties stellen beleid op voor en treffen maatregelen inzake het herkennen en het herstellen van beveiligingsinbreuken, daaronder begrepen misbruik van elektronische identificatiemiddelen. Dit beleid omvat in ieder geval detectie van kwetsbaarheden, rapportage van incidenten, respons, escalatie, schadebeperking, communicatie en evaluatie.

§ 5.2 Standaarden en normen

Artikel 20. Technische standaarden

1. Bestuursorganen en aangewezen organisaties passen bij de inrichting van hun beheerssysteem inzake informatieveiligheid van de toegang tot hun elektronische dienstverlening de technische standaarden toe die bij ministeriële regeling zijn aangewezen.
2. Met technische standaarden als bedoeld in het eerste lid, worden gelijkgesteld standaarden die een

tenminste gelijkwaardig beschermingsniveau bieden. Het aantonen van een gelijkwaardig beschermingsniveau geschiedt op basis van een verklaring van een onafhankelijke en gekwalificeerde auditor. Hieronder wordt mede begrepen een gelijkwaardige bevoegde instelling in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend verdrag dat Nederland bindt.

Artikel 21. Normen

1. Bestuursorganen en aangewezen organisaties worden geacht aan de artikelen 16 tot en met 19 te voldoen, indien zij ISO/NEN 27001 – 27002 aantoonbaar toepassen bij de inrichting van hun beheerssysteem inzake informatieveiligheid van de toegang tot hun elektronische dienstverlening.
2. Aangewezen organisaties als bedoeld in onderdeel 3 van de bijlage bij artikel 2, tweede lid, onder a, van de wet, worden geacht aan de artikelen 16 tot en met 19 te voldoen, indien zij ISO/NEN 7510 aantoonbaar toepassen bij de inrichting van hun beheerssysteem inzake informatieveiligheid van de toegang tot hun elektronische dienstverlening.
3. Aantoonbare toepassing van het in het eerste en tweede lid bepaalde geschiedt door het overleggen van een verklaring van een onafhankelijke en gekwalificeerde auditor. Hieronder wordt mede begrepen een gelijkwaardige bevoegde instelling in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend verdrag dat Nederland bindt.

§ 5.3 Monitoring en verantwoording

Artikel 22. Aansluiting

1. Bestuursorganen en aangewezen organisaties voldoen aan de door Onze Minister gestelde testcriteria voor aansluiting op de voor de toegang tot elektronische dienstverlening relevante voorzieningen, waaronder het gebruik van een gangbare browser en het hebben van een zichtbaar beveiligde verbinding.
2. Bij een nieuwe aansluiting vindt rapportage aan Onze Minister als bedoeld in artikel 24, eerste lid, voor het eerst plaats binnen twee maanden na aansluiting.

Artikel 23. Logging

1. Teneinde onbevoegde informatieverwerking en systeemtechnische fouten bij de toegang tot hun elektronische dienstverlening te kunnen ontdekken, maken bestuursorganen en aangewezen organisaties ter zake van het gebruik van ICT-voorzieningen logbestanden aan die regelmatig worden beoordeeld.
2. De logbestanden betreffen de uitgevoerde authenticaties, de daarbij gebruikte identificatiemiddelen, de tijdstippen waarop is ingelogd en uitgelogd, de systeemtechnische gegevens, waaronder het IP-adres en, indien van toepassing, machtigingsgegevens. Deze gegevens worden maximaal 5 jaar bewaard.

Artikel 24. Audit

1. Bestuursorganen en aangewezen organisaties laten hun informatieveiligheidsbeleid ter zake van de toegang tot elektronische dienstverlening beoordelen door de uitvoering van een controle van hun informatiesystemen en betrekken de resultaten bij een jaarlijkse audit. Rapportage geschiedt jaarlijks via de planning en control-cyclus, voor 1 mei over het voorgaande kalenderjaar, aan Onze Minister.
2. De rapportage, bedoeld in het eerste lid, betreft de opzet en het bestaan van maatregelen en procedures gericht op de beveiliging en kan tevens betrekking hebben op de werking van de genomen beheersmaatregelen.
3. Bestuursorganen en aangewezen organisaties nemen bij het jaarlijkse assessment, zoals bedoeld in het eerste lid, de hiertoe door Onze Minister vastgestelde ICT-beveiligingsrichtlijnen in acht. Deze betreffen onder meer netwerkveiligheid, besturingssysteem, basisbeveiliging, applicatiebeveiliging en penetratietest.
4. Het assessment, bedoeld in het eerste lid, wordt uitgevoerd door een onafhankelijke en gekwalificeerde auditor. Hieronder wordt mede begrepen een medewerker van een gelijkwaardige bevoegde instelling in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend verdrag dat Nederland bindt.

5. Een bestuursorgaan of aangewezen organisatie stelt op basis van de door Onze Minister aangegeven risico-identificatie een verbeterplan op, indien uit de rapportage, bedoeld in het eerste lid, blijkt dat op onderdelen niet wordt voldaan aan het informatieveiligheidsbeleid. Aan Onze Minister wordt een verbeterrapport gezonden binnen de door hem gestelde termijn.
6. Onze Minister kan beleidsregels vaststellen inzake de toepassing van het vierde lid, en met betrekking tot de wijze van beoordeling, rapportage en indiening van een verbeterplan.

S

Artikel 26 (nieuw) komt te luiden:

Artikel 26. Citeertitel

Dit Besluit wordt aangehaald als: Besluit digitale overheid.

Artikel II

De artikelen van dit besluit treden 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 dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

Gegeven,

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

R.W. Knops

Nota van Toelichting

Inhoudsopgave

I Algemeen

1 Inleiding

2 Hoofdlijnen

3 Verhouding tot andere regelgeving

4 Inhoud

4.1 Verwerking persoonsgegevens

- 4.1.1. Persoonsgegevens DigiD, DigiD Machtigen
- 4.1.2. Persoonsgegevens MijnOverheid
- 4.1.3. Persoonsgegevens toegelaten privaat middel voor burgers
- 4.1.4. Persoonsgegevens bedrijfs- en organisatiemiddel
- 4.1.5. Persoonsgegevens BSN-K
- 4.1.6. Persoonsgegevens routeringsvoorziening
- 4.1.7. Persoonsgegevens eIDAS-voorziening

4.2 Informatieveiligheid; werkingssfeer en verhouding tot praktijk

5 Privacy en verhouding tot algemene verordening gegevensbescherming

6 Gevolgen en uitvoerbaarheid (incl. regeldruk)

6.1 Verwerking persoonsgegevens

6.2 Informatieveiligheid

6.3 Resultaten uitvoeringstoetsen (tijdens consultatie)

7 Toezicht en handhaving

8 Evaluatie

9 Consultatie en advies

10 Inwerkingtreding

II Artikelsgewijs

Nota van toelichting

I Algemeen deel

1 Inleiding

De Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft de Tweede Kamer toegezegd regelgeving op te zullen stellen met betrekking tot publieke en private identificatiemiddelen die gebruikt kunnen worden bij het verlenen van toegang tot dienstverlening in het publieke domein. Hiertoe is het wetsvoorstel Digitale overheid voorbereid. Ingevolge dit wetsvoorstel is op diverse onderdelen uitvoeringsregelgeving nodig. Het onderhavige voorstel voor een algemene maatregel van bestuur behoort tot dit regelgevingscluster en stelt regels inzake informatieveiligheid en de verwerking van persoonsgegevens die gebruikt worden in het kader van de toegang tot elektronische overheidsdienstverlening. In het bijzonder dient de algemene maatregel van bestuur

ter uitvoering van de artikelen 4 en 16 van de ontwerpwet. Het huidige Besluit verwerking persoonsgegevens generieke digitale infrastructuur wordt hiertoe gewijzigd en aangevuld voor wat betreft de bepalingen over persoonsgegevensverwerking en aangevuld met een nieuw hoofdstuk, te weten inzake informatieveiligheid ten aanzien van de toegang tot elektronische dienstverlening. Om redenen van deze verbreding wordt ook de citeertitel van het Besluit gewijzigd.

2 Hoofdlijnen

Binnen het stelsel van de generieke digitale infrastructuur, in het bijzonder bij de toegang tot elektronische overheidsdienstverlening, worden (persoons)gegevens verwerkt. Op grond van de Algemene verordening gegevensbescherming[1] (AVG) kan dergelijke gegevensverwerking alleen plaatsvinden indien er een legitieme grondslag voor de verwerking aanwezig is. In het wetsvoorstel Digitale overheid zijn de grondslagen voor de gegevensverwerkingen vastgelegd (artikel 16).

Onze Minister, alsmede bestuursorganen en aangewezen organisaties, mogen persoonsgegevens, waaronder het burgerservicenummer, verwerken voor zover dit noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge de wet Digitale overheid (artikel 16, eerste lid). Ook private partijen mogen persoonsgegevens, waaronder het burgerservicenummer, verwerken, voor zover dit noodzakelijk is voor de werking van toegelaten (erkende) private identificatiemiddelen, erkende bedrijfs- en organisatiemiddelen en de goede en veilige toegang tot elektronische dienstverlening (artikel 16, tweede en derde lid). Nadere uitwerking geschiedt bij algemene maatregel van bestuur; vastgelegd wordt welke persoonsgegevens verwerkt worden, aan wie de gegevens worden verstrekt en hoe lang de gegevens worden bewaard (artikel 16, vierde lid). Het onderhavige Besluit strekt tot uitvoering hiervan.

Het wetsvoorstel Digitale overheid stelt voorts (artikel 4) dat bestuursorganen en aangewezen organisaties - ook wel aangeduid als (publieke) dienstverleners of (semi)overheden – dienen te voldoen aan bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening die zij in stand houden. Ook nader gereguleerd dient te worden op welke wijze zij aantonen dat zij aan de informatieveiligheidseisen voldoen. Doel van deze algemene maatregel van bestuur is beide onderwerpen te reguleren, ten behoeve van veiligheid en betrouwbaarheid van de identificatie- en authenticatieketen. Het betreft hier de ratio en werkingssfeer die ten grondslag liggen aan de beveiligingsverplichtingen en de verantwoording daarop (beveiligingsassessments) zoals thans opgenomen in de aansluitvoorwaarden van DigiD. Beoogd wordt rechtmatigheid, rechtszekerheid en

[1] *Verordening (EU) 2016/679 van het Europees Parlement en de Raad, 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.*

duidelijkheid te bieden. Informatieveiligheid bij publieke dienstverleners en de bescherming van de persoonlijke levenssfeer binnen de generieke digitale infrastructuur betreft een gerechtvaardigd belang aangezien het de dienstverlening betreft in het publieke domein.

De adressaten van de regels in deze algemene maatregel van bestuur zijn:

- Onze Minister: hij moet aan eisen voldoen inzake de verwerking, verstrekking en bewaring van persoonsgegevens in de onder zijn verantwoordelijkheid vallende voorzieningen en bij het voorkomen en de aanpak van fraude en misbruik;

- Bestuursorganen en aangewezen organisaties in de zin van (artikel 2 van) de wet Digitale overheid: zij moeten aan eisen voldoen inzake de informatieveiligheid in verband met de verwerking van persoonsgegevens bij het verlenen van toegang aan burgers en bedrijven tot elektronische dienstverlening alsmede inzake de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening die zij in stand houden;

- Erkende private partijen die diensten in de zin van de artikelen 9-13 van de wet aanbieden, welke verband houden met private identificatiemiddelen voor burgers (artikel 9, tweede lid) respectievelijk bedrijven/organisaties (artikelen 11-13). Deze private partijen moeten aan eisen voldoen inzake de verwerking, verstrekking en bewaring van persoonsgegevens.

- Burgers/natuurlijke personen en bedrijven/ondernemingen: zij zijn indirect betrokken, aangezien de verwerkte persoonsgegevens hen - als houder van een toegelaten of erkend (publiek of privaat uitgegeven) identificatiemiddel - betreffen.

Het onderhavige Besluit voorziet tevens in een wijziging van het onderdeel MijnOverheid. Dit houdt primair verband met de Bekendmakingswet,[2] die een aantal grondslagen bevat met betrekking tot te verzenden attenderingen over bekendmakingen, mededelingen en kennisgevingen in de publicatiebladen. In artikel 20, derde lid, van die wet wordt aangegeven dat bij algemene maatregel van bestuur nadere regels worden gesteld over onder meer de opslag en verwerking van persoonsgegevens. Door middel van aanvulling van de artikelen 4 en 13 wordt hieraan gevolg gegeven.

3 Verhouding tot andere regelgeving

Wet Digitale overheid
Dit Besluit behelst primair de uitvoeringsregels waartoe de artikelen 4 en 16 van de wet digitale overheid verplichten. Ingevolge deze wet zullen meerdere algemene maatregelen van bestuur en ministeriële regelingen worden vastgesteld. Vanwege de aard en systematiek van deze (kader)wet, alsmede vanwege het feit dat er op het gebied van elektronische identificatie reeds regelgeving bestaat[3], is er voor gekozen niet alle (gedelegeerde) onderwerpen in een algemene maatregel van bestuur en een ministeriële regeling op te nemen, maar verschillende uitvoeringsregelingen te realiseren. Een ervan is het onderhavige Besluit, dat het Besluit verwerking persoonsgegevens generieke digitale infrastructuur wijzigt en aanvult. Een andere algemene maatregel van bestuur zal bijvoorbeeld de erkenning van private identificatiemiddelen en bijbehorende private diensten in verband met het bedrijfs- en organisatiemiddel betreffen, er zal een ministeriële regeling inzake bekostiging worden opgesteld, enzovoorts.

Wegenverkeerswet en Paspoortwet
Publieke identificatiemiddelen met het hoogste betrouwbaarheidsniveau (DigiD hoog) zullen worden geplaatst in de elektronische chip die is aangebracht op wettelijke identiteitsdocumenten. In eerste instantie wordt gedacht aan het rijbewijs en de Nederlandse identiteitskaart (NIK) als drager. Doordat de authenticatiefunctie op deze documenten wordt aangebracht, treden afhankelijkheden op met de

[2] Zoals gewijzigd door de Wet Elektronische Publicaties: wijziging van de Bekendmakingswet en een groot aantal andere wetten met als doel alle wettelijk voorgeschreven bekendmakingen, mededelingen en kennisgevingen van (voorgenomen) overheidsbesluiten die niet tot een of meer belanghebbenden zijn gericht, beter toegankelijk en kenbaar te maken door stroomlijning van de publicatievoorschriften.
[3] Gebaseerd op artikel X van de Wet elektronisch Berichtenverkeer Belastingdienst, welk artikel opgaat in de Wet digitale overheid.

processen die te maken hebben met deze documenten. Dit betekent dat in de wetgeving betreffende de NIK (de Paspoortwet; de verantwoordelijkheid van de minister) en het rijbewijs (de Wegenverkeerswet; de verantwoordelijkheid van de Minister van Infrastructuur en Waterstaat) nieuwe taken en grondslagen voor gegevensverwerking worden opgenomen die verband houden met het opnemen van de authenticatiefunctie op deze documenten. De benodigde wijziging van de Wegenverkeerswet is meegenomen in de wet digitale overheid. Aangezien de Paspoortwet een rijkswet is die niet bij nationale wet kan worden aangepast, kon de voor de invoering van het publiek identificatiemiddel op de NIK noodzakelijke wetswijziging niet worden meegenomen in de wet digitale overheid. In de Paspoortwet[4] worden bepalingen opgenomen in verband met het plaatsen van een publiek identificatiemiddel op documenten die op grond van deze wet worden uitgegeven. Daarbij wordt de mogelijkheid opengehouden om op termijn niet alleen de NIK, maar ook andere documenten, zoals paspoorten, als drager van een identificatiemiddel op niveau hoog aan te wijzen. Er worden grondslagen gecreëerd voor de verwerking van gegevens, ontleend aan het basisregister reisdocumenten, die verband houden met het aanbrengen van het publieke identificatiemiddel op de NIK tijdens het productieproces en het activeren daarvan. Doel is interactie te kunnen bewerkstelligen tussen infrastructuurvoorzieningen op basis van de wet digitale overheid en de voorzieningen ingevolge de Paspoortwet.

Privacyregelgeving (AVG)
Hierop wordt ingegaan bij punt 5 van deze toelichting.

4 Inhoud

4.1 Verwerking persoonsgegevens

De bepalingen over de persoonsgegevensverwerkingen die plaatsvinden binnen de generieke digitale infrastructuur, opgenomen in de hoofdstukken 2, 3 en 4 van het onderhavige besluit, dienen ter uitvoering van artikel 16 van de Wet digitale overheid. Hierin is bepaald dat de minister van BZK regels stelt bij algemene maatregel van bestuur over de persoonsgegevensverwerking in het kader van de goede uitvoering van de taken en verplichtingen die op grond van de Wet digitale overheid aan de minister van BZK, bestuursorganen en aangewezen organisaties zijn toebedeeld. Onder meer zorgaanbieders en zorgverzekeraars zijn "aangewezen organisaties" in de zin van de wet. Om die reden bevatten diverse bepalingen in dit Besluit ook grondslagen voor de verwerking van (versleutelde) gezondheidsgegevens. Doel is te waarborgen dat de persoonsgegevensverwerking rechtmatig plaatsvindt.

De bepalingen wijzigen het bestaande Besluit verwerking persoonsgegevens gdi op die punten waar de inwerkingtreding van de Wet digitale overheid heeft geleid tot wijzigingen in de verwerking van persoonsgegevens binnen de generieke digitale infrastructuur. Tevens wordt de verwerking van persoonsgegevens binnen een nieuwe dienst/functie van MijnOverheid toegevoegd. Voor een toelichting op de niet gewijzigde onderdelen van het besluit wordt verwezen naar de nota van toelichting bij het indertijd genaamde Besluit verwerking persoonsgegevens generieke digitale infrastructuur.[5]

De bepalingen in het besluit bieden o.a. de minister van BZK de bevoegdheid om in het kader van een goede inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de identificatiemiddelen, authenticatiediensten en als gevolg van beleids-, privacy- en inrichtingskeuzes randvoorwaardelijke voorzieningen binnen het stelsel van de generieke digitale infrastructuur waarvoor hij verantwoordelijk, is persoonsgegevens te verwerken van de gebruiker van een publiek, privaat, bedrijfs- of organisatiemiddel. Hierbij moet bedacht worden, dat "verwerken" niet betekent dat de genoemde gegevens in elk individueel geval verwerkt moeten worden, maar dat de gegevens het totale pakket omvatten dat (in zijn algemeenheid in het systeem over gebruikers) verwerkt kan worden.

Hieronder wordt per onderdeel op hoofdlijnen de ratio achter de wijzigingen nader toegelicht. Voor een meer gedetailleerde beschrijving van de wijziging wordt verwezen naar de artikelsgewijze toelichting.

[4] *Kamerstukken II* 2018/19, 35 047/R2108.
[5] Stb. 2016, 195.

4.1.1. Persoonsgegevens DigiD, DigiD Machtigen

Binnen de werking van de bestaande voorzieningen voor toegang tot elektronische overheidsdienstverlening is sprake van een aantal belangrijke wijzigingen die het noodzakelijk maken om het besluit aan te passen ten aanzien van de persoonsgegevens die worden verwerkt, en daarvoor de benodigde grondslagen te bieden.

Een belangrijke wijziging betreft het feit dat daar waar dat mogelijk is met pseudonimisering van het burgerservicenummer gewerkt zal gaan worden; in de bepalingen van het besluit wordt dat aangeduid als het burgerservicenummer in afgeleide vorm. Die afgeleide vorm kan nooit worden herleid tot het oorspronkelijke burgerservicenummer. Dit is een belangrijke privacybeschermende maatregel, omdat daarmee de verwerking van burgerservicenummer in belangrijke mate wordt beperkt. Deze maatregel wordt onder meer genomen om het mogelijk te maken dat naast het publieke identificatiemiddel private middelen worden toegelaten en daarbij de verwerking van het burgerservicenummer zoveel mogelijk te beperken. Deze maatregel vloeit mede voort uit de in 2017 uitgevoerde PIA.[6]

Naast het werken met pseudonimisering is voor de voorzieningen DigiD en DigiD Machtigen in het besluit toegevoegd dat ook een versleutelde vorm van het burgerservicenummer kan worden verwerkt ten behoeve van de identificatie van de gebruiker. Een versleutelde vorm kan, in tegenstelling tot een afgeleide vorm, wel worden herleid tot het oorspronkelijke burgerservicenummer en is uitsluitend bedoeld voor dienstverleners die op grond van de wet het burgerservicenummer mogen verwerken.

Ook wordt met de wet digitale overheid beoogd om voor DigiD de eIDAS-betrouwbaarheidsniveaus "substantieel" en "hoog" beschikbaar te laten komen. Daarbij is voorzien dat dit gebeurt met gebruikmaking van (uitgifteprocessen van) het paspoort, identiteitskaart en het rijbewijs. Ook is voorzien dat gebruik wordt gemaakt van bestaande technieken, zoals de zogeheten *remote document authentication (*RDA) ter identificatie van de gebruiker via de chip op het paspoort, identiteitskaart of het rijbewijs waarvoor het gebruik van een mobiele telefoon (of in de toekomst USB) benodigd is.

