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 Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 2018, nr..../CZW/SB;
Gelet op de artikelen 4 en 14 van de Wet Digitale overheid;
De Afdeling advisering van de Raad van State gehoord (advies van.... 2018, No.WO...);
Gezien het nader rapport van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van.... 2018 nr BZK/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. De definitie van "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;
2. Na "afnemer van DigiD en DigiD Machtigen" worden drie definities ingevoegd, luidende:
afnemer van een erkende ontsluitende dienst, bedoeld in artikel 12, tweede lid, van de wet: een bestuursorgaan of aangewezen organisatie die in het kader van elektronische dienstverlening aan de gebruiker van een bedrijfs- en organisatiemiddel gebruik maakt van een erkende ontsluitende dienst, bedoeld in artikel 12, 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;
3. De definitie "BSN-Koppelregister" komt te luiden:
BSN-Koppelregister: de voorziening, bedoeld in artikel 5, eerste lid, onder d, van de wet;
4. De definitie "authenticatie" vervalt.
5. De definitie "DigiD" komt te luiden:
DigiD: de voorziening voor uitgifte of activatie van publieke identificatiemiddelen, waarbij onderscheiden kan worden in drie betrouwbaarheidsniveaus, laag, substantieel en hoog, en authenticatie die bereikbaar is via het webadres www.digid.nl;
6. Na "DigiD Machtigen" wordt een tweetal 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.
7. Na "persoonsgegevens" wordt een definitie ingevoegd, luidende:
routeringsvoorziening: de voorziening, bedoeld in artikel 5, eerste lid, onder c, van de wet;
8. Onder vervanging van de punt door een puntkomma aan het einde van de definitie "vertegenwoordigde in mijn overheid", worden de volgende definities toegevoegd:
informatieveiligheid /informatiebeveiliging: 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;
beschikbaarheid: de mate waarin een informatiesysteem toegankelijk is;
integriteit: betrouwbaarheid

vertrouwelijkheid: het ontsluiten van gegevens door een daartoe bevoegde;
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;
de 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 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 het nummer van een Nederlands rijbewijs en gegevens met betrekking tot het rijbewijs, zoals de geldigheidsdatum".
2. In onderdeel c, onder 3°, wordt na "het versleutelde wachtwoord" ingevoegd ", de gemaskeerde pincode" en wordt "het mobiele telefoonnummer" vervangen door "het mobiele telefoonnummer, de gekozen document soort 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 6°, wordt "ondersteuning van de gebruiker" vervangen door "ondersteuning van de gebruiker of de administratie van DigiD".
4. Aan onderdeel c worden drie onderdelen 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 bedoeld in artikel 5d die noodzakelijk zijn voor de elektronische identificatie terzake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eIDAS-voorziening.

5. 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, indien van toepassing, 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 vorm daarvan ter identificatie van de gebruiker van DigiD Machtigen of het door de Kamer van Koophandel, genoemd 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".
3. 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, indien van toepassing, 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 een versleutelde vorm daarvan ter identificatie van de gebruiker van MijnOverheid;".
2. 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.
3. 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.
4. Er wordt een onderdeel toegevoegd:
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 over de gebruiker van een toegelaten privaat of publiek identificatiemiddel of erkend bedrijfs- of organisatiemiddel die dit middel wil gebruiken in het kader van elektronische dienstverlening:
a. de naam en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum en de datum van overlijden;
b. het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de gebruiker van een toegelaten privaat of publiek identificatiemiddel of bedrijfsmiddel;
c. de datum van totstandkoming en het niet langer gebruiken van de koppeling tussen het toegelaten private of publieke identificatiemiddel of bedrijfs- of organisatiemiddel en de van het burgerservicenummer afgeleide versleutelde vorm ter identificatie van de gebruiker;
d. statusgegevens van de aan de gebruiker gekoppelde middelen

F

Na artikel 5 worden vijf artikelen ingevoegd, luidende:

Artikel 5a. Persoonsgegevens routeringsvoorziening

Onze Minister verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging 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, het uniek identificerend nummer in geval van authenticatie buiten Nederland en binnen de EU, geboortenaam, geboorteplaats, actueel adres en geslacht, in voorkomend geval in versleutelde vorm;
2°. het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de gebruiker van een elektronisch identificatiemiddel.
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 authenticatiemiddel en authenticatieniveau, de website van de instelling 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;
b. de door een gemachtigde vertegenwoordigde: het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de vertegenwoordigde;
c. over 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 toegelaten privaat identificatiemiddel
De aanbieder van een toegelaten privaat identificatiemiddel als bedoeld in artikel 9 van de wet, verwerkt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de voorziening voor de uitgifte en authenticatie van het toegelaten privaat identificatiemiddel over gebruikers van de voorziening, bedoeld in de aanhef:
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, het versleutelde 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 de voorziening, bedoeld in de aanhef, is ingelogd, handelingen van de gebruiker, het door de gebruiker van de voorziening gekozen authenticatieniveau, de website van de instelling waar de gebruiker van de voorziening een toegelaten privaat authenticatiemiddel aanvraagt of vanuit welke de gebruiker van het toegelaten privaat identificatiemiddel met het privaat identificatiemiddel inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik;
e. gegevens die relevant zijn voor de adequate werking van de voorziening, bedoeld in de aanhef, waaronder in ieder geval de kenmerken van de door de gebruiker van de voorziening 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 van de voorziening, bedoeld in de aanhef.

Artikel 5c. Persoonsgegevens bedrijfs- en organisatiemiddel
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 vorm daarvan, het pseudoniem in versleutelde vorm het uniek identificerend nummer in geval van authenticatie buiten Nederland in versleutelde vorm, het nummer van de Kamer van Koophandel;
3°. gegevens betreffende uitgevoerde verificaties en validaties, waaronder het versleutelde wachtwoord, validaties van inschrijvingen in het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 2007, van handgeschreven handtekeningen, van een identiteit door bankoverschrijving, van elektronische handtekeningen, van authenticaties in het elektronische registratieproces en controles van machtigingen;
4°. gegevens noodzakelijk voor de registratie van een machtiging, waaronder de identiteit van de gemachtigde en machtigingsverlener, de dienst ter afname waarvan de machtiging is verleend en de looptijd en status van de machtiging;
5°. 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, handelingen van de gebruiker, het door de gebruiker van een bedrijfs- en organisatiemiddel gebruikte authenticatieniveau, 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;
6°. gegevens afkomstig van het authenticatiemiddel van de gebruiker, waarmee hij heeft ingelogd ter authenticatie;

7°. ondertekende en ontvangen ondertekende berichten over een gebruiker;
8°. gegevens bedoeld in artikel 5d die noodzakelijk zijn voor de elektronische identificatie terzake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eidas-voorziening.
9°. 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;
10°. gegevens noodzakelijk voor de ondersteuning van de gebruiker, waaronder het burgerservicenummer 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, 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 middelenuitgever, een erkende authenticatiedienst, een erkende ontsluitende dienst, een erkende machtigingsdienst of een attributendienst, bedoeld in artikel 12, derde lid, van de wet, 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, beveiliging en betrouwbaarheid 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 ingeval van authenticatie buiten Nederland en binnen de EU;
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;
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;
g. versleutelde vorm van het burgerservicenummer.
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. Persoonsgegevens misbruik generieke digitale infrastructuur
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 17 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.
G
Artikel 6 wordt als volgt gewijzigd:
1. In de aanhef wordt na "de afnemers van DigiD" ingevoegd "en de eidas-voorziening".
2. In onderdeel a, wordt "het burgerservicenummer" vervangen door"het burgerservicenummer, of een versleutelde vorm daarvan ter identificatie van de gebruiker van DigiD,".

3. Er wordt een lid toegevoegd, luidende:
3. 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 terzake van grensoverschrijdende elektronische dienstverlening binnen de Europese Unie welke plaatsvindt door tussenkomst van de eidas-voorziening.

H

Artikel 9 komt te luiden:

Artikel 9. Verstrekkingen in verband met het BSN-Koppelregister

Onze Minister verstrekt het burgerservicenummer 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, in versleutelde vorm aan de routeringsvoorziening ten behoeve van de bedoelde bestuursorganen of aangewezen organisaties en aan de erkende ontsluitende diensten.

I

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, het uniek identificerend nummer in geval van authenticatie buiten Nederland geboortenaam, geboorteplaats, actueel adres en geslacht en het gebruikte authenticatieniveau van de gebruiker van een toegelaten privaat of publiek identificatiemiddel die dit middel gebruiken in het kader van elektronische dienstverlening door bestuursorganen of aangewezen organisaties, en het burgerservicenummer van de door een gemachtigde vertegenwoordigde, zo mogelijk in versleutelde vorm aan de bedoelde bestuursorganen of aangewezen organisaties.