Het is daarvoor noodzakelijk om bepaalde gegevens te verwerken ten aanzien van het paspoort, identiteitskaart en het rijbewijs. Dit betekent dat de daarvoor benodigde persoonsgegevens opgenomen moeten worden in het besluit. De aanpassingen van de te verwerken persoonsgegevens voor DigiD beogen aldus de gegevens die noodzakelijk zijn voor de goede en betrouwbare uitgifte en gebruik van DigiD op de niveaus substantieel en hoog mogelijk te maken. Het betreft de noodzakelijke gegevens die worden verwerkt ten behoeve van de betrouwbare uitgifte van DigiD op de niveaus substantieel en hoog alsmede de gegevens die worden verwerkt om gebruik (elektronische identificatie met het document bij een overheidsdienstverlener) mogelijk te maken.

Voorts wordt in de nieuwe situatie beoogd om ook grensoverschrijdende elektronische dienstverlening mogelijk te maken binnen de Europese Unie. Daarvoor is tussenkomst van de zogenaamde eIDAS-voorziening benodigd. Hiertoe wordt in het wetsvoorstel digitale overheid een grondslag geboden en wordt in dit besluit gegevensverwerking ter zake gereguleerd.

Ook zullen verstrekkingen aan afnemers voortaan plaatsvinden via de routeringsvoorziening. Deze strekt ertoe dienstverleners te 'ontzorgen'; bij gebruik van deze voorziening hebben dienstverleners, ongeacht het aantal toegelaten/erkende identificatiemiddelen, slechts een enkele aansluiting nodig (zie paragraaf 4.1.6.).

Verder wordt het mogelijk om een bedrijfsmiddel te gebruiken als middel voor elektronische identificatie van de gemachtigde, in welk verband het unieke nummer dat door de Kamer van Koophandel is toegekend aan een onderneming die in Nederland is gevestigd en toebehoort aan een natuurlijke persoon verwerkt wordt bij de registratie van de machtigingsrelatie tussen een burger en een dergelijke onderneming.

[6] https://www.rijksoverheid.nl/documenten/rapporten/2017/06/28/gegevensbeschermingseffectbeoordeling-eid-stelsel

Met de huidige wijziging wordt voor de voorzieningen DigiD en DigiD Machtigen tevens gebruik gemaakt van de mogelijkheid om te expliciteren dat er voor de administratieve afhandeling van DigiD en DigiD Machtigen gegevens over afnemers worden verwerkt. Daarbij worden gegevens van contactpersonen van de dienstverleners verwerkt.

4.1.2. Persoonsgegevens MijnOverheid

Als gevolg van de wet Elektronische Publicaties wordt aan de bestaande diensten van MijnOverheid een nieuwe dienst (functie) toegevoegd die de gebruikers van MijnOverheid informeert over algemene bekendmakingen, kennisgevingen en mededelingen die voor hen van belang zullen zijn.[7] De gebruiker wordt hiermee in de gelegenheid gesteld om door middel van een interesseprofiel aan te geven in welke overheidspublicaties hij is geïnteresseerd. In een dergelijk profiel kan worden aangegeven van welke bestuursorganen men informatie gepresenteerd wil zien, welke soorten publicaties het betreft en op welke locatie of welk gebied de publicaties betrekking moeten hebben. Zo is het mogelijk om een straal op te geven van bijvoorbeeld 250, 500 of 1000 meter rond een woonadres en aan te geven dat men alle bekendmakingen, mededelingen en kennisgevingen van (ontwerp-)besluiten wil ontvangen die betrekking hebben op een object dat binnen deze straal valt. Zolang de gebruiker nog geen persoonlijk profiel heeft ingesteld, worden hier de bekendmakingen, mededelingen en kennisgevingen getoond die betrekking hebben op de directe woonomgeving. Daartoe wordt met behulp van het actuele woonadres van de gebruikers van MijnOverheid uit de basisregistratie personen (hierna: BRP) een overzicht gepresenteerd van berichten die betrekking hebben op het gebied dat valt binnen een bepaalde straal rond dit woonadres. Daarnaast zal het, net als bij de berichtenbox van MijnOverheid, mogelijk zijn om per e-mail geattendeerd te worden op nieuwe bekendmakingen, mededelingen en kennisgevingen die vallen binnen het vastgestelde profiel (notificatie). Gebruikers, waarvan het e-mailadres bekend is, zullen automatisch op relevante berichten worden geattendeerd, met de mogelijkheid om deze service te beëindigen (*opt-out*). Om nieuwe publicaties doelmatig te kunnen matchen met het interesseprofiel van de gebruikers zal het adres van alle personen met een actief MijnOverheid-account worden opgeslagen (zie ook artikel 13) en worden geactualiseerd aan de hand van de adresgegevens in de BRP. Daarnaast worden ten behoeve van deze dienst het BSN, de geboortedatum en het e-mailadres gebruikt.[8] Voor de diensten Persoonlijke gegevens en Algemene bekendmakingen, kennisgeving en mededelingen worden meer persoonsgegevens verwerkt dan voor het enkele gebruik van een account van MijnOverheid en de dienst informatieverschaffing Lopende Zaken. In artikel 4, onder b, sub 7° en 8°, is aangegeven welke gegevens dit kan betreffen.

4.1.3. Persoonsgegevens toegelaten privaat middel voor burgers

Omwille van de continuïteit en brede beschikbaarheid van de toegang tot overheidsdienstverlening door burgers, biedt de Wet digitale overheid Onze Minister de mogelijkheid om, naast het publieke identificatiemiddel op meerdere betrouwbaarheidsniveaus (DigiD), ook private identificatiemiddelen toe te laten. Wanneer aan de (bij lagere regelgeving) te stellen eisen wordt voldaan, kan voor deze private middelen een erkenning worden verkregen (artikel 9, tweede lid ev., Wet digitale overheid). Hiermee krijgen burgers (natuurlijke personen) de keuze tussen gebruik van een publiek of privaat identificatiemiddel.

Voor zover het de private (commerciële) werking van een dergelijk identificatiemiddel betreft (bijvoorbeeld om *online* aankopen bij een webwinkel te doen) vallen de verwerkingen van persoonsgegevens buiten de werkingssfeer van het publieke domein en daarmee buiten dit besluit. Voor zover persoonsgegevens worden verwerkt waarvoor een wettelijk grondslag benodigd is of de verwerking direct verbonden is aan, of ontstaan door het gebruik het publieke domein, zoals gegevens over het gebruik van een middel door een burger in het publieke domein, wordt dit in het besluit geregeld. Uitgangspunt bij de regulering van gegevensverwerking ter zake van het toegelaten private

[7] Met deze wet is de Bekendmakingswet gewijzigd, *Kamerstukken II*, 2018/19, 35 218.
[8] Voor een nadere toelichting zie de Memorie van Toelichting bij het wetsvoorstel Elektronische Publicaties, *Kamerstukken II*, 2018/19, 35 218, nr. 3.

middel is dat sprake is van een gelijkwaardige werking en een gelijkwaardig beschermingsniveau als het publieke identificatiemiddel. Een toe te laten privaat middel dient immers een volwaardig alternatief voor burgers te bieden en dient hen toegang te bieden tot elektronische dienstverlening in het publieke domein.

4.1.4. Persoonsgegevens bedrijfs- en organisatiemiddel

Teneinde bedrijven de mogelijkheid te bieden om toegang te verkrijgen tot elektronische dienstverlening in het publieke domein – overheden verlenen immers elektronische diensten aan burgers én bedrijven –, zullen private partijen elektronische identificatiemiddelen ontwikkelen en daarbij betrokken diensten aanbieden. Deze partijen, alsmede de door hen te ontwikkelen zogenoemde bedrijfs- en organisatiemiddelen, dienen ingevolge het wetsvoorstel digitale overheid door de minister te worden erkend. De betreffende partijen verwerken persoonsgegevens zover dit noodzakelijk is voor de werking van het bedrijfs- en organisatiemiddel en goede en veilige toegang met dat middel tot elektronische dienstverlening. Hiertoe biedt het wetsvoorstel de grondslag. In het onderhavige besluit wordt nader geregeld welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Het betreft dus een nieuw onderdeel in het besluit; het Besluit verwerking persoonsgegevens generieke digitale infrastructuur bevat immers geen bepalingen over gegevensverwerking door private partijen en over de toegang door bedrijven tot elektronische diensten van de (semi)overheid. Het betreft met name gegevens over de gebruiker van een erkend bedrijfs- en organisatiemiddel, zijnde een onderneming of rechtspersoon of een natuurlijke persoon die deze onderneming of rechtspersoon vertegenwoordigt (zie artikel 1). Bij overheidsdienstverlening aan bedrijven is een veelheid aan (private) partijen met verschillende rollen en werkzaamheden betrokken, waarbij bovendien relaties bestaan met publieke voorzieningen. Dit geteld bij het feit, dat het bij handelen door bedrijven naar zijn aard niet alleen gaat om identificatie (‘wie ben je’) en authenticatie (‘ben je wie je zegt te zijn’) maar ook om autorisatie (‘wat mag je’, ‘waartoe ben je bevoegd’), brengt mee dat er relatief veel gebruik(er)sgegevens (waaronder burgerservicenummer en *track record*) worden verwerkt teneinde veilige en betrouwbare toegang te kunnen realiseren.

De procedure die voor het aanvragen van een bedrijfs- of organisatiemiddel moet worden doorlopen, is op hoofdlijnen als volgt. Een machtigingsdienst identificeert de hoofdvertegenwoordiger van een bedrijf of organisatie volgens de eisen die bij of krachtens de wet zijn gesteld aan het gewenste betrouwbaarheidsniveau. De gegevens van de hoofdvertegenwoordiger van een bedrijf of organisatie worden daarbij gecontroleerd bij de Kamer van Koophandel op basis van (onder andere) het bij de aanvraag opgegeven nummer van de Kamer van Koophandel van het bedrijf of de organisatie. Bij eenmanszaken is de eigenaar zelf hoofdvertegenwoordiger en zal bij de Kamer van Koophandel enkel het nummer van de Kamer van Koophandel worden gecontroleerd. Indien gewenst kan de machtigingsdienst ook het burgerservicenummer van de eigenaar van diens WID overnemen en (met naam en geboortedatum) bij het BSN-K laten activeren. Een medewerker (of eigenaar) van een bedrijf of organisatie vraagt zelf een persoonlijk middel aan bij een middelenuitgever via een uitgifteproces dat ook weer voldoet aan de eisen die bij of krachtens de wet zijn gesteld voor het aangevraagde betrouwbaarheidsniveau. Bij een machtigingsdienst (meestal dezelfde partij als de middelenuitgever) zal de hoofdvertegenwoordiger vervolgens de betreffende medewerker machtigen op een specifiek betrouwbaarheidsniveau om namens het bedrijf of de organisatie het middel te mogen gebruiken voor een elektronische dienst of diensten. Dit kan ook een machtiging zijn om (als machtigingsbeheerder) namens het bedrijf of de organisatie machtigingen aan medewerkers te autoriseren en beheren. Dan hoeft de hoofdvertegenwoordiger dit niet zelf te doen. Als alle verificaties zijn geslaagd, kan de middelenuitgever overgaan tot verstrekking van het middel aan de hoofdvertegenwoordiger en, indien van toepassing, de medewerkers van een bedrijf of organisatie.

Bij het gebruik van het middel gaat de gebruiker naar de website van de dienstverlener waar hij een elektronische dienst wil afnemen. Op de website geeft hij aan welk bedrijfs- of organisatiemiddel hij wil gebruiken om in te loggen en op dat moment wordt op de achtergrond via de ontsluitende dienst waarmee de dienstverlener een overeenkomst heeft gesloten, contact gelegd met achtereenvolgens de authenticatiedienst en de machtigingsdienst die horen bij het te gebruiken middel. Bij de authenticatiedienst vindt dan het feitelijke inlogproces plaats, waarna de authenticatiedienst - bij geslaagde verificaties en validaties - de identiteit van de gebruiker bevestigt aan de dienstverlener (bestuursorgaan of aangewezen organisatie). Via de machtigingsdienst wordt vervolgens aan de

dienstverlener al dan niet bevestigd of de betreffende gebruiker voor de betreffende dienst namens het bedrijf of de organisatie mag optreden.

Ten slotte kan het bedrijfs- of organisatiemiddel ook worden gebruikt voor elektronische identificatie ter zake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie door tussenkomst van de eIDAS-voorziening.

Uit de bovenstaande beschrijving van de processen bij de aanvraag en uitgifte en bij het gebruik van een bedrijfs- of organisatiemiddel, blijkt dat het noodzakelijk is voor de werking van het middel dat de diverse daarbij betrokken partijen onderling gegevens uitwisselen. Afhankelijk van welke stap in het proces van aanvraag of uitgifte van een middel of welke stap in het proces van gebruik van het middel aan de orde is, worden de daarvoor minimaal noodzakelijke gegevens vertrekt van de ene aan de andere dienst. De gegevens worden steeds een op een verstrekt. Door in het besluit te bepalen dat alleen gegevens aan elkaar mogen worden verstrekt voor zover dat noodzakelijk is voor de werking van het bedrijfs- en organisatiemiddel, wordt de in het kader van de AVG vereiste dataminimalisatie bereikt.

Naast de voor de werking van het bedrijfs- of organisatiemiddel vereiste een-op-een-verstrekkingen tussen de betrokken partijen, worden in twee gevallen gegevens verstrekt aan anderen. Ten eerste verstrekt de ontsluitende dienst gegevens ten behoeve van de vaststelling van de identiteit van de gebruiker van het middel aan de dienstverlener (“afnemer” in de zin van dit besluit) waarmee hij een overeenkomst heeft gesloten om als ontsluitende dienst op te treden. Ten tweede worden, conform de eIDAS-verordening, door alle partijen de zogenaamde eIDAS-gegevens verstrekt in versleutelde vorm ter identificatie van bedrijven.

4.1.5. Persoonsgegevens BSN-K

De hiervoor genoemde verwerking met pseudoniemen binnen de voorzieningen voor elektronische toegang wordt mogelijk gemaakt door het BSN-koppelregister (BSN-K). De voorziening wijzigt daarmee wat betreft de functionaliteit ten opzichte van de huidige inrichting, die als een vertaalregister functioneerde.

De nieuwe functionaliteit van de voorziening maakt het mogelijk om identificatiemiddelen bij aanmelding voor toegang tot een dienstaanbieder een pseudoniem (burgerservicenummer in afgeleide vorm) of een polymorfe identiteit (burgerservicenummer in versleutelde vorm) toe te kennen, dat wordt gebruikt bij de identificatie bij dienstaanbieders (authenticatiefunctie). Hierdoor wordt het gebruik van het BSN geminimaliseerd.

De inrichting van het BSN-K is zodanig dat bij de koppeling tussen het private en het publieke domein geen koppeling gemaakt kan worden tussen pseudoniem en burgerservicenummer. Bij gebruik van het BSN-K binnen het publieke domein kan de polymorfe identiteit via ontsleuteling worden herleid door de dienstaanbieder die op grond van de wet het burgerservicenummer mag verwerken. De afgeleide vorm wordt gebruikt in het private domein, bij diensten waarvoor geen BSN verwerkt mag worden. De afgeleide vorm bevat namelijk geen BSN.
Door versleuteling en pseudonimisering ontstaat er geen onwenselijke concentratie van persoonsgegevens. Er wordt eenmalig een pseudoniem of polymorfe identiteit aangemaakt, waarna geen burgerservicenummer meer wordt opgeslagen. Vanuit privacy-oogpunt is dit zowel vanuit oogpunt van pseudonimisering als vanuit dataminimalisatie een belangrijke verbetering. De verwerking van persoonsgegevens voor deze voorziening die daarvoor nodig is, verandert daardoor uiteraard mee. Gelet daarop wordt ook het bepaalde inzake het BSN-K gewijzigd.

4.1.6. Persoonsgegevens routeringsvoorziening

Beleidsuitgangspunt en wens van overheidsdienstverleners is om op eenvoudige wijze en eenmalig op de voorzieningen voor elektronische toegang te kunnen aansluiten. Daartoe wordt ingevolge de wet digitale overheid een nieuwe voorziening ingericht, de routeringsvoorziening, waarvoor Onze Minister verantwoordelijk is. De routeringsvoorziening heeft tot doel (semi-)publieke dienstverleners te ‘ontzorgen’ in hun aansluiting op wettelijk verplichte authenticatielandschappen (DigiD, DigiD Machtigen, erkende bedrijfs- en organisatiemiddelen, eIDAS, etc.). De routeringsvoorziening biedt de

afnemer/dienstverlener hiertoe één koppelvlak, één aanspreekpunt en één factuur. De routeringsvoorziening voorziet hierin door te fungeren als tussenpartij die elektronisch berichtenverkeer met de authenticatielandschappen enerzijds vertolkt naar de dienstverlener anderzijds. Technisch bestaat de routeringsvoorziening uit één of meerdere publieke en mogelijk één of meerdere private routeringsdiensten. Omdat de routeringsvoorziening een centrale functie vervult tussen de authenticatiediensten en de afnemers, is het noodzakelijk dat deze voorziening, gelet op het technisch afhandelen en doorgeleiden van authenticaties, al dan niet gepseudonimiseerde persoonsgegevens verwerkt van gebruikers die bij een dienstverlener willen inloggen met een toegelaten publiek of privaat identificatiemiddel. Het Besluit voorziet in nadere regulering van de persoonsgegevens die het betreft.

4.1.7. Persoonsgegevens eIDAS-voorziening

De Minister is verantwoordelijk voor een voorziening die het mogelijk maakt identificatiemiddelen te ontsluiten waarmee natuurlijke personen, ondernemingen en rechtspersonen uit andere EU-lidstaten toegang willen tot elektronische dienstverlening in Nederland en vice versa (artikel 5, tweede lid, van de wet). Achtergrond hiervan is dat de bovenliggende eIDAS-verordening verplicht tot wederzijdse erkenning van elektronische identificatiemiddelen op de niveaus substantieel en hoog. Binnen de eIDAS-voorziening is sprake van een aantal functionaliteiten en componenten. Doel ervan is het mogelijk maken van elektronische dienstverlening aan diegenen in de EU of EER die niet (kunnen) beschikken over een toegelaten of erkend middel als bedoeld in de wet digitale overheid maar die, bijvoorbeeld vanwege werk of onderwijs, een relatie hebben met een of meerdere publieke dienstverlener(s) in Nederland (inkomend verkeer). Kortgezegd dient de eIDAS-voorziening er dan toe iemand op basis van buitenlandse persoonsgegevens te herkennen. Het systeem voorziet daarom in een – onder de verantwoordelijkheid van de minister uitgevoerde - koppeling van uit een andere lidstaat binnenkomende gegevens aan een burgerservicenummer en een versleutelde vormen afgeleide vorm daarvan. Alleen indien en voor zover met dit proces geen zekerheid omtrent uniciteit kan worden verkregen, worden aanvullende gegevens verwerkt (dataminimalisatie). Ook voor wat betreft uitgaand verkeer heeft deze voorziening een functie: Nederlandse identificatiemiddelen worden ontsloten op een voor openbare instanties in andere lidstaten toegankelijke wijze, doordat de eIDAS-voorziening voor elke persoon een landspecifiek uniek identificerend nummer levert.

4.2 Informatieveiligheid; werkingssfeer en verhouding tot praktijk

De informatieveiligheidsbepalingen, opgenomen in het nieuwe hoofdstuk 5 van het onderhavige Besluit, dienen ter uitvoering van artikel 4 van de voorgenomen wet Digitale overheid, dat luidt:

> 1. Bestuursorganen en aangewezen organisaties voldoen aan bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten op verschillende betrouwbaarheidsniveaus.
> 2. Bestuursorganen en aangewezen organisaties overleggen aan Onze Minister een verklaring van een auditor waaruit blijkt of zij voldoen aan de in het eerste lid bedoelde regels.
> 3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de wijze waarop bestuursorganen en aangewezen organisaties aantonen dat zij aan de regels, bedoeld in het eerste lid, voldoen.