Artikel 9b. Verstrekkingen in verband met het toegelaten privaat identificatiemiddel

De aanbieder van een toegelaten privaat identificatiemiddel verstrekt aan de afnemers van de voorziening voor de uitgifte en authenticatie van het toegelaten privaat identificatiemiddel:
a. het burgerservicenummer of een versleutelde vorm daarvan ten behoeve van de vaststelling van de identiteit van de gebruiker van de voorziening, bedoeld in de aanhef;
b. het door de gebruiker van de voorziening, bedoeld in de aanhef, en het gekozen betrouwbaarheidsniveau.

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

1. Een erkende middelenuitgever, een erkende authenticatiedienst, een erkende ontsluitende dienst, een erkende machtigingsdienst of een attributendienst, bedoeld in artikel 12, derde lid, van de wet, verstrekkenaan de eidas-voorziening: de gegevens, bedoeld in artikel 5c, onderdeel a, onder 8°, in versleutelde vorm.
2. Een erkende ontsluitende dienst verstrekt aan afnemers in verband met hun elektronische dienstverlening aan de gebruikers van een bedrijfs- en organisatiemiddel:
1°. het burgerservicenummer in versleutelde vorm en het pseudoniem in versleutelde vorm, ten behoeve van de vaststelling van de identiteit van de gebruiker van een bedrijfs- en organisatiemiddel;
2°. het door de gebruiker van een bedrijfs- en organisatiemiddel gekozen authenticatieniveau;
3°. de voornaam, achternaam, geboortedatum of de daarvan afgeleide leeftijd of leeftijdscategorie, geboortenaam, geboorteplaats, actueel adres, e-mailadres, telefoonnummer en geslacht in versleutelde vorm.

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

Onze Minister verstrekt 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 aan de routeringsvoorziening en de erkende ontsluitende dienst in de zin van artikel 1 van de wet de versleutelde vorm van het burgerservicenummer.

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 5e, onderdeel c, over 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.

J

Artikel 11 wordt als volgt gewijzigd:
1. In het vijfde lid wordt "en de status van het account "vervangen door "de status van het account, de gekozen document soort 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".
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 drie 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 1 week 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.

K

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 wordt een lid 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.

L

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. Er wordt een lid toegevoegd, luidende:
7. 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.

M

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. naam, geboortedatum en datum van overlijden worden niet langer bewaard dan nodig is om de gegevens op juistheid te controleren;
b. het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de gebruiker van een toegelaten privaat of publiek identificatiemiddel of erkend bedrijfs- of organisatiemiddel wordt maximaal 18 maanden na registratie van de koppeling bewaard;
c. de datum van totstandkoming en het niet langer gebruiken van de koppeling tussen het toegelaten private of publieke identificatiemiddel of erkende bedrijfs- of organisatiemiddel en het van het burgerservicenummer afgeleide nummer ter identificatie van de gebruiker wordt maximaal 18 maanden bewaard.

N

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 worden bewaard zolang de gebruiker het identificatiemiddel gebruikt;

b. het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de gebruiker van een toegelaten privaat of publiek identificatiemiddel of erkend bedrijfs- of organisatiemiddel en het burgerservicenummer of een versleutelde vorm daarvan ter identificatie van de door een gemachtigde vertegenwoordigde worden maximaal 18 maanden na registratie van de koppeling 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 door de routeringsvoorziening en daarna maximaal vijf jaar.

Artikel 14b. Bewaartermijnen in verband met het toegelaten 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 mobiele 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 4°, 8° en 10°, worden bewaard zolang de gebruiker het bedrijfs-en organisatiemiddel of de machtiging gebruikt en zodra dat niet meer het geval is maximaal 18 maanden jaar.

2. De gegevens, bedoeld in artikel 5c, onderdeel a, onder 5°, 6° en 9°, worden maximaal 5 jaar bewaard, met dien verstande dat de sessiegegevens slechts worden bewaard tot het moment van uitloggen door de gebruiker.