Doel is een verplichtend kader te realiseren voor dienstverleners in de relevante beleidsdomeinen. De huidige regels zijn, meer of minder uitgebreid, vindbaar in diverse generieke en sectorspecifieke documenten, die op verschillende (semi)overheidsniveaus worden gehanteerd en bovendien een grote overlap vertonen, bijvoorbeeld de *Baseline* Informatiebeveiliging Rijksdienst (BIR), *Baseline* Informatiebeveiliging Gemeenten (BIG)[9], de aansluitvoorwaarden inzake diverse gdi-voorzieningen (oa DigiD) en de ICT-beveiligingsrichtlijnen van het NCSC. Deze documenten[10] zijn richtinggevend en daarmee in zekere zin vrijblijvend van aard; ze hebben de status van beleidsregels of richtsnoeren,

[9] Deze zijn vervangen door de Baseline Informatieveiligheid Overheid BIO (*Kamerstukken II* 2018/19, 26 643, nr 574. De BIO, een circulaire, vervangt de bestaande *baselines* informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Hiermee is één gezamenlijk normenkader voor informatiebeveiliging ontstaan binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.
[10] Ze behelzen regels op strategisch, tactisch en/of operationeel niveau.

dan wel maken ze onderdeel uit van door dienstverleners met de minister gesloten privaatrechtelijke overeenkomsten. Teneinde, in aansluiting op de formeelwettelijke grondslag in de wet Digitale Overheid, duidelijkheid en rechtszekerheid te scheppen, liggen algemeen verbindende regels in de rede. Om dit te bewerkstelligen zijn de bepalingen in hoofdstuk 5 van dit Besluit gedestilleerd uit de in de praktijk gehanteerde documenten. Met dit Besluit is dus sprake van stroomlijning en codificering; materieel gaan er niet of nauwelijks nieuwe verplichtingen gelden. Hierdoor kunnen naar verwachting de administratieve lasten en kosten (regeldruk) voor dienstverleners beperkt blijven. Zie nader punt 6 van deze toelichting.

De bepalingen in hoofdstuk 5 richten zich tot bestuursorganen en aangewezen organisaties in de zin van de wet, oftewel dienstverleners. Zij moeten de bepalingen van hoofdstuk 5 in acht nemen bij het verlenen van toegang tot hun elektronische dienstverlening (elektronische identificatie). De werkingssfeer van de bepalingen is dus beperkt en ziet niet op informatieveiligheid van de identificatiemiddelen en generieke voorzieningen en ook niet op informatieveiligheid van de elektronische dienstverlening van de dienstverleners zelf. Het primaire proces is hun eigen verantwoordelijkheid. Omdat sprake is van samenhangende processen (ketens) tussen verschillende componenten van de digitale overheid en andere dienstverleners, zullen dienstverleners niettemin de intern te hanteren regels op elkaar (moeten) afstemmen. Dat is niet problematisch, omdat ook bij het primaire proces de hierboven genoemde documenten een rol spelen – zij het dat die niet algemeen verbindend zijn. Met uitzondering van de privaatrechtelijke documenten met informatiebeveiligingsvoorschriften inzake toegang, die zullen opgaan in het onderhavige Besluit,[11] blijven de andere documenten, zoals de *baselines*, voorschriften beveiliging rijksdienst (VIR) en ICT-beveiligingsrichtlijnen, gewoon bestaan. Zoals gezegd hebben deze een ruimere werkingssfeer; ze zien op informatieveiligheid van de dienstverleners in den brede, dus ook buiten toegangsverlening. Voor wat betreft toegangsverlening zullen ze (blijven) functioneren als handvatten bij de praktische vormgeving en toepassing van de – bindende – kaders in dit Besluit.

De informatiebeveiligingsbepalingen in dit Besluit zijn doel- oftewel resultaatsverplichtingen. Met de opzet en formulering ervan wordt een evenwicht gevonden tussen enerzijds normerend en toetsbaar zijn (houvast bieden) gelet op de veiligheid in de keten, en anderzijds ruimte laten. Hierdoor worden dienstverleners in staat gesteld maatwerk te realiseren die past bij de inrichting van hun dienstverlening. Op deze wijze wordt recht gedaan aan de systeemverantwoordelijkheid van de Minister van BZK en aan de verantwoordelijkheid die dienstverleners voor hun eigen bedrijfsvoering hebben.

5 Privacy en verhouding tot algemene verordening gegevensbescherming

In de memorie van toelichting bij het wetsvoorstel digitale overheid[12] is uitgebreid ingegaan op de privacy-aspecten, en wel met name in het licht van de AVG. De AVG werkt rechtstreeks en in dat verband bevat dit besluit enkel bepalingen die aanvullend zijn op of uitwerking vormen van de waarborgen van de AVG ten aanzien van de bescherming van persoonsgegevens. Andersom is het zo, dat voor alles wat dit besluit niet regelt over de verwerking van persoonsgegevens in het kader van toegang tot elektronische dienstverlening, de bepalingen van de AVG gelden, zoals voorschriften over transparantie en recht van inzage en rectificatie. De diverse aspecten van de bescherming van persoonsgegevens in verband met dit besluit, zullen hieronder nader worden toegelicht.

<u>Grondslag voor verwerking</u>
De grondslag voor de gegevensverwerking ten aanzien waarvan dit besluit regels stelt over de verstrekkingsmogelijkheden en bewaartermijnen is gelegen in artikel 16 van de wet digitale overheid. In dat artikel zijn de doelen van de gegevensverwerking vastgelegd. Daarmee is de verwerking rechtmatig op grond van de in artikel 6, eerste lid, onder e, van de AVG genoemde rechtsgrond (verwerking noodzakelijk voor de vervulling van een taak van algemeen belang), artikel 6, eerste lid,

[11] Tot op heden worden tussen Onze Minister (Logius) en dienstverleners overeenkomsten gesloten die de aansluiting op publieke voorzieningen, behorend tot de generieke digitale infrastructuur, tot onderwerp hebben. Nu aansluiting op de voorzieningen die een rol spelen bij de toegang tot elektronische dienstverlening (artikel 5, eerste en tweede lid jo. artikelen 7 en 13 van de Wet digitale overheid) niet langer vrijblijvend is, moeten de dienstverleners aan algemeen verbindende voorschriften inzake onder meer informatieveiligheid en de verwerking van persoonsgegevens voldoen. Hiermee komen de overeenkomsten ter zake te vervallen.
[12] *Kamerstukken II* 2017/18, 34 972, nr. 3, paragraaf 4.

onder c AVG (verwerking noodzakelijk om te voldoen aan een wettelijke plicht) in samenhang met artikel 6, derde lid, onder b (bedoelde rechtsgrond moet worden vastgelegd bij lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is).

Een andere verwerkingsgrond is relevant in verband met de mogelijkheid om een bedrijfsmiddel te gebruiken als middel voor elektronische identificatie van een gemachtigde (zie par. 4.1.1.). Bij de registratie van die machtigingsrelatie tussen een burger en een onderneming in DigiD Machtigen kan sprake zijn van de verwerking van bijzondere categorieën van persoonsgegevens in de zin van de AVG. Daarvan kan bijvoorbeeld sprake zijn als een burger lid is van een vakbond, die vakbond machtigt om te helpen bij het doen van belastingaangifte en de vakbond het beleid heeft om deze hulp uitsluitend aan leden te verlenen. In die situatie kan namelijk uit de registratie van de machtiging blijken dat iemand lid is van de betreffende vakbond. Hetzelfde kan gelden voor bijvoorbeeld kerkelijke organisaties of belangengroeperingen die zich inspannen om hun leden te helpen en daarvoor gemachtigd worden. Uit de machtigingsrelatie, maar ook uit de dienst waarvoor gemachtigd is, zoals inzage in de berichtenbox van het CIZ, kan dan een specifieke connectie of indicatie van bijzondere omstandigheden (bijvoorbeeld gezondheidsklachten/zorgbehoefte) worden afgeleid. Voor die situaties geldt het verbod om bijzondere categorieën van persoonsgegevens te verwerken, tenzij de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang (artikel 9, tweede lid, onderdeel g, van de AVG).

Ingevolge het wetsvoorstel tot wijziging van de Awb inzake modernisering elektronisch bestuurlijk verkeer[13] krijgen burgers en bedrijven het recht op elektronisch zakendoen met de overheid. Op grond van het wetsvoorstel Digitale overheid zal het bestuursorgaan, de aangewezen organisatie of een rechterlijke instantie, voor zover het gaat om dienstverlening waarvoor het betrouwbaarheidsniveau substantieel of hoog geldt, deze dienstverlening aan burgers alleen kunnen aanbieden met gebruik van (voor burgers) toegelaten identificatiemiddelen, door de Minister van BZK afgegeven elektronische verklaringen waaruit blijkt dat een natuurlijke persoon of rechtspersoon gemachtigd is namens een natuurlijke persoon op te treden bij de toegang tot elektronische dienstverlening of erkende bedrijfs- en organisatiemiddelen (indien en voor zover die worden gebruikt in de toegang van een door de burger gemachtigde houder die met dat middel handelt namens een onderneming of rechtspersoon) (artikel 7 van het wetsvoorstel Digitale overheid). Ook artikel 2:1 van de Algemene wet bestuursrecht is hier relevant, op grond waarvan eenieder zich ter behartiging van zijn belangen in het verkeer met bestuursorganen kan laten bijstaan of door een gemachtigde laten vertegenwoordigen. De Minister van BZK heeft de taak om dat recht op vertegenwoordiging tegenover bestuursorganen, aangewezen organisaties en rechterlijke instanties met elektronische toegangsdiensten te waarborgen (artikel 5 van het wetsvoorstel Digitale overheid). Als een burger een dergelijke machtiging wil registreren, dan is het verwerken van informatie over de gemachtigde daar onlosmakelijk mee verbonden en aldus noodzakelijk om de machtiging te laten functioneren. Daar komt bij, dat de verwerking van informatie over de gemachtigde ook noodzakelijk is op grond van het in artikel 15 van de AVG vastgelegde recht van de burger op inzage van de persoonsgegevens die over hem worden verwerkt. Daar hoort bij dat de burger kan inzien of en zo ja, wie hij heeft gemachtigd om namens hem elektronische diensten af te nemen, zodat hij dit zo nodig kan controleren en maatregelen kan treffen als hij een onjuistheid constateert. Aan de (overige) voorwaarden die de AVG in artikel 9, tweede lid, onderdeel g, stelt is overigens ook voldaan. De verwerking is gebaseerd op het wetsvoorstel Digitale overheid. De evenredigheid met het nagestreefde doel is gewaarborgd, omdat de verwerking uitsluitend geschiedt indien de burger er zelf voor kiest om een bepaalde organisatie te machtigen en de verwerking vervolgens uitsluitend geschiedt om die machtiging veilig en naar de burger transparant te laten werken. De wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt om diezelfde reden ook geëerbiedigd, waarbij komt dat het doel van de verwerking nadrukkelijk niet is om onderscheid te maken tussen burgers op basis van de door hen gemachtigde organisaties. Er worden ten slotte passende en specifieke maatregelen getroffen ter bescherming van de grondrechten en fundamentele belangen van de betrokkene, zoals dat voor alle verwerking van persoonsgegevens onder het wetsvoorstel digitale overheid gebeurt in overeenstemming met de bij of krachtens dat wetsvoorstel opgestelde regels over informatieveiligheid.
De grondslag om de bedoelde gegevens over bijvoorbeeld vakbonden te verwerken, kan vervolgens worden gevonden in artikel 6, eerste lid, onderdeel c, de verwerking is namelijk noodzakelijk om te

[13] *Kamerstukken II* 2018/19, 35 261.

voldoen aan een wettelijke verplichting die op de minister van BZK rust op grond van het wetsvoorstel digitale overheid.

Wat betreft de verwerking van het burgerservicenummer bevat de AVG een grondslag in artikel 87 om bij nationaal recht specifieke voorwaarden te stellen voor de verwerking van een nationaal identificatienummer. De Uitvoeringswet AVG[14] regelt het gebruik van wettelijk voorgeschreven nummers, overeenkomend met het huidige artikel 24 van de Wbp. Dit betekent dat voor de verwerking van het burgerservicenummer dient te worden voorzien in een wettelijke grondslag. In het algemeen biedt de Wet algemene bepalingen burgerservicenummer die grondslag. In aanvulling daarop is in de Wet digitale overheid opgenomen dat het burgerservicenummer door de genoemde betrokkenen mag worden verwerkt voor zover dat noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge die wet. Daarbij geldt dat gebruik van het burgerservicenummer tot een minimum wordt beperkt en zoveel mogelijk wordt gewerkt met pseudonimisering en polymorfe identiteiten (afgeleide en versleutelde, zie paragrafen 4.1.1. en 4.1.5.). Gelet op het voorgaande is de verwerking van het burgerservicenummer in overeenstemming met de AVG.

Proportionaliteit en subsidiariteit

Zoals aangegeven in de memorie van toelichting bij het wetsvoorstel, zijn onder meer de beginselen van proportionaliteit en subsidiariteit leidend geweest bij de totstandkoming van dit besluit.

Wat betreft de eis van proportionaliteit – weegt de privacyinbreuk op tegen de effecten voor burgers - bevat het besluit de nodige bepalingen die waarborgen dat er geen verdergaande inmenging plaatsvindt met het recht van betrokkene dan noodzakelijk is. Het besluit is het resultaat van een zorgvuldige afweging tussen het belang van de overheid bij een doelmatige invulling van de zorgplicht die bij haar is neergelegd in de Wet digitale overheid enerzijds en de bescherming van de persoonlijke levenssfeer van de gebruikers anderzijds. Dit uit zich in de eerste plaats in het feit dat de verwerking van persoonsgegevens beperkt is tot zo min mogelijk gegevens en alleen tot die gegevens van de burger die echt essentieel zijn om de voorzieningen beschikbaar te kunnen stellen, in stand te kunnen houden, te laten werken en beveiligen en betrouwbaar te houden. Het burgerservicenummer speelt hierbij een cruciale rol. Voor zover afnemers van de voorzieningen meer persoonsgegevens van de betreffende burger nodig hebben, zullen zij die via andere wegen moeten verkrijgen. Doorgaans zullen afnemers de voor hen noodzakelijk gegevens die behoren bij een bepaald BSN (dat zij bijvoorbeeld in het kader van het gebruik van een burger van DigiD of een via het BSN-K gevalideerd authenticatiemiddel verstrekt krijgen), verstrekt kunnen krijgen uit de basisregistratie personen (BRP), mits uiteraard zij op grond van de Wet basisregistratie personen in aanmerking komen voor verstrekking van bepaalde gegevens uit de BRP. Op die manier is het aantal persoonsgegevens dat in het kader van de bedoelde voorzieningen wordt verwerkt, grotendeels beperkt tot het burgerservicenummer en bijbehorende gebruiks- en accountgegevens.

In het algemeen deel en het artikelsgewijze deel van deze nota van toelichting is uitgebreid ingegaan op de noodzaak en de wijze van de verwerking van de nieuwe gegevens die als gevolg van dit besluit in de bestaande voorzieningen en in nieuwe voorzieningen zullen worden gebruikt. De proportionaliteit van de gegevensverwerking valt ook af te leiden uit de bepalingen over de bewaartermijnen van de gegevens, waarbij de bewaartermijn duidelijk is onderbouwd en beperkt tot het doel van de verwerking. Ook is duidelijk vastgelegd aan wie welke gegevens mogen worden verstrekt. De desbetreffende bepalingen waarborgen dat gegevens niet langer worden bewaard en niet meer gegevens worden verstrekt dan noodzakelijk.

Wat betreft de eis van subsidiariteit - zijn er nog andere manieren om het doel te bereiken - is, gelet op de beleidsuitgangspunten[15] bij de ontwikkeling en het beheer van de generieke digitale infrastructuur, gekozen voor een opzet, inrichting en samenstel van (ICT-) producten en diensten voor de digitale overheid, waaronder inlogmiddelen voor burgers, waarbij de verwerking van persoonsgegevens zo minimaal mogelijk is en met de minst mogelijke risico's. Alternatieven zouden tot een omvangrijkere verwerking van meer persoonsgegevens hebben geleid. Dit blijkt ook uit de uitgevoerde *privacy impact assessments.*

[14] Stb. 2018, 144.
[15] Zie MvT bij het bovenliggende wetsvoorstel *Kamerstukken II* 2017/18, 34 972, nr. 3.

Transparantie
In de memorie van toelichting bij het wetsvoorstel digitale overheid[16] is aangegeven dat in hoofdstuk III van de AVG transparantievoorschriften zijn opgenomen, waarbij onderscheid wordt gemaakt tussen het geval dat de verkrijging van de gegevens bij de burger zelf plaatsvindt (artikel 13 AVG) en dat waarbij de gegevens niet bij hem zijn verkregen (artikel 14 AVG). Ingevolge de wet en de bijbehorende uitvoeringsregelgeving vindt het verkrijging van de gegevens op beide wijzen plaats en voor dit besluit geldt hetzelfde. Zo verstrekt de burger zelf bepaalde informatie als hij DigiD aanvraagt. En er is sprake van informatie die buiten de burger om wordt verkregen, bijvoorbeeld gegevens die nodig zijn om de juistheid van gegevens te controleren, zoals de controle van de identiteit door het BSN-K, in het kader van de toegang tot elektronische dienstverlening. Aan de transparantieverplichtingen zal door de minister en andere betrokkenen worden voldaan door een privacyverklaring op hun website te plaatsen, waarin onder andere staat wie de verantwoordelijke is voor de verwerking van persoonsgegevens en met welk doel de persoonsgegevens worden verwerkt. Ook zal op de websites een link worden opgenomen naar de bijbehorende wet- en regelgeving, waaronder dit besluit.

Het recht van inzage en rectificatie
Zoals in de memorie van toelichting bij het wetsvoorstel[17] is aangegeven, heeft een burger op grond van artikel 15 AVG het recht om te weten welke persoonsgegevens door de verantwoordelijke worden verwerkt, onder meer voor welke doeleinden en aan welke personen of instanties deze gegevens zijn verstrekt. Op grond van de artikelen 16 tot en met 18 AVG heeft hij het recht de verantwoordelijke te verzoeken hem betreffende gegevens te rectificeren, gegevens te wissen, of de verwerking te beperken. De wijze waarop uitvoering wordt gegeven aan deze rechten zal, wat betreft de voorzieningen in dit besluit onder de verantwoordelijkheid van de Minister van BZK, worden vastgelegd in op te stellen privacyverklaringen die op de betrokken websites zullen worden geplaatst. Het moet hierbij gaan om meer dan een algemeen *privacy statement,* algemene disclaimer of een enkele verwijzing naar elders verkrijgbare informatie. Om aan de informatieverplichting in de AVG (artikelen 13 en 14) te voldoen moet sprake zijn van een specifieke, zichtbare en toegankelijke verklaring. Vanzelfsprekend geldt voor bestuursorganen en aangewezen organisaties dat de AVG rechtstreeks van toepassing is voor wat betreft (inzage en rectificatie van) de gegevens waar zij verantwoordelijk voor zijn.
Privacy impact assessments
Gedurende het proces om te komen tot elektronische identificatie ter zake van de toegang tot dienstverlening in het publieke domein ('eID-stelsel') is meerdere malen een *privacy impact assessment* (PIA) uitgevoerd. De uitkomsten daarvan hebben tot technische en organisatorische aanpassingen geleid en zijn verwerkt in regelgeving. Conform artikel 35 AVG zullen ook in de toekomst met regelmaat PIA's worden opgesteld (het betreft een voortdurend proces) en zullen waar nodig de resultaten ervan hun beslag krijgen. In dit verband zij tevens verwezen naar hoofdstuk 4 van het algemeen deel van de memorie van toelichting bij het wetsvoorstel digitale overheid.

6 Gevolgen en uitvoerbaarheid (incl. regeldruk)

6.1 Verwerking persoonsgegevens

De gegevensverwerkingsbepalingen in dit Besluit vinden hun grondslag in artikel 16 van de wet. De bepalingen richten zich voor het overgrote deel tot de minister, als verantwoordelijke voor de (publieke, ICT-) voorzieningen en de daarin plaatshebbende gegevensverwerking. Hij is degene die in dit verband de technische, organisatorische en bestuurlijke lasten en kosten draagt, zij het dat ingevolge het wetsvoorstel doorbelasting zal plaatsvinden aan de dienstverleners.
Voor een deel richten de gegevensverwerkingsbepalingen in dit Besluit zicht tot aanbieders van private diensten die in aanmerking willen komen voor erkenning ingevolge de wet. Ook deze gegevensverwerkingsbepalingen hebben hun basis in het wetsvoorstel. Het Besluit behelst een specificatie daarvan. Gevolg is dat deze private partijen hiermee bij hun (technische en organisatorische) inrichting rekening moeten houden, met de financiële aspecten van dien.

[16] *Kamerstukken II* 2017/18, 34 972, nr. 3, paragraaf 4.
[17] *Kamerstukken II* 2017/18, 34 972, nr. 3, paragraaf 4.

6.2 Informatieveiligheid

De informatieveiligheidsbepalingen in dit Besluit, welke de uitwerking vormen van artikel 4 van de wet, behelzen voor het overgrote deel van de dienstverleners niets nieuws. Omdat hun informatiebeveiliging reeds via generieke en/of sectorspecifieke *baselines* is 'gereguleerd' alsmede vanwege het feit, dat ze in het kader van de toegang tot hun elektronische dienstverlening reeds zijn aangesloten op DigiD, zijn zij namelijk al bekend met de in dit Besluit voorgeschreven (doel)maatregelen, risicomanagement en het laten uitvoeren van *audits* en *assessments.* Ze zijn technisch en organisatorisch al aangesloten op de voor hen relevante (landelijke) voorzieningen, hebben passende ICT-systemen beschikbaar en hebben informatie-uitwisseling ingericht. Het Besluit betreft voor hen primair een voortzetting van de huidige praktijk en wordt in dat verband uitvoerbaar geacht. Wel is sprake van een veranderde status van de regels: de te nemen maatregelen zijn niet langer vrijblijvend, maar worden door de publiekrechtelijke inkadering (juridisch) bindend. Hierdoor zullen dienstverleners zich naar verwachting meer bewust worden van de noodzaak om, met betrekking tot de toegang tot hun elektronische diensten, informatieveiligheidsbeleid en –maatregelen te realiseren en hun processen zorgvuldig in te richten, mede gelet op de verplichting om hierover jaarlijks te rapporteren. Dat dienstverleners bij de invulling en vormgeving van de te nemen maatregelen de nodige ruimte hebben, zal naar verwachting behulpzaam zijn bij de uitvoering en de uitvoerbaarheid.
Voor dienstverleners die (nog) niet gewend zijn te werken met de materie zoals neergelegd in de wet Digitale overheid, met name zorginstellingen (aangewezen organisaties als bedoeld in onderdeel 3 van de bijlage bij de wet) brengt het onderhavige Besluit het nodige met zich. Vooral het monitoren en verantwoorden is voor hen in de praktijk vaak nieuw; naleving hiervan betekent voor hen administratieve lasten en kosten.

6.3 Resultaten (internet)consultatie

Gedurende de (internet)consultatie, die plaats had van 27 maart – 30 april 2018, is eenieder in de gelegenheid geweest input te leveren op het besluit. Vanwege de beschikbare voorbereidingstijd (die verband hield met de parlementaire behandeling van het bovenliggende wetsvoorstel) waren ook nadien uitvoeringsinstanties in de gelegenheid het concept (nogmaals) te bezien. Bezien is of de toepassing van het Besluit problematisch is (uitvoerbaarheid), wat er voor nodig is om aan het Besluit te voldoen (impact), waaronder wat de ingeschatte kosten op jaarbasis zijn van toepassing (kwantificering, zie ook hierna bij advies ATR), en of de invoeringstermijn haalbaar is.
Over het algemeen wordt het Besluit goed uitvoerbaar en implementeerbaar geacht.

Er is een beperkt aantal reacties ontvangen, met name vanuit de zorgsector. Op hoofdlijnen komen deze neer op opmerkingen over de uitvoerbaarheid van het besluit, in het bijzonder de met naleving van het bepaalde inzake informatieveiligheid (hst. 5 van het Besluit) gemoeide kosten. Ook de Unie van Waterschappen en de RDW – die reeds elektronische diensten aanbieden die ontsloten worden door DigiD en voor wie de normen en auditlast dus al golden en niet verzwaard worden – vragen aandacht voor de uitvoerbaarheid, met name op het punt van aard en reikwijdte van de audit en de auditlasten. Zie in dit verband de paragrafen 4.2 en 6.2 van het algemeen deel van deze toelichting, waarin wordt ingegaan op de mate waarin dit besluit andere/nieuwe eisen aan dienstverleners stelt. Voorts hebben enkele private partijen en de Kamer van Koophandel input (opmerkingen en vragen) geleverd op het punt van gegevensverwerking, welke geleid heeft tot verduidelijking van de betreffende onderdelen van het besluit en de toelichting.

In reactie op de geleverde input inzake uitvoerbaarheid wordt het volgende opgemerkt. Voor zorginstellingen en zorgverleners geldt, dat zij in de toekomst toegelaten identificatiemiddelen moeten accepteren; zij worden "aangewezen organisatie" in de zin van de wet en moeten bijgevolg ook het bij en krachtens de wet bepaalde inzake informatieveiligheid naleven. Zorgpartijen zullen derhalve rekening moeten houden met (eenmalige en structurele) investeringen en kosten voor systeemaanpassingen en aanpassingen in proces, werkwijzen en organisatie. Van belang hierbij is de mate waarin het onderhavige besluit eisen stelt die voor deze partijen nieuw zijn, dat wil zeggen aanvullend op hetgeen reeds voor hen geldt. Voor de zorgsector geldt dat zij reeds verplicht zijn om

informatiebeveiligingsmaatregelen te treffen, teneinde NEN 7510 *compliant* te zijn.[18] Het betreft de sectorspecifieke uitwerking van ISO/NEN 27001-27002, welke ten grondslag ligt aan het onderhavige besluit.[19] Om die reden wordt in artikel 21 van dit besluit naar norm NEN 7510 verwezen. Materieel bevat dit besluit voor zorginstellingen op het punt van informatiebeveiliging dus geen aanscherping. Naast maatregelen die zorginstellingen – op basis van risicomanagement - moeten treffen ter beveiliging van de informatievoorziening, is vereist dat informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht. In dit verband bevat NEN 7510 onder meer verplichte monitoring en analyse en documentatie, alsmede de noodzaak van het systematisch uitvoeren van (interne) audits om te bezien of conform NEN 7510 wordt gehandeld; over de auditresultaten moet worden gerapporteerd aan de eigen directie. Ook auditing is voor zorginstellingen en zorgverleners derhalve niet nieuw cq zou niet nieuw behoren te zijn.

Het verplicht via rapportage aan de minister van BZK, aantonen van conformiteit, zoals voorzien in de wet Digitale overheid en in dit besluit, is voor zorginstellingen die niet eerder waren aangesloten op DigiD (vooral kleine zorgpartijen) wel nieuw. De in dat kader uitgevoerde wijze van beoordeling, gebaseerd op de ICT-beveiligingsrichtljinen van de minister van BZK, en de daarbij gelegde accenten verschillen van de NEN 7510 audit. Dit geldt ook voor de (externe) zorgaudits die via de Raad voor Accreditatie (RvA) worden gefaciliteerd en gecertificeerd.[20] Op dit punt is dus voor (een deel van) de zorgpartijen sprake van als gevolg van dit besluit aanvullend te nemen stappen. Niettemin zal, doordat het besluit aansluit bij de reeds voor de zorg bestaande (materiële en procedurele) verplichtingen, naar verwachting de via zorgaudits gegenereerde informatie (deels) tevens bruikbaar zijn voor de rapportage aan Onze Minister. Bij de nadere uitwerking van artikel 24 van dit besluit zal, mede met het oog op beperking van de auditlasten- en kosten, waar mogelijk rekening worden gehouden met door zorginstellingen reeds gehanteerde methodieken en wijzen van beoordeling en rapportage en zal worden gestreefd naar het behalen van synergie. Ook zal de opportuniteit worden bezien van meervoudige/clusteraansluiting op de door BZK te ontwikkelen routeringsvoorziening, teneinde aansluit- en auditkosten (verder) te beperken voor bijvoorbeeld individuele zorgaanbieders. Uitgangspunt is evenwel alle dienstverleners op eenduidige wijze te (kunnen) beoordelen; hierdoor is de ruimte voor eigen vormgeving van audits en rapportage beperkt.

Voor wat betreft de (haalbaarheid van de) invoering wordt opgemerkt, dat de bepalingen in dit besluit naar verwachting toegepast kunnen worden vanaf het moment van inwerkingtreding van de bovenliggende wetsbepalingen (artikelen 4 en 16 van de wet).

7 Toezicht en handhaving

Het toezicht op de naleving van de bepalingen in dit Besluit over de verwerking van persoonsgegevens geschiedt door de Autoriteit persoonsgegevens (artikel 6 Uitvoeringswet AVG), wat betreft toezicht op de beveiliging van persoonsgegevens (artikel 51, eerste lid, AVG j° artikel 32 AVG).

Voor wat betreft het in dit Besluit bepaalde inzake informatieveiligheid is het toezicht op de dienstverleners belegd bij de Minister van BZK. Zijn taken en bevoegdheden zijn verankerd in de wet (artikelen 17, vierde lid, en de artikelen 18 en 19 van de wet). Misbruik en oneigenlijk gebruik van de toegang tot elektronische dienstverlening moet worden voorkomen middels pro-actief handelen bij een vermoeden en moet worden beëindigd bij vastgestelde compromittering. Teneinde dit te kunnen waarmaken, kunnen de uitwisseling van gegevens tussen dienstverleners en de minister en, ultimo, het door de minister afsluiten van de toegang in de rede liggen. In dit verband is tevens van belang, dat dienstverleners rapporteren over de naleving van de regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot hun elektronische diensten, zoals verankerd in artikel 4 van de wet en uitgewerkt in dit Besluit. Zoals onder punt 6 van deze toelichting is aangegeven, is voor een deel van de dienstverleners het in dit Besluit inzake informatieveiligheid bepaalde nieuw; met name de nalevingsbereidheid ter zake van de bepalingen inzake monitoring en

[18] Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders), Stb. 2017, 446.
[19] Werkenmetnen7510.nl.
[20] Hoewel gangbaar, zijn deze ingevolge NEN 7510 niet verplicht; ze vormen ook geen onderdeel van de GBZ-kwalificatie.

verantwoording vormt een punt van aandacht. Overigens zullen door de minister bij dienstverleners geen nieuwe kosten in rekening worden gebracht voor het in behandeling nemen van de auditrapportages (artikel 24). Deze zijn reeds verdisconteerd in de kostprijs die aan de afnemers van DigiD en DigiD Machtigen in rekening worden gebracht.

8 Evaluatie

De Wet digitale overheid bevat een evaluatiebepaling, ingevolge welke de minister binnen vijf jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag zendt over de doeltreffendheid en de effecten van deze wet in de praktijk. In het bijzonder wordt hierbij aandacht geschonken aan de getroffen maatregelen op het gebied van beveiliging en privacybescherming. Bij deze gelegenheid zal ook het onderhavige besluit worden betrokken.

9 Uitgebrachte adviezen

Adviescollege Toetsing Regeldruk (ATR)

Gedurende de (internet)consultatie is tevens advies ontvangen van het ATR. De focus ligt in het advies op de informatieveiligheids-regeldruk effecten voor aangewezen organisaties (hoofdstuk 5 van het Besluit), in het bijzonder de (kleine) zorgaanbieders. Geadviseerd wordt om:
- te onderbouwen in hoeverre de mogelijkheden zijn verkend voor aangewezen organisaties om, op een bij hun omvang passende wijze, aan te kunnen tonen dat zij voldoen aan de informatieveiligheidseisen;
- de uitkomsten van uitgevoerde uitvoeringstoetsen herleidbaar te verwerken in de toelichting en daarbij te onderbouwen dat de regeling ook uitvoerbaar is voor kleine (zorg)organisaties; - te zorgen voor duidelijke verplichtingen in en bij het besluit, in het belang van de uitvoerbaarheid; - de regeldrukgevolgen van de voorgestelde bepalingen in kaart te brengen conform de rijksbrede methodiek.

In reactie hierop wordt het volgende opgemerkt (zie tevens paragraaf 6.3). De kosten van aansluiting/acceptatie, naleving van de veiligheidsnormen en auditing – strict genomen voortvloeiend uit de bovenliggende wet en niet uit het onderhavige besluit – bestaan deels uit eenmalige kosten en deels uit vaste kosten. Grofweg gaat het per organisatie om enkele tienduizenden euro's per jaar, waarvan het grootste deel, tot zo'n 20.000 euro, bestaat uit de kosten voor een jaarlijkse audit. Voor met name kleine zorgaanbieders die onder de reikwijdte van de WDO gaan vallen, bijvoorbeeld een huisarts, is dit een substantieel bedrag. Het is echter, mede gelet op de samenhang binnen het stelsel en de veiligheid en betrouwbaarheid van de gehele keten, noodzakelijk dat informatieveiligheid ook op orde is bij kleine zorgaanbieders. Bovendien gaat het hier om verplichtingen die én bij hen reeds bekend (behoren te) zijn én ruimte laten voor inpassing die aansluit bij de aard en kenmerken van de eigen organisatie (maatwerk). Er is niet of nauwelijks sprake van ten opzichte van de huidige situatie aangescherpte eisen en daarmee samenhangende regeldrukeffecten. Materieel bevat het besluit voor de zorgsector – als zij zich reeds aan de voor hen geldende NEN 7510 houden – niets nieuws. Wel kan, afhankelijk van de aard en grootte van de desbetreffende zorginstelling en de huidige stand van hun interne systemen en processen, auditing en rapportage tot extra kosten leiden. Er wordt in dit verband naar gestreefd de opzet en inrichting van de zorgaudits en de daaruit gegenereerde informatie zoveel mogelijk te benutten, zodat op passende wijze kan worden gerapporteerd over de naleving van de informatieveiligheidseisen en dubbelingen en extra werk worden voorkomen. Hierdoor kan de regeldruk beperkt worden. Voorts zal bezien worden of via meervoudige/clusteraansluiting en groepsgewijze audits rekening kan worden gehouden met beperkte schaalgrootte van dienstverleners, waaronder zorginstellingen. Gewerkt wordt aan een methodiek waarbij de auditkosten substantieel worden gereduceerd voor de kleinere aansluitingen. Hierbij is het de bedoeling dat het assessment voor de aangesloten partijen centraal en in nauw overleg met BZK/Logius wordt gecoördineerd en uitgevoerd. Het besluit biedt hiertoe de ruimte; bij de uitwerking van artikel 24 zal zoveel mogelijk rekening worden gehouden met (informatie afkomstig uit) elders voorgeschreven audits en rapportage. Dit draagt bij aan de uitvoerbaarheid. Gewezen zij in dit verband op de ruimte die gemeenten hebben om volgens het principe van *single information single audit (*ENSIA*)* informatie, die noodzakelijk is voor de horizontale verantwoording (aan de gemeenteraad) over informatieveiligheid van eigen systemen, ook bij de verticale verantwoording (aan BZK) te gebruiken, teneinde hun audit- en monitorlast te beperken.

Autoriteit Persoonsgegevens (AP)

Na afloop van de (internet)consultatie is advies ontvangen van de AP. De focus in dit advies ligt op de wijze waarop uitkomsten van de gedurende ontwikkeling van het eID-stelsel uitgevoerde *privacy impact assessments* (PIA's) in het onderhavige besluit zijn verwerkt. Als onderdeel van een breder pakket uitvoeringsregelgeving bij de WDO vormt ook dit besluit immers de weerslag van veiligheids- en privacybeschermende maatregelen die in een PIA worden beschreven.

De AP merkt op dat de nota van toelichting bij het conceptbesluit op een aantal punten tekortschiet als het gaat om de afwegingen die zijn gemaakt en de wijze waarop de bescherming van persoonsgegevens als geheel vorm krijgt. Zij noemt enkele concrete punten voor verbetering en adviseert om de nota van toelichting en het conceptbesluit aan te vullen.

In de eerste plaats wordt aanbevolen in de nota van toelichting alsnog een relatie te leggen tussen enkele aandachtspunten die uit de PIA naar voren kwamen en genomen maatregelen in de regelgeving als gevolg daarvan. Zo wordt ter zake van artikel 5f, dat een grondslag biedt voor gegevensverwerking in het kader van misbruikbestrijding in den brede, geadviseerd om in de nota van toelichting aan te geven dat hiermee gevolg wordt gegeven aan de aanbeveling in de PIA van 28 juni 2017, om misbruik- en incidentbestrijding op stelselniveau in te richten en de hiervoor te gebruiken gegevens uit te werken. Dit advies is overgenomen.
Daarnaast constateert de AP dat in het besluit weliswaar toepassing van functiescheiding is voorgeschreven, maar dat deze norm zich richt tot bestuursorganen en aangewezen organisaties (publieke dienstverleners). De AP vraagt zich af hoe is gewaarborgd dat ook (ICT)leveranciers voor overheidspartijen maatregelen nemen om functiescheiding te bewerkstelligen. In aansluiting hierop is in de nota van toelichting bij artikel 19 aangegeven, dat dienstverleners die opdrachten verlenen aan leveranciers moeten bewerkstelligen dat laatstgenoemden, mede met inachtneming van de AVG, de benodigde beveiligingsmaatregelen treffen.
Tot slot vraagt de AP zich af hoe wordt bewerkstelligd dat logging bij authenticatiedienstverlening niet voor andere doeleinden wordt gebruikt. In dit verband zij verwezen naar de uitvoeringsregelgeving ingevolge artikel 9 van de wet, die tevens regels zal bevatten over misbruik van logging door betrokken (private) partijen. Daarnaast bevat het onderhavige besluit zowel geboden om gegevens te gebruiken voor de beschreven doeleinden (doelbinding), als een verbod (artikel 5e) om gegevens op basis van andere verwerkingsgronden te gebruiken. Daarmee wordt geëxpliciteerd dat gegevens niet op basis van bijvoorbeeld toestemming voor andere doelen kunnen worden gebruikt.

In de tweede plaats is het volgens AP van belang dat inzicht wordt geboden in het geheel aan beveiligingsmaatregelen en dat de essentie ervan in regelgeving is geborgd. In dit verband wordt opgemerkt dat herstelvermogen op stelselniveau wordt gerealiseerd door het samenstel van wettelijke bepalingen, uitvoeringsregelgeving op basis van de eIDAS-verordening, de beleidskaders inzake privacy, PSA's en inbedding in (technische en operationele) systemen. Het onderhavige Besluit maakt daar onderdeel van uit. De door de AP genoemde notificatieplicht aan de burger wanneer op zijn naam een nieuw identificatiemiddel wordt aangevraagd, zal worden opgenomen in de uitvoeringsregelgeving ingevolge artikel 9 van de wet.

In de derde plaats adviseert de AP om in de nota van toelichting alsnog aandacht te besteden aan het subsidiariteitsbeginsel. Aan dat advies is gevolg gegeven onder het kopje "Proportionaliteit en subsidiariteit" van paragraaf 5.

Voorts adviseert de AP om de nota van toelichting aan te passen wat betreft de toezichthoudende rol van de AP op de beveiliging van persoonsgegevens ingevolge artikel 51, eerste lid, van de AVG juncto artikel 32 van de AVG. Paragraaf 7 van de nota van toelichting is op dit punt aangevuld.

De AP adviseert om alsnog de lengte van de bewaartermijnen met betrekking tot persoonsgegevens die worden verwerkt in het kader van het bedrijfs-en organisatiemiddel (artikel 14c) te onderbouwen. De nota van toelichting is op dit punt aangevuld.

Vervolgens adviseert de AP om de in de nota van toelichting genoemde bewaartermijnen van reservekopieën voor DigiD, DigiD Machtigen en MijnOverheid alsnog op te nemen in het conceptbesluit

en om de lengte van de bewaartermijn van maximaal 4 maanden te onderbouwen in de nota van toelichting. Dit advies is overgenomen.

Ook adviseert de AP om het conceptbesluit in overeenstemming te brengen met de nota van toelichting, in verband met het feit dat het toepassen van de betreffende ISO/NEN-normen een weerlegbaar rechtsvermoeden oplevert dat aan de informatiebeveiligingseisen als bedoeld in de artikelen 16 tot en met 19 van het conceptbesluit wordt voldaan. Artikel 21 van het besluit is in deze zin aangepast.

Tenslotte stelt de AP nog twee tekstuele verbeteringen voor (artikel 14c en onderdeel M van het artikelsgewijze deel van de nota van toelichting), die beide zijn overgenomen.

Voor de volledigheid wordt op deze plaats opgemerkt, dat de bescherming van persoonsgegevens een in de praktijk doorlopende – operationele - verantwoordelijkheid is. Privacy wordt niet alleen beschermd door dat in wet- en regelgeving te verankeren. Die bescherming moet in de praktijk vorm krijgen en moet kunnen meegroeien met de in de tijd ontstane dreigingen en ter beschikking komende beschermingsmaatregelen. In de wet en dit besluit worden verwerkingsgrondslagen, bewaartermijnen en verstrekkingen geregeld die deze verantwoordelijkheid inkaderen, en die tegelijkertijd de ruimte bieden om de operationele bescherming van persoonsgegevens toe te snijden op de in de praktijk benodigde en veranderende behoeften.

10 Inwerkingtreding

Beoogd moment van inwerkingtreding is de datum van inwerkingtreding van de wet, ervan uitgaand dat de voorzieningen, waarin gegevens worden verwerkt, dan functioneren en de publieke dienstverleners gereed zijn voor uitvoering van de informatieveiligheidsbepalingen. Gedifferentieerde inwerkingtreding is mogelijk. Overgangsrecht is niet opportuun.

II Artikelsgewijze toelichting

Artikel I

Onderdeel A

In verband met de inwerkingtreding van de Wet digitale overheid, waarin enige nieuwe of aangepaste definities worden geïntroduceerd, worden de definities in het besluit aangepast en aangevuld.