3. De gegevens, bedoeld in artikel 5c, onderdeel a, onder 7°, worden 5 jaar bewaard.

4. De eidas-gegevens, bedoeld in artikel 5c, onderdeel c, onder 8°, worden maximaal 1 week bewaard, met uitzondering van uniek identificerende nummers, burgerservicenummers en de versleutelde vormen daarvan, welke maximaal 5 jaar worden bewaard.

5. De gegevens, bedoeld in artikel 5c, onderdeel b, worden maximaal 5 jaar bewaard.

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

De bewaartermijn van de gegevens, bedoeld in artikel 5d, is maximaal 1 week, met uitzondering van uniek identificerende nummers, burgerservicenummers en de versleutelde vormen daarvan, welke maximaal 5 jaar worden bewaard.

Artikel 14e Bewaartermijnen in verband met misbruik generieke digitale infrastructuur

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

O
Onder vernummering van de artikelen 16 en 17 tot 25 en 26 komt hoofdstuk 5 te luiden:

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, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening.

Artikel 17. Organisatie en beheer

1 Bestuursorganen en aangewezen organisaties beleggen taken, verantwoordelijkheden en coördinatie terzake 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 terzake 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.
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 voldoen aan de artikelen 16 tot en met 19, indien zij ISO/NEN 27001 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, voldoen aan de artikelen 16 tot en met 19, 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 en preproductie

1 Bestuursorganen en aangewezen organisaties voldoen aan de door Onze Minister gestelde testcriteria voor aansluiting op de voor hen relevante voorzieningen als bedoeld in artikel 5 van de wet, 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 2 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 terzake 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. Assessment en audit

1 Bestuursorganen en aangewezen organisaties laten hun informatieveiligheidsbeleid terzake van de toegang tot elektronische dienstverlening beoordelen door de uitvoering van een technische controle van hun informatiesystemen en betrekken de resultaten bij een jaarlijkse audit. Rapportage geschiedt jaarlijks via de eigen planning en control-cyclus alsmede, voor 1 mei over het voorgaande kalenderjaar, aan Onze Minister.

2 De beoordeling, bedoeld in het eerste lid, betreft de opzet van het beveiligingsproces en het bestaan van beheersmaatregelen 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 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.
P
Artikel 26 (nieuw) komt te luiden:
Artikel 26. Citeertitel
Dit Besluit wordt aangehaald als: Besluit digitale overheid.

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

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Nota van Toelichting

Inhoudsopgave

Nota van Toelichting

I Algemeen deel

1 Inleiding; aanleiding voor het voorstel

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft de Tweede Kamer herhaaldelijk 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. Meer in het bijzonder dient de algemene maatregel van bestuur ter uitvoering van de artikelen 4 en 14 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 van het voorstel

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 (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 14). Dit wordt nader uitgewerkt bij algemene maatregel van bestuur; vastgelegd wordt welke persoonsgegevens verwerkt worden, aan wie de gegevens worden verstrekt en hoe lang de gegevens worden bewaard. 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 (beveligingsassessments) zoals thans opgenomen in de aansluitvoorwaarden van DigiD. Beoogd wordt rechtmatigheid, rechtszekerheid en 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 normadressaten (doelgroepen) van de regels in deze algemene maatregel van bestuur zijn:

- Onze Minister: hij moet aan eisen voldoen inzake de verwerking 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 verwerking van persoonsgegevens bij het verlenen van toegang aan burgers en bedrijven tot elektronische dienstverlening en inzake de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening die zij in stand houden;
- Toegelaten en erkende private authenticatiediensten, erkende private ontsluitingsdienstenen erkende private machtigingsdiensten: zij moeten aan eisen voldoen inzake de verwerking van persoonsgegevens.
- Burgers/natuurlijke personen: zij zijn indirect betrokken, aangezien de verwerking van persoonsgegevens gegevens betreft van de houder van een toegelaten (publiek of privaat uitgegeven) identificatiemiddel.

3 Verhouding tot andere regelgeving

Wet Digitale overheid
Dit Besluit behelst de uitvoeringsregels waartoe de artikelen 4 en 14 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, is er voor gekozen niet alle (gedelegeerde) onderwerpen in een algemene maatregel van bestuur en een ministeriele 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 (grondslag: artikel 11 van de wet), er zal een ministeriële regeling inzake bekostiging worden opgesteld (grondslag: artikel 19 van de wet) 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 processen die te maken hebben met de aanvraag, productie, uitreiking en intrekking van 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 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 open gehouden 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 14 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. Doel van de betreffende bepalingen 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. 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.