Wat betreft de beschrijving van de afnemer van een routeringsvoorziening wordt erop gewezen dat het daarbij gaat om de verlening van toegang met zowel identificatiemiddelen voor burgers als voor bedrijven en ondernemingen; daarom wordt gesproken over toegelaten en erkende identificatiemiddelen. Voor de beschrijving van het begrip routeringsvoorziening wordt verwezen naar artikel 5 van de wet; voor de volledigheid wordt hier toegevoegd dat die beschrijving mede omvat het gebruik van machtigingen (bijvoorbeeld DigiD Machtigen) via routeringsvoorzieningen en dat een gemachtigde ook een rechtspersoon met een bedrijfs- of organisatiemiddel kan zijn. Ook de eIDAS-voorziening wordt beslagen.

Wat betreft de nieuwe beschrijving van DigiD is het relevant toe te lichten dat de omschrijving "voorziening voor uitgifte of activatie van elektronische identificatiemiddelen" betekent dat de voorziening voor uitgifte en/of activatie kan worden gebruikt. Zie verder de toelichting bij onderdeel B.

Wat betreft de beschrijving van de gebruiker van een bedrijfs- en organisatiemiddel is het relevant om toe te lichten dat deze beschrijving weliswaar ondernemingen en rechtspersonen omvat, ook al gaat het onderhavige besluit enkel over de verwerking van persoonsgegevens. De reden daarvoor is tweeërlei. Ten eerste kunnen ook natuurlijke personen die deze onderneming of rechtspersoon vertegenwoordigen (als tekenbevoegde, machtigingenbeheerder of medewerker) als gebruiker worden aangemerkt en ook over hen kunnen dus persoonsgegevens worden verwerkt. Ten tweede zijn gegevens over eenmanszaken eenvoudig te herleiden tot de natuurlijke persoon die de betreffende zaak runt, reden waarom bij de verwerking van persoonsgegevens over eenmanszaken sprake is van persoonsgegevens.

De nieuwe beschrijving van MijnOverheid houdt verband met de toegevoegde dienst/functie Algemene bekendmakingen, kennisgevingen en mededelingen. Tot slot worden enkele beschrijvingen toegevoegd die verband houden met het nieuwe hoofdstuk 5, inzake informatieveiligheid.

Onderdeel B

In dit onderdeel wordt artikel 2 over de verwerking van persoonsgegevens door de minister van Binnenlandse Zaken en Koninkrijksrelaties in het kader van de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van DigiD aangepast in verband met de introductie van de elektronische identificatiemiddelen op betrouwbaarheidsniveaus substantieel en hoog. In verband met deze introductie zullen nieuwe persoonsgegevens verwerkt worden over de gebruikers van DigiD.

Ten eerste zal artikel 2, onderdeel c, onder 2°, worden uitgebreid voor substantieel met de gegevens over het Nederlands rijbewijs, het Nederlandse paspoort of de Nederlandse identiteitskaart zoals geldigheidsdata van het Nederlandse paspoort of Nederlandse identiteitskaart en het documentnummer van het rijbewijs. Deze verwerking is noodzakelijk omdat het rijbewijs, paspoort of identiteitskaart geïntroduceerd zal worden als activatie en gebruikersbeheer van het elektronisch identificatiemiddel op betrouwbaarheidsniveau substantieel. Daarnaast wordt het uitgebreid voor hoog met het versleutelde en afgeleide burgerservicenummer, volgnummer en document type. Deze verwerking is noodzakelijk omdat het rijbewijs en de Nederlandse identiteitskaart geïntroduceerd zullen worden bij het gebruik en gebruikersbeheer van het elektronisch identificatiemiddel op betrouwbaarheidsniveau hoog. In verband hiermee zullen deze gegevens verwerkt worden door de minister van BZK.

Ten tweede wordt artikel 2, onderdeel c, onder 3°, uitgebreid met de gegevens de gekozen documentsoort voor elektronische identificatie, status van het identificatiemiddel, het soort apparaat (onder andere naam en modelnummer voor activatie gebruikte apparaat) waarmee op elektronische wijze gecommuniceerd kan worden met het Nederlandse paspoort, de Nederlandse identiteitskaart of het Nederlands rijbewijs voor betrouwbaarheidsniveau substantieel. Daarnaast wordt dit artikel uitgebreid met de status van het identificatiemiddel waarmee op elektronische wijze gecommuniceerd kan worden met de Nederlandse identiteitskaart of het Nederlands rijbewijs voor betrouwbaarheidsniveau hoog. Deze persoonsgegevensverwerkingen door de minister van BZK zijn noodzakelijk in verband met de introductie van het elektronische identificatiemiddel op betrouwbaarheidsniveau substantieel voor activatie en gebruikersbeheer en voor betrouwbaarheidsniveau hoog. Verder wordt het begrip "versleuteld wachtwoord" vervangen door "een afgeleide vorm van het wachtwoord" om aan te geven dat deze niet herleidbaar is tot het origineel. Tenslotte wordt een afgeleide vorm van de pincode toegevoegd, omdat de gebruiker een pincode kiest voor het gebruik van de app. Deze pincode wordt versleuteld bewaard.

Ten derde wordt artikel 2, onderdeel c, onder 6°, uitgebreid met de categorie gegevens noodzakelijk voor de administratie van DigiD (betrouwbaarheidsniveau substantieel). In het kader van het uitbrengen van een factuur door een verwerker aan de minister van BZK vanwege werkzaamheden die de verwerker verricht voor DigiD, zal het burgerservicenummer van gebruikers verwerkt worden door de minister van Binnenlandse Zaken en Koninkrijksrelaties. Deze verwerking vindt plaats om de hoeveelheid werkzaamheden te kunnen bepalen die voor facturering in aanmerking komen.

Aan artikel 2, onderdeel c, zijn daarnaast drie onderdelen toegevoegd. In deze onderdelen wordt vastgelegd dat de minister van BZK drie nieuwe categorieën persoonsgegevens verwerkt binnen DigiD: gegevens afkomstig van de chip van het Nederlands rijbewijs, het Nederlandse paspoort en de identiteitskaart waarmee de gebruiker van DigiD toegang heeft voor substantieel of gegevens afkomstig van de chip van het Nederlandse rijbewijs en de identiteitskaart waarmee de gebruiker van DigiD toegang heeft voor betrouwbaarheids hoog en tenslotte gegevens die noodzakelijk zijn in het kader van de uitvoering van de eIDAS-verordening. Met de introductie van DigiD op niveaus substantieel zal in het activatieproces de chip op het paspoort, de identiteitskaart of het rijbewijs worden uitgelezen en op niveau hoog zal in het activatie en authenticatieproces de chip op het Nederlandse rijbewijs en identiteitskaart worden uitgelezen om de identiteit van de burger te kunnen vaststellen. Voor substantieel bij het openen van de chip van een Nederlands paspoort of een Nederlandse identiteitskaart zullen automatisch de volgende persoonsgegevens worden verwerkt door de minister van BZK: documentcode van het paspoort of de identiteitskaart, uitgevende staat of

organisatie van het paspoort of de identiteitskaart, naam van de houder, documentnummer van het paspoort of de identiteitskaart, nationaliteit van de houder, geboortedatum van de houder, geslacht van de houder, geldigheidsdata van het paspoort of de identiteitskaart en het burgerservicenummer. Indien een persoon een rijbewijs gebruikt voor authenticatie zullen bij het openen van de chip automatisch de documentcode en het documentnummer van het rijbewijs worden verwerkt door de minister van BZK. De gegevens die zijn uitgelezen van de chip van het paspoort, de identiteitskaart en het rijbewijs worden na verificatie van de identiteit van de gebruiker direct verwijderd. Voor betrouwbaarheidsniveau hoog bij het openen van de chip van het Nederlandse identiteitskaart of rijbewijs zullen de volgende persoonsgegevens verwerkt worden door de minister van BZK: het versleutelde en afgeleide burgerservicenummer, documentnummer en documentcode. Tot slot worden door de minister van BZK persoonsgegevens van contactpersonen bij de afnemers van DigiD verwerkt in het kader van het aansluiten van de afnemers en de verdere ondersteuning van de afnemers in het gebruik van DigiD. Nu de aansluitvoorwaarden niet langer worden vastgelegd bij overeenkomst is de grondslag voor de verwerking van deze gegevens komen te vervallen. Vandaar dat een specifieke grondslag hiertoe wordt opgenomen in het besluit door middel van een wijziging van artikel 2 van het besluit.

Onderdeel C

In dit onderdeel wordt artikel 3 van het besluit over de persoonsgegevensverwerking door de minister van BZK die plaatsvindt in verband met de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van DigiD Machtigen gewijzigd. De kans is groot dat als gevolg van voorziene ontwikkelingen DigiD Machtigen in de toekomst naast het burgerservicenummer ook de versleutelde of afgeleide vorm daarvan gaat verwerken. Om die reden is die versleutelde of afgeleide vorm als optie toegevoegd. In verband met de introductie van het bedrijfsmiddel als middel voor elektronische identificatie van de gemachtigde, wordt in artikel 3, onderdeel b, onder 2°, het unieke nummer dat door de Kamer van Koophandel is toegekend aan een onderneming die in Nederland is gevestigd en toebehoort aan een natuurlijke persoon toegevoegd. Bij de registratie van de machtigingsrelatie tussen een burger en een dergelijke onderneming wordt dit nummer door de minister van BZK verwerkt. Indien de onderneming toebehoort aan een natuurlijke persoon valt dit nummer te herleiden tot deze natuurlijke persoon indien dit een zzp-er betreft, door middel van het raadplegen van het handelsregister. Daarnaast is gebleken dat niet de datum overlijden van de gebruiker gebruikt wordt om de beëindiging van de machtigingsrelatie vast te stellen, maar het gegeven reden opschorting persoonslijst van de gebruiker in de BRP. Hieruit wordt de datum overlijden afgeleid. In artikel 3, onderdeel b, onder 1°, wordt dit gegeven daarom aangepast. Ook worden door de minister van BZK persoonsgegevens van contactpersonen bij de afnemers van DigiD Machtigen verwerkt in het kader van het aansluiten van de afnemers en de verdere ondersteuning van de afnemers in het gebruik van DigiD Machtigen. Nu de aansluitvoorwaarden niet langer worden vastgelegd bij overeenkomst is de grondslag voor de verwerking van deze gegevens komen te vervallen. Vandaar dat een specifieke grondslag hiertoe wordt opgenomen in het besluit door middel van een wijziging van artikel 3 van het besluit. In onderdeel 6° wordt toegevoegd dat notificatiegegevens kunnen worden verwerkt. Dit houdt verband met het feit dat aan gebruikers, uit service-overwegingen, attenderingen terzake van de verrichte diensten kunnen worden verstuurd. Indat verband wordt het door de gebruiker opgegeven voorkeurskanaal, via welke communicatie met de overheid plaatsvindt (e-mail of telefoon), verwerkt. Artikel 4, onderdeel 6, onder 3°, kent reeds een vergelijkbare bepaling op grond waarvan de accountgegeven, waaronder het voorkeurskanaal waarop de gebruiker van MijnOverheid notificaties ontvangt en gegevens over de verificatie daarvan, worden verwerkt.

Onderdeel D

In dit onderdeel wordt artikel 4 zodanig gewijzigd dat ook een versleutelde vorm van het burgerservicenummer binnen MijnOverheid door de minister van BZK verwerkt kan worden. Dit is noodzakelijk omdat binnen MijnOverheid gewerkt kan worden met versleutelde burgerservicenummers. Met deze versleutelde burgerservicenummers wordt op versleutelde wijze de koppeling tussen een gebruiker van een elektronisch identificatiemiddel en het middel vastgelegd. De minister van BZK als verantwoordelijke voor het stelsel heeft echter de bevoegdheid om bij misbruik binnen het stelsel (de versleutelde vorm van) het burgerservicenummer te herleiden tot de gebruiker. In die zin betreft ook het versleutelde burgerservicenummer een persoonsgegeven, aangezien deze onder bepaalde omstandigheden (misbruik) is te herleiden tot de gebruiker. Voorts wordt in de

onderdelen b en c aangegeven dat gegevens in het bericht van de afnemer (dienstverlener) of in een andere functionaliteit van MijnOverheid worden verwerkt. Deze aanvulling brengt met zich, dat ter zake niet langer verwerkersovereenkomsten tussen de minister (verwerker) en de afnemers behoeven te worden gesloten.[21] Ook worden door de minister van BZK persoonsgegevens van contactpersonen bij de afnemers van MijnOverheid verwerkt in het kader van het aansluiten van de afnemers en de verdere ondersteuning (door het klantcontactcentrum van BZK/Logius) van de gebruikers in het gebruik van MijnOverheid. Nu de aansluitvoorwaarden niet langer worden vastgelegd bij overeenkomst is de grondslag voor de verwerking van deze gegevens komen te vervallen. Vandaar dat een specifieke grondslag hiertoe wordt opgenomen in het besluit door middel van een wijziging van artikel 4 van het besluit. Tot slot is artikel 4 aangepast met het oog op de nieuwe dienst/functie die de gebruikers van MijnOverheid informeert over algemene bekendmakingen, kennisgevingen en mededelingen die voor hen van belang zullen zijn.

Onderdeel E

Dit onderdeel regelt dat artikel 5 qua terminologie wordt aangepast aan de nieuwe definities zoals opgenomen in de Wet digitale overheid en de vernieuwde werking van het BSN-K binnen het stelsel van de generieke digitale infrastructuur. Belangrijke vernieuwing betreft de rol van het BSN-K bij de authenticatie met een publiek middel en de rol die de voorziening speelt binnen het stelsel bij de versleuteling van het burgerservicenummer. Daarnaast wordt opgenomen dat naast het burgerservicenummer, ook een versleutelde of afgeleide vorm daarvan verwerkt kan worden door de minister van BZK als verantwoordelijke voor het BSN-K. De verschillende functionaliteiten van het BSN-K maken gebruik van burgerservicenummers in versleutelde of afgeleide vorm van gebruikers. Onder bepaalde omstandigheden, namelijk bij misbruik, kan het van het burgerservicenummer versleutelde of afgeleide gegeven door de minister van BZK herleid worden tot de betreffende gebruiker. Daarom dient voor een rechtmatige verwerking van dit gegeven door de minister van BZK een grondslag te worden opgenomen in dit besluit. Artikel 5 wordt tenslotte zodanig aangepast dat het uniek identificerende kenmerk op het private authenticatiemiddel wordt verwijderd als persoonsgegeven welke verwerkt wordt door de minister van BZK, aangezien gebleken is dat dit niet tot de persoon te herleiden is door de minister van BZK, maar enkel onderscheid aan dient te brengen tussen de verschillende middelen van de gebruiker, dus enkel voor de gebruiker onderscheidend is. Verder worden, in verband met de inzagefunctie van het BSN-K, in onderdeel a, onder 4°, de statusgegevens toegevoegd van de aan een gebruiker gekoppelde identificatiemiddelen. Met de inzagefunctie (die wordt ontsloten via MijnOverheid) kan de gebruiker inzage krijgen in welke middelen aan hem zijn of waren gekoppeld en de status van die middelen (hiertoe wordt enkel het burgerservicenummer in afgeleide vorm gebruikt). Verder wordt niet langer door de minister van BZK het inlogtijdstip van de gebruiker bij de publieke dienstverlener verwerkt op tot het individu herleidbare wijze. Vanwege deze nieuwe werkwijze kan artikel 5, onderdeel e, komen te vervallen. Overigens kunnen ook rechtspersonen gebruik maken van het BSN-K. Aangezien zij daarbij worden vertegenwoordigd door natuurlijke personen, kan ook in die gevallen sprake zijn van verwerking van het burgerservicenummer van die vertegenwoordigers.
Tot slot worden bij het BSN-K ook gegevens verwerkt over afnemers van het BSN-Koppelregister, denk aan de erkende partijen als de middelenuitgever, de machtigingsdienst, de authenticatiediensten, de routeringsvoorziening en de eIDAS-voorziening. Het gaat daarbij om administratieve gegevens die noodzakelijk zijn in verband met het gebruik van het BSN-K (met name het inzageregister). Het gaat om onder andere de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van de routeringsvoorziening en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer.

Onderdeel F

In onderdeel F worden de artikelen toegevoegd over de gegevens die kunnen worden verwerkt in de nieuwe voorzieningen. Voor de volledigheid wordt opgemerkt dat, net als bij de reeds in het Besluit verwerking persoonsgegevens generieke digitale infrastructuur geregelde voorzieningen, ook voor deze nieuwe voorzieningen en erkende diensten alle persoonsgegevens worden genoemd die in het algemeen worden verwerkt. Dat wil niet zeggen dat van alle individuele gebruikers de hele set van gegevens wordt verwerkt. Zoals blijkt uit de beschrijving van de werking van de voorzieningen in het algemeen deel van deze nota van toelichting (zie paragraaf 4.1) is de verwerking van gegevens

[21] Vide de ingevolge artikel 28 AVG op de verwerker rustende verplichtingen.

afhankelijk van bijvoorbeeld de wens of de situatie van de gebruiker of de specifieke activiteit van een erkende dienst (bv. een authenticatiedienst of een machtigingsdienst).

Artikel 5a
In dit onderdeel wordt door middel van het invoegen van een nieuw artikel 5a de persoonsgegevensverwerking geregeld die plaatsvindt door de minister van BZK in het kader van de goede beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de routeringsvoorziening. De minister van BZK verwerkt hiertoe van de gebruiker van het elektronisch identificatiemiddel onder meer een nummer dat ter identificatie van een persoon kan worden gebruikt of tot een persoon kan worden herleid (waaronder het burgerservicenummer of een versleutelde of afgeleide vorm daarvan). Het gaat daarbij om gebruikers van een toegelaten publiek of privaat identificatiemiddel of erkend bedrijfs- of organisatiemiddel. Van degene die wordt vertegenwoordigd door een gemachtigde wordt ook het burgerservicenummer of een versleutelde of afgeleide vorm daarvan verwerkt in verband met de routeringsvoorziening (onderdeel b van artikel 5a in samenhang de definitie van "gemachtigde" in artikel 1). De in onderdeel a, onder 1°, genoemde gegevens worden vooral, maar niet uitsluitend, versleuteld verwerkt; de routeringsvoorziening ontvangt de gegevens versleuteld, maar zal ze waarschijnlijk weer ontsleutelen en opnieuw versleutelen, omdat uiteindelijk maar één versleutelmethode gewenst is naar de afnemer/dienstverlener toe.

Artikel 5b
Door invoering van artikel 5b wordt de persoonsgegevensverwerking geregeld die plaatsvindt door de aanbieder van een toegelaten (erkend) privaat identificatiemiddel als bedoeld in artikel 9, tweede lid, van de wet, of door de erkende ontsluitende dienst als bedoeld in artikel 9, derde lid van de wet. Aangezien de werking hiervan voor een groot deel op een zelfde manier geconstrueerd zal zijn als de DigiD-voorziening voor elektronische dienstverlening met publieke identificatiemiddelen, zullen dezelfde soort gegevens verwerkt worden, met die uitzondering dat gegevens gerelateerd aan het Nederlands paspoort, de Nederlandse identiteitskaart of het Nederlands rijbewijs slechts een beperkte rol zullen spelen in het proces van uitgifte, activatie en authenticatie, namelijk slechts ter identificatie van de gebruiker van het middel aan het begin van het aanvraagproces, aangezien deze identificatiemiddelen enkel gebruikt zullen worden als drager van het publieke identificatiemiddel en niet als drager van het private elektronische identificatiemiddel. Benadrukt zij dat de onderhavige gegevensverwerking plaatsvindt binnen de werkingssfeer van de wet digitale overheid en dus alleen ten behoeve van elektronische dienstverlening in het publieke domein.

Artikel 5c
Artikel 5c formuleert gegevens die kunnen worden verwerkt door de erkende private partijen die betrokken zijn bij het aanbieden van elektronische identificatiemiddelen voor bedrijven (identificatiemiddelen voor een onderneming of rechtspersoon als bedoeld in artikel 5 onderscheidenlijk 6 van de Handelsregisterwet 2007 of een op grond van artikel 8, aanhef en onderdeel a, van die wet aangewezen rechtspersoon dat wordt uitgegeven aan een natuurlijke persoon die blijkens een aan dat middel gekoppelde of te koppelen machtiging van een erkende machtigingsdienst bevoegd is om namens die onderneming of rechtspersoon te handelen en waarmee deze onderneming of rechtspersoon toegang kan krijgen tot elektronische dienstverlening, zie artikel 1 van de wet). Deze partijen verwerken persoonsgegevens zover dit noodzakelijk is voor de werking van het bedrijfs- en organisatiemiddel en goede en veilige toegang met dat middel tot elektronische dienstverlening. Het geformuleerde pakket wordt door de keten heen verwerkt; partijen verwerken bepaalde gegevens naar gelang hun rol/plek en de omstandigheden van het geval. Wat betreft de in onderdeel a, onder 5°, genoemde website van de instelling waar de gebruiker een bedrijfs- of organisatiemiddel aanvraagt kan bijvoorbeeld worden gedacht aan de website van de middelenuitgever.

Gegevens over een gebruiker die in dit proces van aanvraag en uitgifte van een bedrijfs- of organisatiemiddel (zie daarover verder paragraaf 4.1.4. van het algemeen deel van deze nota van toelichting) kunnen worden verwerkt zijn, afhankelijk van de persoon die het aanvraagt of voor wie het wordt aangevraagd, de naam, de geboortedatum, de geboorteplaats, de nationaliteit, het actuele adres, het e-mailadres, het telefoonnummer, de foto en het type identiteitsbewijs, een gekwalificeerd certificaat dat wordt gebruikt als elektronische handtekening en bedrijfsgegevens (artikel 5c, onderdeel a, onder 1°), een nummer dat ter identificatie van een persoon kan worden gebruikt of tot een persoon kan worden herleid (denk aan het burgerservicenummer of een versleutelde of afgeleide vorm daarvan, het uniek identificerend nummer in geval van authenticatie buiten Nederland in

afgeleide vorm, het nummer van een rijbewijs, het nummer van de Kamer van Koophandel, zie artikel 5c, onderdeel a, onder 2°) en gegevens die noodzakelijk voor de registratie van een machtiging (zoals de identiteit van de gemachtigde en machtigingsverlener, de dienst ter afname waarvan de machtiging is verleend, de looptijd en status van de machtiging en gegevens betreffende uitgevoerde verificaties en validaties, zie artikel 5c, onderdeel a, onder 3°). Ten aanzien van het in onderdeel a, onder 2°, is een toelichting wenselijk over het nummer dat ter identificatie van een persoon kan worden gebruikt of dat tot een persoon herleidbaar is; de laatste toevoeging houdt verband met het daarna genoemde nummer van de Kamer van Koophandel, dat, indien de onderneming toebehoort aan een natuurlijke persoon, valt te herleiden tot deze natuurlijke persoon indien dit een zzp-er betreft, door middel van het raadplegen van het handelsregister.

Gegevens over de gebruiker die in het proces van het gebruik van een bedrijfs- of organisatiemiddel (zie daarover verder paragraaf 4.1.4. van het algemeen deel van deze nota van toelichting) kunnen worden verwerkt zijn, afhankelijk van de persoon die het middel gebruikt of het gekozen middel, de zogenaamde gebruiksgegevens, waaronder het IP-adres, gegevens afkomstig van het authenticatiemiddel van de gebruiker waarmee hij heeft ingelogd ter authenticatie, het gebruikte authenticatieniveau, gegevens over ondertekende en ontvangen ondertekende berichten over de gebruiker die tussen de diensten worden uitgewisseld (zoals datum en tijdstip van ontvangst), sessiegegevens en overige gegevens met betrekking tot het soort en tijdstip en kenmerken van het gebruik (zie artikel 5c, onderdeel a, onder 4°). Onder deze gegevens vallen ook de zogenaamde 'comfortgegevens': indien van toepassing, worden gegevens op het beeldscherm getoond zodat de gebruiker kan zien wie de gemachtigde is die namens hem handelingen heeft verricht. Ook zullen in het proces van gebruik enkele gegevens worden verwerkt ter identificatie van de gebruiker (of degene die hij als gemachtigde vertegenwoordigt) die toegang krijgt tot de elektronische dienst van een bestuursorgaan of aangewezen organisatie (zie artikel 5c, onderdeel a, onder 1°, 2° en 3°).

De gegevens die worden verwerkt door tussenkomst van de eIDAS-voorziening en die in het kader van de eIDAS-verordening ter zake worden voorgeschreven (zie ook paragraaf 4.1.4. van het algemeen deel van deze nota van toelichting) zijn gegeven zoals de identificerende gegevens, gebruiksgegevens, gegevens die relevant zijn voor de adequate werking van de voorziening, het burgerservicenummer, en, indien op basis van die gegevens geen zekerheid omtrent uniciteit kan worden verkregen, de geboortenaam, geboorteplaats, geslacht en adres (vgl. artikel 5d).

Bij alle bovenstaande processen worden verder gegevens over de gebruiker verwerkt die relevant zijn voor de adequate werking van de toegang tot elektronische dienstverlening (zoals kenmerken van de door de gebruiker gebruikte software en hardware, zie artikel 5c, onderdeel a, onder 6°). En, mocht de gebruiker ondersteuning behoeven, dan worden gegevens verwerkt ter identificatie van de gebruiker en andere gegevens die bij de ondersteuning nodig zijn.

Ten slotte worden gegevens verwerkt wanneer een gebruiker, telefonisch of online, contact opneemt voor ondersteuning. Om die ondersteuning te kunnen verlenen, zijn bijvoorbeeld identificerende gegevens nodig (zie artikel 5c, onderdeel a, onder 7°).

Behalve over de gebruikers van bedrijfs- of organisatiemiddelen, worden ook gegevens verwerkt over over afnemers van een erkende ontsluitende dienst (een partij die het elektronisch verkeer tussen een bestuursorgaan of aangewezen organisatie en erkende authenticatiediensten, machtigingsdiensten en attributendiensten routeert teneinde toegang tot elektronische dienstverlening te faciliteren, zie artikel 1 van de wet). Het gaat dan om administratieve gegevens die noodzakelijk zijn in verband met het gebruik door de gebruiker van een bedrijfs- en organisatiemiddel. Te denken valt aan gegevens als de naam van de bevoegde bestuurder van de rechtspersoon die gebruik maakt van de ontsluitende dienst, en de naam, de functie, het e-mailadres en het telefoonnummer van contactpersonen bij de betreffende afnemer (zie artikel 5c, onderdeel b).

Artikel 5d
Het nieuwe artikel 5d vloeit voort uit het feit, dat de minister ingevolge artikel 5, tweede lid, van de wet verantwoordelijk is voor een voorziening die het mogelijk maakt identificatiemiddelen te ontsluiten waarmee natuurlijke personen, ondernemingen en rechtspersonen uit andere EU-lidstaten toegang willen tot elektronische dienstverlening in Nederland en vice versa. Achtergrond hiervan is dat de bovenliggende EU-regelgeving, de zogeheten eIDAS-verordening, voorziet in wederzijdse erkenning

van elektronische identificatiemiddelen op de niveaus substantieel en hoog.[22] Binnen deze voorziening, die wordt aangeduid als eIDAS-voorziening, is sprake van een aantal functionaliteiten en componenten. Doel ervan is het mogelijk maken van elektronische dienstverlening aan diegenen in de EU of EER die niet (kunnen) beschikken over een toegelaten of erkend middel als bedoeld in de wet maar die, bijvoorbeeld vanwege werk of onderwijs, een relatie hebben met een of meerdere publieke dienstverlener(s) in Nederland, zoals de Belastingdienst, de SVB, het UWV of DUO. Kortgezegd dient de voorziening er toe iemand op basis van buitenlandse persoonsgegevens te herkennen. Het systeem voorziet in een - onder de verantwoordelijkheid van de minister uitgevoerde - koppeling van uit een andere lidstaat binnenkomende gegevens (onder meer naam, geboortedatum en uniek identificerend nummer) aan een versleutelde vorm van een burgerservicenummer, indien de gebruiker beschikt over een burgerservicenummer, of, indien hij niet beschikt over een burgerservicenummer, aan een afgeleide vorm van het uniek identificerend nummer.[23] Wanneer met dit proces geen zekerheid omtrent uniciteit kan worden verkregen, worden aanvullende gegevens verwerkt. Het proces resulteert uiteindelijk in het door de dienstverlener kunnen verlenen van toegang tot zijn elektronische diensten.

Artikel 5e
Belangrijk uitgangspunt van de AVG en van de Wet digitale overheid is doelbinding. Artikel 16 van de wet stelt dat de bij de uitvoering van de wet betrokken – publieke en private partijen – alleen persoonsgegevens mogen verwerken voor zover dit noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge deze wet, in het bijzonder het bieden van goede en veilige toegang tot elektronische dienstverlening en het voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening. Hieruit volgt onder meer dat commercieel gebruik van persoonsgegevens voor andere doelen dan de vervaardiging van een identificatiemiddel (dus: het 'vermarkten' van gegevens) niet is toegestaan.

De uitwerking van artikel 16, inzake persoonsgegevensverwerking en privacybescherming, geschiedt in het onderhavige besluit (zie tevens de hoofdstukken 4.1 en 5 van het algemeen deel van deze toelichting). In de artikelen 5 tot en met 5d wordt gespecificeerd welke gegevens door publieke en private partijen kunnen worden verwerkt in verband met de goede werking van identificatiemiddelen en de goede en veilige toegang met die middelen tot elektronische dienstverlening.

Om ondubbelzinnig duidelijk te maken dat het is verboden om bijvoorbeeld via het geven van toestemming toch ander (commercieel) gebruik mogelijk te maken, is artikel 5e opgenomen. Naast het formeel-juridisch vastleggen van doelbinding, is het vanzelfsprekend ook nodig om feitelijk (technische) waarborgen te eisen. Dat geschiedt door van de private aanbieders van identificatiemiddelen – als voorwaarde voor het kunnen verkrijgen van een erkenning - te eisen, dat zij zorgen voor gescheiden opslag van gegevens, waardoor gegevens over de gebruiker van het private identificatiemiddel worden bewaard op een wijze die is afgescheiden van gegevens over het gebruik van het middel door die gebruiker (zie de amvb ingevolge artikel 9 van de wet).

Artikel 5f
Onderdeel F regelt tot slot dat een nieuw artikel 5f wordt ingevoegd, opdat een grondslag wordt opgenomen voor de minister van BZK voor persoonsgegevensverwerking in het kader van het waarborgen van de veilige toegang tot en de werking van de elektronische dienstverlening en teneinde misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening te voorkomen. Het betreft een grondslag voor gegevensverwerking in het kader van misbruikbestrijding in den brede, dus over de diverse voorzieningen heen. Hiermee wordt invulling gegeven aan de aanbeveling in de PIA van 28 juni 2017, om misbruik- en incidentbestrijding op stelselniveau in te richten en de hiervoor te gebruiken gegevens uit te werken. De persoonsgegevens die de minister hiertoe van gebruikers van elektronische identificatiemiddelen voor elektronische dienstverlening kan verwerken zijn de gegevens, bedoeld in de artikelen 2 tot en met 5d, die verwerkt worden voor de inrichting,

[22] Uitvoering van (het onderdeel elektronische identificatie in) de eIDAS-verordening (EU 910/2014) is niet verplicht. Nederland heeft er voor gekozen aan te sluiten; onder de wet digitale overheid toe te laten en te erkennen identificatiemiddelen zullen bij de EU Commissie worden genotificeerd teneinde deze in andere lidstaten te kunnen gebruiken. Omgekeerd kunnen door andere lidstaten genotificeerde middelen in Nederland worden gebruikt bij de afname van elektronische diensten van publieke dienstverleners (wederzijdse erkenning)
[23] Bijlage bij (EU) Uitvoeringsverordening 2015/1501, Pb EU 2015, L 235.

beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de voorzieningen binnen de generieke digitale infrastructuur en de gegevens en inlichtingen, bedoeld in artikel 19 van de wet, die verstrekt worden door de bestuursorganen en aangewezen organisaties, aanbieders van een toegelaten identificatiemiddel en op grond van artikel 11 van de wet erkende middelenuitgevers en diensten. De minister zal die gegevens kunnen verwerken die noodzakelijk zijn voor het waarborgen van de veilige toegang tot de elektronische dienstverlening en het (pro actief) voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening. De bedoelde gegevens worden verwerkt in het kader van onderzoek naar mogelijk misbruik of oneigenlijk gebruik van de diverse voorzieningen en middelen. Dat onderzoek op zich genereert ook weer persoonsgegevens, die worden genoemd in onderdeel c.

Onderdeel G

In onderdeel G wordt artikel 6 gewijzigd dat betrekking heeft op de verstrekkingen door de Minister van BZK aan de afnemers van DigiD. De gegevens die aan afnemers van DigiD (dienstverleners) worden verstrekt, kunnen voortaan ook worden verstrekt aan de eIDAS-voorziening. Deze verstrekking is nodig op het moment dat iemand met DigiD elektronische diensten wil afnemen bij dienstverleners in andere EU-lidstaten. Ook verstrekking aan een routeringsvoorziening is mogelijk, gelet op de 'ontzorgende' functie van deze publieke voorziening richting dienstverleners.

In verband met die eIDAS-voorziening wordt ook een nieuw derde lid toegevoegd, waarin de gegevens zijn opgenomen die worden verstrekt ten behoeve van de elektronische identificatie bij grensoverschrijdende elektronische dienstverlening binnen de Europese Unie via de eIDAS-voorziening. De verstrekking van deze gegevens is noodzakelijk in het kader van de uitvoering van de eIDAS-verordening.

Verder wordt de mogelijkheid om het burgerservicenummer te verstrekken aangevuld met de verstrekking van een versleutelde of afgeleide vorm daarvan. Dit in verband met de introductie van de elektronische identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog, zoals toegelicht bij onderdeel B (wijziging van artikel 2 over de gegevens die in het kader van DigiD worden

Onderdeel H

Het aangevulde onderdeel a van artikel 8 maakt mogelijk dat op hun verzoek aan afnemers van MijnOverheid informatie wordt verschaft over het al dan niet afleveren en openen (aanklikken) van berichten door gebruikers, opdat een dergelijk signaal wordt benut om de gebruiker te rappelleren over het feit dat bij hem eerder een bericht is bezorgd. Dit is in het belang van de gebruiker zelf, het voorkomt problemen voor hem. Deze gegevensverstrekking, die alleen geschiedt wanneer een afnemer hierom verzoekt gelet op aard en belang van het desbetreffend bericht, moet daarom proportioneel en gerechtvaardigd worden geacht. Benadrukt zij dat de Minister van BZK het bericht niet inhoudelijk beziet. De informatie wordt verstrekt met als doel dat de afnemer daadwerkelijk contact zoekt met de burger. De afnemer kan deze gegevens dus alleen opvragen om vervolgens de burger (alsnog) te bereiken en kan geen rechten ontlenen aan het feit dat een bericht wel of niet gelezen is.

Het nieuwe onderdeel c van artikel 8 maakt het mogelijk inlichtingen aan een afnemer te verstrekken om de aflevering van een bericht te kunnen bevestigen. Het bezorgen van het bericht (of het überhaupt gebruiken van MijnOverheid) wordt soms betwist, waardoor sprake is van een geschil tussen afnemer en gebruiker. Het kan dan nodig zijn, bijvoorbeeld voor gebruik in een rechtszaak, dat afnemers inlichtingen ontvangen om de ontvangst van een bericht te kunnen bevestigen (zoals moment van activeren account, aanpassen mailvoorkeuren door de gebruiker of verzenden notificaties).

Onderdeel I

Dit onderdeel regelt dat de gebruikte terminologie in artikel 9 van het besluit wordt aangepast aan de Wet digitale overheid. Daarnaast wordt het ook mogelijk met deze wijziging dat de minister van BZK verstrekkingen doet van de versleutelde of afgeleide vorm van het burgerservicenummer van gebruikers van bedrijfs-en organisatiemiddelen vanuit het BSN-K aan erkende authenticatiediensten of machtigingsdiensten. Dit is noodzakelijk omdat het BSN-K met de introductie van de Wet digitale overheid ook een rol zal spelen in het versleutelingsproces bij de elektronische dienstverlening aan

gebruikers van bedrijfs- en organisatiemiddelen, namelijk bij die gebruikers wiens burgerservicenummer of een versleutelde of afgeleide vorm daarvan gebruikt wordt om een koppeling te maken tussen elektronisch identificatiemiddel en gebruiker. Op deze wijze wordt het bijvoorbeeld ook mogelijk om natuurlijke personen die een onderneming drijven (eenmanszaken) te faciliteren die inloggen met een bedrijfs- en organisatiemiddel.

Verder wordt de verstrekking geregeld vanuit het BSN-K van de afgeleide vorm van het uniek identificerend nummer in het kader van grensoverschrijdende authenticatie ter uitvoering van de eIDAS-verordening. Dat uniek identificerende nummer is ontvangen van de eIDAS-voorziening en de door het BSN-K vervaardigde afgeleide vorm daarvan wordt vanuit de eIDAS-voorziening weer verstrekt aan de bestuursorganen en aangewezen organisaties die elektronische diensten verlenen.

Onderdeel J

Artikel 9a
Wat betreft de verstrekkingen in verband met de routeringsvoorziening (artikel 9a) is bepaald dat deze zo mogelijk in versleutelde vorm worden verstrekt. De achtergrond hierbij is dat op grond van het huidige systeem van een van de aangesloten voorzieningen, namelijk DigiD, alleen onversleutelde gegevens worden verstrekt. Het is de bedoeling dat de huidige vorm van DigiD kan werken via de routeringsvoorziening, reden waarom het nodig is om te bepalen dat de gegevens ook onversleuteld kunnen worden verwerkt. De in ontwikkeling zijnde nieuwe vorm van DigiD zal wel met versleutelde gegevens kunnen en gaan werken, zodat ik de toekomst, zodra het huidige DigiD geheel is uitgefaseerd, de gegevens alleen nog in versleutelde vorm zullen worden verstrekt.

Artikel 9b
De verstrekkingen in verband met het toegelaten private identificatiemiddel (artikel 9b) zijn beperkt. De aanbieder van het middel verstrekt – vergelijkbaar met hetgeen ter zake van het publieke middel geldt - aan bestuursorganen en aangewezen organisaties (publieke dienstverleners) die elektronische diensten verlenen en aan de – dienstverleners 'ontzorgende'- routeringsvoorziening slechts het burgerservicenummer (in versleutelde of afgeleide vorm) teneinde de identiteit van de gebruiker van het desbetreffende middel te kunnen vaststellen en het betrouwbaarheidsniveau van het gehanteerde middel zodat de toegang tot de betreffende diensten op een passend veiligheids- en betrouwbaarheidsniveau kan plaatsvinden.

Artikel 9c
Ook de verstrekkingen in verband met een bedrijfs- en organisatiemiddel (artikel 9c) zijn beperkt. Erkende ontsluitende diensten (ook wel 'makelaars' genoemd) verstrekken aan publieke dienstverleners in verband met hun elektronische dienstverlening aan bedrijven een beperkte gegevensset teneinde de identiteit van de gebruiker van het desbetreffende middel (rechtspersoon of natuurlijke persoon) te kunnen vaststellen en het authenticatieniveau van het gehanteerde middel zodat de toegang tot de betreffende diensten op een passend veiligheids- en betrouwbaarheidsniveau kan plaatsvinden.

De gegevens die bij de aanvraag en uitgifte en bij het gebruik van een bedrijfs- of organisatiemiddel, tussen de diverse daarbij betrokken partijen onderling een op een kunnen worden verstrekt, zijn (kort gezegd) naam, adres en woonplaatsgegevens, identificerende nummers, overige gebruikersgegevens en de zogenaamde gebruiksgegevens (kortom, de gegevens, bedoeld in artikel 5c, onderdeel a, onder 1°, 2°, 3° en 4°). De gegevens worden steeds een op een verstrekt en deze verstrekking is geregeld in artikel 9c, eerste lid.

Ten tweede worden in lijn met de eIDAS-verordening door de authenticatiedienst via de ontsluitende dienst of een routeringsvoorziening de zogenaamde eIDAS-gegevens verstrekt in versleutelde vorm (artikel 9c, tweede lid) aan de eIDAS-voorziening, opdat identificatie van bedrijven ten behoeve van grensoverschrijdende elektronische dienstverlening binnen de EU kan plaatsvinden.

In het derde lid is de verstrekking geregeld die een erkende machtigingsdienst kan doen van het burgerservicenummer van de eigenaar met naam en geboortedatum aan het BSN-K ter activering (zie paragraaf 4.1.4. van het algemeen deel van deze nota van toelichting).

In artikel 9c, vierde lid, is de verstrekking geregeld door de ontsluitende dienst of een routeringsvoorziening aan de dienstverlener ("afnemer" in de zin van het besluit), namelijk het burgerservicenummer in versleutelde of afgeleide vorm van de gebruiker die inlogt met een middel, ten behoeve van de vaststelling van zijn identiteit. Uiteraard wordt ook het door de gebruiker gekozen authenticatieniveau aan de dienstverlener verstrekt. Op deze manier kunnen de identiteit van de gebruiker van het desbetreffende middel (rechtspersoon of natuurlijke persoon) en het authenticatieniveau van het gehanteerde middel worden vastgesteld zodat de toegang tot de betreffende diensten op een passend veiligheids- en betrouwbaarheidsniveau kan plaatsvinden.

Artikel 9d
Voor wat betreft verstrekkingen in de eIDAS-voorziening (artikel 9d), verstrekt de minister aan het BSN-K (dus: aan zichzelf, als verantwoordelijke voor het BSN-K) het burgerservicenummer van de gebruiker van een toegelaten of erkend identificatiemiddel, opdat het versleuteld kan worden. Vervolgens wordt het versleutelde burgerservicenummer aan de routeringsvoorziening (ook een verantwoordelijkheid van de minister) dan wel aan de erkende (private) ontsluitende dienst verstrekt, opdat doorzetting aan en ontzorging van de dienstverlener mogelijk wordt (artikel 9d, onderdeel a).

Voorts verstrekt de minister in verband met de eIDAS-voorziening de naam, geboortedatum, geboorteplaats, adres, en geslacht van EU-burgers die met een buitenlands erkend middel inloggen (in versleutelde vorm) aan de erkende ontsluitende dienst of de – publieke - routeringsvoorziening. Via de ontsluitende dienst ofwel de routeringsvoorziening komt die informatie dan terecht bij het bestuursorgaan of aangewezen organisatie die de elektronische dienst levert (artikel 9d, onderdeel b).

Ten slotte wordt bij grensoverschrijdende authenticatie (ingaand verkeer) het uniek identificerend nummer aan het BSN-Koppelregister verstrekt alsmede, indien beschikbaar (omdat de gebruiker in de BRP is opgenomen) het burgerservicenummer, en een afgeleide vorm daarvan aan bestuursorganen of aangewezen organisaties in het kader van elektronische dienstverlening (artikel 9d, onderdeel c).

Bij uitgaand verkeer levert de eIDAS-voorziening voor elke persoon onder meer een landspecifiek uniek identificerend nummer; dit is afgeleid van het burgerservicenummer en gaat (naar de eIDAS-voorziening in de) betreffende andere lidstaat (onderdeel d).

Artikel 10
Artikel 10 is grotendeels gelijkluidend aan het bestaande artikel 10 van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur. In verband met de bescherming van de persoonlijke levenssfeer was in artikel 10 bepaald dat verstrekking van gegevens aan anderen dan de bezoeker of de gebruiker van DigiD, DigiD Machtigen of MijnOverheid zelf (in het kader van bijvoorbeeld hun recht op inzage) slechts mogelijk is als zij daartoe toestemming hebben gegeven. Het bepaalde is nu uitgebreid tot de gebruikers van de overige voorzieningen en middelen, zoals de routeringsvoorziening en de authenticatiemiddelen. Benadrukt wordt, dat sprake moet zijn van vrijelijk gegeven toestemming; deze moet door de bezoeker of de gebruiker ook geweigerd kunnen worden. In twee gevallen is toestemming niet aan de orde. Ten eerste is geen toestemming nodig indien het gaat om het verstrekken van gegevens aan overheidsorganen of rechtspersonen met een wettelijke taak die bijvoorbeeld behulpzaam kunnen zijn in de constatering of bij bepaalde door de Minister van BZK opgemerkte signalen inderdaad sprake is van misbruik of oneigenlijk gebruik van de voorzieningen, mits dat verstrekken noodzakelijk is voor de borging van de beveiliging en betrouwbaarheid van de betreffende voorziening (onderdeel a). Dit is mede in het belang van de rechtmatige houder van een DigiD, een machtiging, een MijnOverheid-account of authenticatiemiddel in die gevallen waarin hij schade ondervindt als gevolg van misbruik of oneigenlijk gebruik ervan. Ten tweede is geen toestemming nodig indien de Minister van BZK op grond van andere wettelijke bepalingen gerechtigd is tot verstrekking van bepaalde gegevens over te gaan.

Onderdeel K

In dit onderdeel wordt geregeld dat artikel 11 zodanig wordt aangepast dat ook de bewaartermijnen voor de nieuwe persoonsgegevens die verwerkt worden door de minister van BZK in het kader van DigiD op grond van artikel 2 van het besluit aansluiten bij de bestaande systematiek. Wat betreft de nieuwe accountgegevens en gebruiksgegevens, wordt gekozen voor bewaartermijnen die overeenkomen met de bestaande bewaartermijnen voor gegevens die eenzelfde soort functie vervullen binnen DigiD. Wat betreft de gegevens die verwerkt worden bij het openen van de chip van

het Nederlands paspoort, de Nederlandse identiteitskaart of het Nederlands rijbewijs geldt dat zij na de sessie van de gebruiker niet bewaard blijven, maar enkel bewaard worden zolang de gebruiker is ingelogd, aangezien de verwerking enkel plaatsvindt om de chip te kunnen openen in het proces van activatie. De gegevens die de minister van BZK verwerkt voor de ondersteuning van de administratie van DigiD worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden. Gebleken is dat dit de periode betreft waarbinnen de factureringsprocessen richting verwerkers voor DigiD, in het kader waarvan de gegevens verwerkt worden, zijn afgerond. De gegevens die verwerkt worden in het kader van de ondersteuning van het gebruik van de afnemer worden bewaard gedurende de duur van het gebruik van DigiD door de afnemer en daarna maximaal vijf jaar. De bewaartermijn van vijf jaar is gekozen, omdat gebleken is dat dit de periode is waarin afnemers mogelijk nog verplichtingen jegens DigiD hebben lopen, waarover contact met de afnemers opgenomen dient te kunnen worden.

Om DigiD, DigiD Machtigen en Mijn Overheid te kunnen herstellen na een calamiteit worden reservekopieën van gegevens gemaakt. De reservekopieën zijn niet bruikbaar om gegevens te raadplegen of om gegevens op enige andere wijze beschikbaar te stellen. Het doel van de reservekopieën is om het gehele productiesysteem terug te kunnen zetten in het geval van een calamiteit. Omdat gegevens in de reservekopieën niet raadpleegbaar of beschikbaar zijn, wordt het maken van de reserviekopieën gezien als eerste stap in het vernietigingsproces. De reservekopieën worden maximaal vier maanden bewaard. Deze bewaartermijn is voor DigiD opgenomen in artikel 11, twaalfde lid. Aan deze termijn ligt primair ten grondslag, dat voorzieningen hersteld moet kunnen worden na een calamiteit; het kan enige tijd vergen om sommige vormen van datacorruptie of datamanipulatie te detecteren en te herstellen. Calamiteiten van deze aard kunnen doorgaans binnen enkele weken gedetecteerd en opgelost worden. Gezien het belang van de voorzieningen is het prudent om een veiligheidsmarge te hanteren. Daarom wordt de bewaartermijn van reservekopieën op vier maanden gesteld.

Overigens moet er in verband met het eventueel opvragen van gegevens voor alle nieuwe bewaartermijnen in dit besluit en alle bestaande bewaartermijnen in het met dit besluit gewijzigde Besluit verwerking persoonsgegevens generieke digitale infrastructuur rekening worden gehouden met de datums waarop deze bewaartermijnen zijn ingegaan (de inwerkingtredingsdatum van dit (wijzigings)besluit en de inwerkingtredingsdatum van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur op 1 november 2015) en de bewaartermijnen zoals die golden voor die datums. Zo zal bijvoorbeeld een gegeven van een gebruiker van DigiD uit januari 2014 niet meer beschikbaar zijn; de destijds geldende bewaartermijn van 18 maanden is immers al verlopen en de voor dat gegeven eventuele langere bewaartermijnen op grond van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur golden toen nog niet.

Onderdeel L

In dit onderdeel wordt artikel 12 zodanig gewijzigd dat de bewaartermijnen voor de nieuwe persoonsgegevens die verwerkt worden door de minister van BZK in het kader van DigiD Machtigen op grond van artikel 3 van het besluit aansluiten bij de bestaande systematiek. Wat betreft het nummer van de kamer van koophandel van de zelfstandige zonder personeel en het gegeven reden opschorting van de persoonslijst in de basisregistratie personen, wordt gekozen voor bewaartermijnen die overeenkomen met de al bestaande bewaartermijnen voor gegevens die eenzelfde soort functie vervullen binnen DigiD Machtigen. De gegevens die verwerkt worden in het kader van de ondersteuning van het gebruik van de afnemer worden bewaard gedurende de duur van het gebruik van DigiD Machtigen door de afnemer en daarna maximaal vijf jaar. De bewaartermijn van vijf jaar is gekozen, omdat gebleken is dat dit de periode is waarin afnemers mogelijk nog verplichtingen jegens Digid Machtigen hebben lopen, waarover contact met de afnemers opgenomen dient te kunnen worden. Bij onderdeel J is al toegelicht dat het maken van reservekopieën van gegevens wordt gezien als eerste stap in het vernietigingsproces. De reservekopieën worden maximaal vier maanden bewaard en alleen gebruikt ten behoeve van een calamiteit (artikel 12, achtste lid).

Onderdeel M

In dit onderdeel wordt geregeld dat artikel 13 zodanig wordt aangepast dat de gegevens die verwerkt worden in het kader van de ondersteuning van het gebruik van de afnemer van MijnOverheid worden bewaard gedurende de duur van het gebruik van MijnOverheid door de afnemer en daarna maximaal

vijf jaar. De bewaartermijn van vijf jaar is gekozen, omdat gebleken is dat dit de periode is waarin afnemers mogelijk nog verplichtingen jegens MijnOverheid hebben lopen, waarover contact met de afnemers opgenomen dient te kunnen worden. Bij onderdeel J is al toegelicht dat het maken van reservekopieën van gegevens wordt gezien als eerste stap in het vernietigingsproces. De reservekopieën worden maximaal vier maanden bewaard (artikel 13, achtste lid).

Daarnaast wordt de kortere bewaartermijn van 1 jaar voor de gegevens nationaliteit, geboortedatum en datum van overlijden geschrapt. De reden daarvoor is dat alleen de nationaliteit in afgeleide vorm (Nederlander = Ja/Nee) wordt bewaard bij het account en alleen gebruikt tijdens de duur van het aanmaakproces en bij de ontvangst van mutaties op dit gegeven. Voor het gegeven nationaliteit zelf geldt de gewone bewaartermijn van duur van het account en daarna maximaal 1 jaar. Hetzelfde geldt voor de geboortedatum, waarvan de afgeleide vorm (Is 14 jaar of ouder = Ja/Nee) wordt bewaard bij het account en alleen gebruikt tijdens de duur van het aanmaakproces en bij de ontvangst van mutaties (correcties) op dit gegeven. De datum van overlijden is niet beschikbaar bij het aanmaakproces, maar wordt later aangeleverd en blijft bewaard vanaf ontvangst van deze mutatie tot en met het verwijderen/opschonen van het account. Daarom dient ook voor dit gegeven de gewone bewaartermijn te gelden van duur van het account en daarna maximaal 1 jaar.

Tot slot wordt, met het oog op de nieuwe dienst/functie die de gebruikers van MijnOverheid informeert over algemene bekendmakingen, kennisgevingen en mededelingen die voor hen van belang zullen zijn, ingevoegd dat de betreffende gegevens over een gebruiker worden bewaard zolang het bijbehorende MijnOverheid-account bestaat, en zodra het account is opgeheven, maximaal 1 jaar. Dit is nodig om nadien fouten te kunnen herstellen en klachten te kunnen afhandelen.

Onderdeel N

Dit onderdeel regelt dat artikel 14 wordt aangepast qua terminologie op de introductie van de Wet digitale overheid en de nieuwe werkwijze van het BSN-K binnen de generieke digitale infrastructuur.

Daarnaast wordt het artikel zodanig gewijzigd dat niet langer de bewaartermijnen staan opgenomen voor de gegevens die binnen deze nieuwe constellatie niet meer als persoonsgegevens worden verwerkt door de minister van BZK.

De bewaartermijn van de naam, de geboortedatum, de datum van overlijden en het van het burgerservicenummer in versleutelde vorm is niet langer dan nodig is om de gegevens op juistheid te controleren. Voor de overige gegevens geldt een bewaartermijn zolang de koppeling tussen het middel en het burgerservicenummer in afgeleide vorm of het uniek identificerend nummer in afgeleide vorm bestaat en zodra die koppeling is beëindigd, nog maximaal 5 jaar. Deze bewaartermijn is nodig in verband met de inzagefunctie van het BSN-K, waarmee de gebruiker inzicht heeft in de status van zijn actieve middelen. Voor de gegevens die over de afnemers van het BSN-K worden bewaard geldt na afloop van het gebruik van het register nog 5 jaar vanwege verplichtingen die in die periode nog kunnen lopen van afnemers jegens het register.

Onderdeel O

Artikel 14a
De bewaartermijnen in de routeringsvoorziening (artikel 14a) zijn ingegeven door het doel van de verwerking van de gegevens: het – door te functioneren als tussenpartij die authenticaties afhandelt en doorgeleidt – 'ontzorgen' van dienstverleners in hun aansluiting op andere (publieke) voorzieningen en toegelaten of erkende identificatiemiddelen. Waar mogelijk worden gegevens meteen na gebruik van het middel verwijderd. De 18-maandstermijn na afloop van het authenticatieproces ter zake van een identificatienummer (waaronder het burgerservicenummer al dan niet in versleutelde of afgeleide vorm) in onderdeel b is ingegeven door de koppeling van de identificatie van de gebruiker van een toegelaten of erkend identificatiemiddel aan de toegang tot specifieke elektronische diensten. De gegevens worden, afhankelijk van het authenticatiemiddel dat wordt gebruikt, verwerkt gedurende de authenticatiesessie vanaf het moment dat de routeringsvoorziening de gegevens ontvangt tot aan verstrekking aan de dienstverlener. Na afloop daarvan is bewaring van maximaal 18 maanden nodig vanwege de samenhang met (de gebruikersgegevens inzake) DigiD (zie artikel 11).

De vijfjaarstermijn in de onderdelen c en d is nodig voor auditdoeleinden (audittrail) en dient ertoe ketenlogging mogelijk te maken, zodat de routeringsvoorziening een rol kan spelen bij het voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening.

Artikel 14b
De bewaartermijnen zoals die gelden ten aanzien van DigiD alsmede de – door de betreffende verwerkingsdoelen ingegeven - onderbouwing daarvoor zijn leidend voor de bewaartermijnen ter zake van het toegelaten private middel, zoals deze worden gesteld in artikel 14b. Het betreft hier immers een alternatief voor het publieke middel, waarbij uitgangspunt is dat ter zake een gelijkwaardig veiligheids- en betrouwbaarheidsniveau geldt en aan dezelfde eisen moet worden voldaan (gelijk speelveld).

Artikel 14c
Wat betreft de bewaartermijnen voor de persoonsgegevens die worden verwerkt ten behoeve van het bedrijfs- en organisatiemiddel (artikel 14c) is van belang, dat de gegevens voor vijf doelen worden verwerkt, te weten een functioneel doel (het laten werken van de systemen), een verantwoordingsdoel (zodat kan worden aangetoond dat de werkzaamheden correct zijn uitgevoerd), het doel van foutopsporing (zodat problemen, zo nodig in samenwerking met ketenpartners, kunnen worden opgelost), het doel calamiteitenbestrijding (opdat de werking van het systeem kan worden hersteld na een probleem) en de bestrijding van misbruik. Deze doelen spelen een rol bij de processen bij de aanvraag en uitgifte en bij het gebruik van een bedrijfs- of organisatiemiddel (zie paragraaf 4.1.4. van het algemeen deel van deze nota van toelichting) en dat vertaalt zich voor de verschillende gegevens die in het kader van het bedrijfs- en organisatiemiddel worden verwerkt in de volgende bewaartermijnen.
De aan de gebruiker gerelateerde gegevens (identificerende gegevens en gegevens in verband met de registratie van machtigingen) zijn zowel nodig in het proces van aanvraag en uitgifte als bij het gebruik van het middel. In verband daarmee worden deze gegevens bewaard zolang de gebruiker het middel of de machtiging gebruikt. Vanaf het moment dat dat gebruik is beëindigd, worden de gegevens nog maximaal 18 maanden bewaard.
De uitsluitend aan het gebruik gerelateerde gegevens, de gebruiksgegevens en de gegevens die relevant zijn voor de adequate werking van de toegang tot elektronische dienstverlening, worden maximaal 5 jaar bewaard, met dien verstande dat sessiegegevens direct na het uitloggen al worden gewist.
De eIDAS-gegevens worden bewaard zolang de gebruiker het bedrijfs-en organisatiemiddel of de machtiging gebruikt, en zodra dat niet meer het geval is maximaal 5 jaar. Deze bewaartermijn is nodig omdat een buitenlands middel kan worden gelinkt aan het burgerservicenummer en die koppeling ook blijft bestaan als het buitenlandse middel vervalt; andere landen geven het namelijk niet door als een middel bij hun vervalt. De termijn van maximaal vijf jaar wordt toegelicht bij artikel 14d, dat over de eIDAS-voorziening gaat en op welke bewaartermijn de bewaartermijn in het kader van het bedrijfs- of organisatiemiddel aansluit.
De bewaartermijn die nodig is voor de gegevens die bewaard worden over afnemers van een erkende ontsluitende dienst is maximaal vijf jaar.
De gegevens die nodig zijn in het kader van ondersteuning van de gebruiker worden bewaard voor de duur van de ondersteuning en daarna maximaal 18 maanden; dat is in lijn met de bewaartermijn voor gegevens in het kader van ondersteuning bij DigiD en DigiD Machtigen.

Artikel 14d
De bewaartermijnen van de gegevens die worden verwerkt in de eIDAS-voorziening zijn ingegeven door redenen van functioneel en technisch beheer (goede werking van de eIDAS-keten) en foutopsporing en misbruikdetectie. Uniek identificerende nummers, burgerservicenummers en de versleutelde vormen daarvan, worden voor maximaal vijf jaar bewaard. Reden hiervoor is dat de minister omwille van veiligheid en betrouwbaarheid enige tijd de mogelijkheid moet houden een koppeling van de Europese identiteit aan deze nummers ongedaan te maken.

Artikel 14e
De bewaartermijn van de gegevens in het kader van misbruikbestrijding in den brede, is maximaal 5 jaar na afloop van de in de artikelen 11 tot en met 14d genoemde bewaartermijnen (artikel 14e). De bedoelde gegevens worden verwerkt in het kader van onderzoek naar mogelijk misbruik of oneigenlijk gebruik van de diverse voorzieningen en middelen in het authenticatieproces. Dat onderzoek genereert op zijn beurt ook weer persoonsgegevens. De verlengde bewaartermijn is ingegeven door

de noodzaak patronen te kunnen onderkennen en (juridisch) te kunnen afhandelen; een zogeheten 'audittrail' verschaft inzicht door de jaren heen.

Onderdeel P

Het nieuwe artikel 15a geeft aan dat de gremia die ingevolge dit besluit persoonsgegevens verwerken – de Minister van BZK als verantwoordelijke voor de in het besluit genoemde voorzieningen, respectievelijk private partijen voor wat betreft privaat aangeboden middelen – deze ook (aantoonbaar) moeten beveiligen. Dit is vereist ingevolge de AVG (mn artikelen 5, 28 en 32). Omwille van de duidelijkheid en rechtszekerheid zijn in dit verband enkele elementen van de AVG in de onderhavige bepaling opgenomen; de beveiliging van persoonsgegevens vormt een dermate essentiële waarborg voor burgers, dat die in het besluit geëxpliciteerd is. Hiertoe biedt (overweging 8 van) de AVG nadrukkelijk de ruimte. Detailuitwerking zal geschieden in de werkprocessen van de genoemde verwerkers; hierbij dient transparantie te worden betracht.

Onderdeel Q

Artikel 16

Hoofdstuk 5 van dit besluit richt zich tot bestuursorganen en aangewezen organisaties in de zin van de wet digitale overheid, oftewel (publieke) dienstverleners. Artikel 16 is een inleidende ('paraplu') bepaling, die in de navolgende artikelen wordt uitgewerkt. De paragrafen 5.1 en 5.2 dienen ter uitvoering van lid 1 van artikel 4 van de wet en behelzen de uitwerking van het beheer(ssysteem) inzake informatieveiligheid van de toegang tot elektronische dienstverlening. Gesproken wordt ook wel over informatiebeveiliging, om de voortdurendheid en het cyclische karakter van het proces tot uiting te brengen.

Lid 1:

Dienstverleners zijn verantwoordelijk voor het eigen primaire proces en dus ook voor de veilige toegang tot de digitale dienstverlening. Uitgangspunt hierbij is risicomanagement: om tot de juiste beveiliging van informatie(systemen) te komen, moeten dienstverleners risicogebaseerd te werk gaan. Dit betekent dat risico's inzichtelijk en systematisch moeten worden geïnventariseerd, beoordeeld en beheersbaar gemaakt (zie artikel 1). Dienstverleners maken dus een eigen, bewuste, beoordeling en moeten verantwoord omgaan met risico's, waarbij de te hanteren wegingsfactoren tevens gericht zijn op consistentie, harmonisatie en uniformiteit en daarmee de veiligheid van het geheel. Inherent aan risicogebaseerde bedrijfsvoering is dat dat de uitkomsten van een risicoanalyse en de te nemen maatregelen (waaronder het accepteren van restrisico's) per dienstverlener kan verschillen; het betreft immers maatwerk. De ruimte die individuele dienstverleners hebben, wordt – om redenen van goede werking en veiligheid van de toegang tot elektronische dienstverlening in Nederland - door dit Besluit in zekere mate geüniformeerd en ingeperkt. Het door dienstverleners op te stellen, op risicoanalyse en risicoafweging gebaseerde, informatieveiligheidsbeleid en de in dat verband te nemen maatregelen dienen in ieder geval de aspecten te behelzen, zoals aangegeven in de (hiernavolgende) artikelen van deze paragraaf.

Lid 2:

Risicomanagement mag geen betrekking hebben op elektronische identiteitsverificatie. Elektronische identificatie en authenticatie zijn immers strict gereguleerd in de wet Digitale overheid; wanneer een elektronisch identificatiemiddel aan de daarvoor geldende eisen voldoet[24] is een dienstverlener verplicht dit middel te accepteren bij het verlenen van toegang tot zijn elektronische diensten. Er is voor dienstverleners derhalve geen ruimte voor het stellen van meer of minder vergaande toegangseisen op basis van een eigen risico-inschatting

Lid 3:

[24] De ter zake geldende eisen zijn ontleend aan Uitvoeringsverordening (EU) 2015/1502 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van verordening (EU) nr. 910/2014 (eIDAS).

Veilige toegang tot elektronische dienstverlening maakt onderdeel uit van het integrale informatieveiligheidsbeleid van een organisatie. Op haar beurt maakt informatieveiligheid deel uit van de bedrijfsvoering (primaire proces). Het op te stellen veiligheidsplan behoeft in dit verband jaarlijks actualisering. Informatiebeveiliging is een continu proces; in dit verband is sprake van een 'Plan-Do-Check-Act' cyclus, waarbij naast een plan jaarlijks een verslag wordt opgesteld en dit wordt geëvalueerd (zogeheten planning en control-cyclus).

Lid 4:

Dit lid geeft de minister de bevoegdheid om nadere regels te stellen met betrekking tot de werking en beveiliging van de toegang tot elektronische dienstverlening. De in hoofdstuk 5 van dit Besluit gereguleerde aspecten van informatieveiligheid kunnen derhalve onderwerp zijn van nadere (uitvoerings)regels. Het gaat daarbij om (technische) details, waarbij het principe van risicogebaseerde bedrijfsvoering ongemoeid wordt gelaten. Het kan verder noodzakelijk zijn om nadere regels te stellen met betrekking tot de beschikbaarheid van elektronische dienstverlening als element van informatieveiligheid. De privaatrechtelijke afspraken die thans in zogeheten Service Niveau Overeenkomsten (SNO's) en Dossier Afspraken en Procedures (DAP's) zijn opgenomen, kunnen aldus publiekrechtelijk geregeld worden. Het kan hier bijvoorbeeld gaan om operationele procedures, onderhoud(skalenders), informatie over releasebeheer en continuïteit.

Artikelen 17-18

Informatiebeveiliging is geen vanzelfsprekendheid, maar moet georganiseerd worden. Intern moeten taken, verantwoordelijkheden en coördinatie worden belegd en moeten er beheersmaatregelen worden genomen, onder meer ter zake van het gebruik van bedrijfsmiddelen (zoals computers en mobiele apparatuur) en informatieclassificatie (vaststellen van het benodigde beschermingsniveau van informatie behorend bij het belang ervan voor de dienstverlener). Bij de invulling en concrete vormgeving hiervan bestaat de nodige ruimte en is maatwerk mogelijk, zij het dat de organisatie en de maatregelen moeten passen bij het risicoprofiel van de desbetreffende dienstverlener. Hetzelfde geldt voor personeelsbeleid en beveiliging van de (fysieke) omgeving. Beheersmaatregelen betreffen bijvoorbeeld screening en opleiding, het realiseren van toegangsrechten, sleutelbeheer, zonering en onderhoud. Van belang is dat dienstverleners een bewuste en integrale afweging maken bij het beveiligen van de toegang tot elektronische dienstverlening en dat ze de voor hen relevante aspecten bij die afweging betrekken. Bovendien moeten de genomen maatregelen inzichtelijk en toetsbaar zijn.

Artikel 19

De in dit artikel genoemde maatregelen – die, evenals de andere bepalingen in dit hoofdstuk, aan de individuele dienstverlener ruimte laten voor maatwerk - zijn nodig om een goede en veilige toegang tot elektronische dienstverlening te kunnen bieden en misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening te voorkomen. Bij de uitvoering hiervan verwerken bestuursorganen en aangewezen organisaties de hiertoe benodigde persoonsgegevens, in het bijzonder het burgerservicenummer, van gebruikers (houders) van elektronische identificatiemiddelen die bij hen elektronische diensten afnemen. Dienstverleners (afnemers) zijn hiertoe gelegitimeerd ingevolge de verstrekkingsbepalingen in het onderhavige Besluit en ingevolge de artikelen 16, 18-19 van de wet.

Bescherming en beveiliging van gegevens zijn onderwerp van regulering in de Europese Algemene Verordening Gegevensbescherming (AVG). Relevant in dit verband zijn de artikelen 25 en 32 AVG. Deze bepalingen zijn voor dienstverleners in de lidstaten rechtstreeks toepasselijk, maar zijn dermate ruim geformuleerd dat nadere uitwerking in (sectorspecifieke) regelgeving in de rede kan liggen. Met hoofdstuk 5 van het onderhavige Besluit, in het bijzonder artikel 19, wordt hieraan invulling gegeven. Hierbij zij opgemerkt dat dit artikel ziet op ICT-voorzieningen en informatiesystemen (zie ook de definitiebepaling). Artikel 19 bevat geen verplichting tot opstelling van een *privacy-impact analyse* (PIA). Dit wil echter niet zeggen, dat een ten behoeve van het opstellen van informatieveiligheidsbeleid benodigde risicoanalyse geen PIA hoeft te omvatten. Gelet op artikel 35 AVG is het de verantwoordelijkheid van de dienstverleners om dit wel of niet te doen, afhankelijk van de aard van hun dienstverlening en de toegang daartoe, alsmede van de omstandigheden van het geval. Aan de hand van de voorwaarden in artikel 35 AVG zullen dienstverleners dus zelf moeten bezien of zij een PIA moeten (doen) opstellen.

Tot slot is van belang te benadrukken, dat wanneer dienstverleners opdrachten verlenen aan (ICT)leveranciers, zij - als verantwoordelijke - moeten bewerkstelligen dat de betreffende leveranciers, mede met inachtneming van de AVG, de benodigde beveiligingsmaatregelen treffen.

Artikel 20

Lid 1-2:

Ook de bepalingen in paragraaf 5.2 dienen ter uitvoering van lid 1 van artikel 4 van de wet. De door dienstverleners toe te passen technische standaarden zullen bij ministeriële regeling worden aangewezen. Naar verwachting zal het hier in eerste instantie gaan om de koppelvlakken SAML en CGI. Het tweede lid bevat een gelijkwaardigheidsclausule. Dit heeft als voordeel, dat dienstverleners ruimte hebben voor de toepassing van andere dan de bij ministeriële regeling voorgeschreven technische standaarden, mits deze - gelet op de werking van de betrokken systemen - aantoonbaar een gelijkwaardig beschermingsniveau bieden. Om discussie over de beoordeling van de gelijkwaardigheid te voorkomen, is er tevens in voorzien dat het aantonen van een gelijkwaardig beschermingsniveau dient te geschieden door een onafhankelijke en gekwalificeerde (nationale of internationale) auditor. Zie tevens de toelichting bij artikel 24.

Artikel 21

Zoals gezegd laten de artikelen 16 tot en met 19 aan dienstverleners ruimte voor eigen invulling. Genoemde bepalingen zijn doelvoorschriften, die dienstverleners de gelegenheid geven tot het operationaliseren ervan in bij hun risicoprofiel passende concrete en toetsbare maatregelen (maatwerk). Het onderhavige artikel maakt het voor dienstverleners mogelijk om te voldoen aan het bepaalde in de artikelen 16 tot en met 19 van dit Besluit, indien zij met betrekking tot de toegang tot hun elektronische dienstverlening de voor hen relevante ISO/NEN-normen voor informatiebeveiliging toepassen. Deze norm wordt dus niet dwingend aan de dienstverleners opgelegd; het volgen ervan levert echter het vermoeden op dat zij aan de eisen van de artikelen 16-19 voldoen.[25] In deze norm zijn de desbetreffende onderdelen en maatregelen namelijk geïncorporeerd (in het jargon: geselecteerd of geïmplementeerd). ISO/NEN 27001 heeft betrekking op (de eisen ter zake van) managementsystemen voor informatiebeveiliging en wordt wereldwijd gebruikt als (uniformerende) basis voor informatiebeveiliging. Bijbehorende (uitvoerings)norm ISO/NEN 27002 bevat praktische handvatten voor de implementatie van ISO 27001. Beide zijn ook als Europese norm vastgesteld (NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017). Voor zorginstellingen geldt een vergelijkbare bepaling: voor hen is het mogelijk om te voldoen aan het bepaalde in de artikelen 16 tot en met 19 van dit Besluit, door norm ISO/NEN 7510 toe te passen. Deze norm behelst de sectorspecifieke uitwerking van ISO/NEN 27001, 27002 en 27799[26] voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de Nederlandse gezondheidszorg. ISO/NEN 7510 is dus een integraal normenkader voor informatiebeveiliging, toegespitst op de zorg.[27] Toepassing ervan dient door de dienstverlener te worden aangetoond door overlegging van een verklaring van een onafhankelijke en gekwalificeerde (nationale of internationale) auditor.

Artikel 22

De bepalingen in paragraaf 5.3 (artikelen 22-24), dienen ter uitvoering van de leden 2 en 3 van artikel 4 van de wet, ingevolge welke dienstverleners moeten kunnen aantonen dat zij voldoen aan de regels inzake informatieveiligheid voor wat betreft de toegang tot hun elektronische dienstverlening.

Het onderhavige artikel verplicht dienstverleners in dit verband te voldoen aan de door de minister gestelde testcriteria voor aansluiting op de voor hen in het kader van toegang relevante – dus waarop zij (moeten) aansluiten – (gdi)voorzieningen, waaronder het gebruik van een gangbare browser en het hebben van een zichtbaar beveiligde verbinding. De testcriteria, die betrekking hebben op techniek en communicatie, zijn vindbaar op www.logius.nl. Bij een nieuwe aansluiting mag voor het overleggen van een auditrapport aan de minister niet gewacht worden tot 1 mei van het opvolgende kalenderjaar,

[25] Conform Ar 3.48 Aanwijzingen voor de regelgeving. De betreffende normen zijn beschikbaar voor medewerkers van (uitvoeringsinstanties van) het Rijk (via lees-rijk.nl), provincies, gemeenten en waterschappen (via NEN Connect).
[26] Medische informatica – Informatiebeveiligingsmanagement in de gezondheidszorg volgens ISO 27002.
[27] Beschikbaar via https://www.werkenmetnen7510.nl/normen/download7510.

maar moet het bestuursorgaan of de aangewezen organisatie reeds binnen 2 maanden na aansluiting (ten eersten male) rapporteren. De eerstvolgende rapportage dient te worden ingediend conform het eerste lid van artikel 24, met dien verstande dat in de eerste 12 maanden na aansluiting hooguit eenmaal een auditrapport hoeft te worden ingediend. Het herhaaldelijk niet aan de testcriteria voldoen kan aanleiding zijn voor door de minister te nemen maatregelen (zie ook artikel 24 van dit besluit en artikel 16 van de wet).

Artikel 23

Ingevolge dit artikel leggen dienstverleners gegevens vast over het gebruik van hun ICT-voorzieningen, teneinde de controle van de juiste werking ervan mogelijk te maken in relatie tot toegang tot hun elektronische dienstverlening. Doel is het, door middel van het (met risicogebaseerde bedrijfsvoering samenhangend) regelmatig checken van alle transacties, waarborgen van de veilige toegang, het voorkomen van misbruik of oneigenlijk gebruik van de toegang, het kunnen managen van incidenten (alarmeringen) en disputen.[28] De te verwerken gebruiksgegevens (lid 2) kunnen verschillen naar gelang de (technische) omstandigheden van het geval. In dit verband worden gegevens verstrekt aan de minister indien nodig ingevolge de artikelen 18 en 19 van de wet. Zie in dit verband ook artikel 5f van dit Besluit, ingevolge welke bepaling de minister bepaalde gegevens kan verwerken, indien dit noodzakelijk is voor het waarborgen van de veilige toegang tot de elektronische dienstverlening en het voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening.

Artikel 24

Leden 1-3 en 5:

Dienstverleners moeten hun informatieveiligheidsbeleid met betrekking tot de toegang tot elektronische dienstverlening laten beoordelen. Dit geschiedt door de uitvoering van een controle van hun informatiesystemen, op basis van een door de dienstverlener opgesteld (evaluatie)verslag; de resultaten moeten bij een jaarlijks uit te voeren audit worden betrokken.[29] De op basis hiervan opgestelde rapportage dient onderdeel uit te maken van de reguliere verantwoording (planning en control-cyclus) en dient daarnaast jaarlijks[30] via de voorgeschreven gestandaardiseerde methode,[31] door de dienstverleners te worden overlegd aan de minister. Bij het opstellen van de rapportage dienen de hiertoe vastgestelde ICT-beveiligingsrichtlijnen in acht te worden genomen.[32] Elementen van het assessment zijn onder meer netwerkveiligheid (systeem- en infrastructuurkoppelingen) besturingssysteem, basisbeveiliging, applicatiebeveiliging en penetratietest.[33] Het gaat hierbij om het beoordelen van de opzet van het beveiligingsproces en het toetsen van het bestaan van beheersmaatregelen. De focus (gesproken wordt wel van *scope of applicability*) ligt daarbij op de (technische) ICT-voorzieningen en de bijbehorende beheersprocessen. Reden hiervoor is het uitgangspunt om, om redenen van uitvoerbaarheid, de auditlast van dienstverleners niet te verzwaren. Dit betekent dat fysieke en personele beveiliging, hoewel dit door dienstverleners verplicht toe te passen onderdelen van het informatieveiligheidsbeleid zijn en onderwerp vormen van hun (reguliere) horizontale verantwoording, niet onderworpen worden aan een auditbeoordeling door de minister. Ook de verwerking van persoonsgegevens en privacybescherming, ter zake waarvan ingevolge de - rechtstreeks toepasselijke - AVG voor dienstverleners een verantwoordingsplicht bestaat,[34] is geen verplicht onderdeel van de onderhavige rapportage aan de Minister. Op basis van

[28] Voor de zorg geldt terzake de sectorspecifieke norm NEN 7513, dat strookt met ISO/NEN 7510 (zie artikel 21, tweede lid, van het onderhavige besluit).
[29] *Auditing* is het intern of extern (laten) controleren van een organisatie en de daarin uitgevoerde processen of onderdelen daarvan.
[30] Voor nieuwe aansluitingen geldt bovendien dat rapportage voor het eerst plaats moet vinden binnen 2 maanden na aansluiting.
[31] Vindbaar op: www.logius.nl/ondersteuning/digid/beveiligingsassessments.
[32] Normenkader ICT-beveiligingsassessments DigiD versie 2.0 dd december 2016. Vindbaar op: www.logius.nl/ondersteuning/digid/beveiligingsassessment. Voor auditors is ter zake een handreiking opgesteld door NOREA (de beroepsorganisatie van ICT-auditors), teneinde een uniform toetsbaar kader te bieden voor het uitvoeren van de assessments.
[33] Vindbaar op: www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221 norm_ict-beveiligingsassessments.
[34] Artikel 30 AVG. De Autoriteit Persoonsgegevens (AP) houdt hierop toezicht.

opgedane ervaringen (ingevolge artikel 23 van de wet dient er binnen vijf jaar na de inwerkingtreding geëvalueerd te worden, in het bijzonder ten aanzien van beveiliging en privacybescherming) zal bezien worden of brede en meer integrale rapportage aan de minister opportuun is. Naast het beoordelen van de opzet van het beveiligingsproces en het bestaan van beheersmaatregelen, wordt in de rapportage ingegaan op de werking van de beveiliging indien door de minister is bepaald dat de audit hierop mede betrekking heeft. Aan de hand van de overlegde rapportages kan worden bezien in hoeverre dienstverleners aan de veiligheidseisen voldoen en of er ten opzichte van de vorige jaren verschuiving, verbetering of verslechtering heeft plaatsgevonden. Bij deze beoordeling geeft de minister – op een risicoclassificatie gestoelde en binnen een voorgeschreven termijn te realiseren - verbeterpunten aan, mede op basis waarvan de dienstverlener een verbeterrapport moet (laten) opstellen. Dit verbeterrapport moet worden opgestuurd aan de minister.

De Minister gebruikt de verkregen informatie om informatieveiligheid te kunnen monitoren alsmede om regulier, al dan niet sectorspecifieke, stelsel-risicoanalyses te kunnen uitvoeren. Hierbij wordt met name bezien of sprake is van een risico voor de toegang tot elektronische dienstverlening. De Minister kan ter zake, afhankelijk van aard, ernst en omvang van niet-naleving en mits proportioneel, (interbestuurlijke) maatregelen nemen. Hij is immers verantwoordelijk voor toezicht ter zake (artikel 17, vierde lid, van de wet). In het ultieme geval kan hij zonder aankondiging vooraf overgaan tot het opschorten of afsluiten van de toegang, zoals bij (dreigende) beveiligingsinbreuken (artikel 18 van de wet). Naar verwachting gaat er preventieve werking uit van deze bevoegdheden.

Leden 4 en 6:

De dienstverlener dient ten behoeve van de doorlichting een onafhankelijke (externe) en ter zake gekwalificeerde auditor in te schakelen. Deskundigheid en betrouwbaarheid dienen aantoonbaar te zijn. Hiervan is volgens bestaand beleid sprake van bij registratie bij de beroepsorganisatie van IT-auditors NOREA, of van accreditatie bij de Raad voor Accreditatie (de nationale accreditatie-instantie, RvA) of een gelijkwaardige Europese of internationale instelling, zoals de leden van de EA[35] of het *International Accreditation Forum*. Van deze instellingen is zeker dat de leden voldoen aan bepaalde opleidingseisen en onderworpen zijn aan nationale en internationale (bijvoorbeeld ethische) regelgeving. Daarnaast zijn ze onderworpen aan kwaliteitstoezicht. Het is aan de minister om te bepalen of een niet bij een van de genoemde organisaties aangesloten auditor, die ten behoeve van een dienstverlener een audit als bedoeld in dit Besluit uitvoert, geschikt (deskundig en betrouwbaar) is. De Minister kan ter zake beleidsregels vaststellen. Initieel zal van deze mogelijkheid gebruik gemaakt worden waarbij aangesloten wordt bij de huidige praktijk waarbij bij NOREA aangesloten auditors zullen worden aangemerkt als auditors die voldoen. Dit laat onverlet dat ook andere auditors moeten kunnen worden ingezet bij de uitvoering van de beveiligingsassessments. Het bepaalde geeft de mogelijkheid om op enig moment ook andere auditors toe te laten.

De vorm waarin rapportage plaats vindt, is die van een verklaring van conformiteit die een oordeel omvat "met een redelijke mate van zekerheid". Het is aan het professionele oordeel van de auditor om te bepalen of hij mede kan steunen op de rapportage van de auditor van bijvoorbeeld een leverancier. De rapportage, in jargon ook wel aangeduid met de term *assurance* - kan hiertoe een *Third Party*-mededeling van een derde inzake de desbetreffende beheerprocessen bevatten. Een dergelijke verklaring kan slechts eenmaal gebruikt worden en mag niet ouder zijn dan 12 maanden. Het uitbesteden van delen van het auditproces (*outsourcing*) laat de verantwoordelijkheid van de dienstverlener onverlet.

Voor wat betreft de wijze van auditing: deze vindt plaats op basis van een vooraf, aan de hand van een vast format, vastgesteld auditplan (schematische aanpak) met betrekking tot de desbetreffende dienstverlener. Het jaarlijks (laten) uitvoeren van een audit en de rapportage ter zake brengen voor de desbetreffende dienstverlener kosten met zich mee. De minister van BZK brengt voor zijn (monitorings)werkzaamheden aan de dienstverlener geen afzonderlijke kosten in rekening. De kosten ter zake zijn verdisconteerd in de kosten voor de voorzieningen en de toelating van identificatiemiddelen ingevolge de wet digitale overheid en worden aldus doorberekend aan de dienstverleners.

[35] www.european-accreditation.org/ea-members

De minister kan beleidsregels stellen met betrekking tot de wijze van beoordeling en rapportage. Het kan daarbij onder meer gaan om richtlijnen over de manier van toetsen *(guidance* voor de auditor, vergelijkbaar met een controleprotocol voor accountants, teneinde grote verschillen bij de beoordeling te voorkomen), nadere eisen aan de inrichting/vormgeving van de verklaring/het certificaat en het voor dienstverleners mogelijk maken van meervoudige/clustersaansluiting op de routeringsvoorziening teneinde de kosten voor audits en rapportage te beperken.

Tot slot is het voor gemeenten mogelijk jaarlijks over informatieveiligheid te rapporteren via de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Dit houdt in dat gebundeld verantwoording aan de gemeenteraad kan plaatsvinden alsmede een separate rapportage aan de Minister.[36]

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

[36] https://www.ensia.nl