De bepalingen in het besluit bieden o.a. grondslagen aan de minister van BZK 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 organisatie middel. 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.

4.1.1. Persoonsgegevens DigiD, DigiD Machtigingen

Binnen de werking van de bestaande voorzieningen voor toegang tot elektronische overheidsdienstverlening is een aantal belangrijke wijzigingen voorzien 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. 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 kunnen worden toegelaten zonder dat daarbij verwerking van het burgerservicenummer benodigd is. Deze maatregel vloeit mede voort uit de in 2017 uitgevoerde PIA.

De werking met pseudonimisering betekent dat voor de voorzieningen DigiD en DigiD Machtigen in het besluit wordt toegevoegd dat ook een versleutelde vorm van het BSN kan worden verwerkt ten behoeve van de identificatie van de gebruiker.

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 waarvoor het gebruik van een mobiele telefoon 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 terzake gereguleerd.

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

4.1.2. Persoonsgegevens toegelaten privaat middel

Omwille van de continuïteit van de toegang tot overheidsdienstverlening zal ingevolge de wet digitale overheid aan Onze minister de mogelijkheid worden geboden om naast het publieke identificatiemiddel DigiD een privaat identificatiemiddel toe te laten. Voorzien is om dit door middel van een aanbesteding te realiseren. Dit kan een bestaand of te ontwikkelen identificatiemiddel zijn dat na aanbesteding mede een rol vervult ten behoeve van de toegang tot elektronische overheidsdienstverlening.

Voor zover het de private werking van een dergelijk identificatiemiddel betreft 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 terzake van het toegelaten private middel is dat sprake is van een gelijkwaardige werking en een gelijkwaardig beschermingsniveau. 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.

4.1.3 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 gdi bevat immers geen bepalingen over gegevensverwerking door private partjjen 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.

4.1.4 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 dienstaanbieder in het publieke domein een pseudoniem toe te kennen (activatiefunctie), dat wordt gebruikt bij de identificatie bij dienstaanbieders (authenticatiefunctie of transformatiefunctie).

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 en er geen onwenselijke concentratie van persoonsgegevens ontstaat. Er wordt eenmalig een pseudoniem aangemaakt, waarna geen burgerservicenummer meer wordt opgeslagen. Vanuit privacy-oogpunt is de zowel vanuit oogpunt van pseudonimisering als dataminimalisatie een belangrijke verbetering. De

verwerking van persoonsgegevens voor deze voorziening die daarvoor nodig is verandert daardoor uiteraard mee. Gelet daarop wordt ook het besluit ten aanzien van het BSN-K gewijzigd.

4.1.5 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 de minister verantwoordelijk is. De routeringsvoorziening heeft tot doel (semi-) publieke dienstverleners te ontzorgen in hun aansluiting op wettelijk verplichte authenticatielandschappen (DigiD, 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.

4.1.6 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 maar die, bijvoorbeeld vanwege werk of onderwijs, een relatie hebben met een of meerdere publieke dienstverlener(s) in Nederland. Kortgezegd dient de eidas-voorziening er toe iemand op basis van buitenlandse persoonsgegevens te herkennen. Het systeem voorziet daarom in – onder de verantwoordelijkheid van de minister uitgevoerde - koppeling van uit een andere lidstaat binnenkomende gegevens aan een burgerservicenummer en een versleutelde vorm daarvan ('pseudoID'). Alleen indien en voor zover met dit proces geen zekerheid omtrent uniciteit kan worden verkregen, worden aanvullende gegevens verwerkt (dataminimalisatie).

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, waarbij er inhoudelijk geen 'licht' zit tussen dit kader en de regels die thans in de praktijk gehanteerd worden. Deze 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), de aansluitvoorwaarden DigiD en de ICT-beveiligingsrichtlijnen van het NCSC. Deze documenten zijn richtinggevend en daarmee vrijblijvend

van aard; ze hebben de status van beleidsregels of richtsnoeren, 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, 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 is uitgebreid ingegaan op de privacy-aspecten, en wel met name in het licht van de AVG. De AVG werkt rechtstreeks en aldus bevat dit besluit enkel bepalingen die aanvullend zijn op of en uitwerking 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 14 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) in samenhang met artikel 6, derde lid, onder b (bedoelde rechtsgrond moet worden vastgelegd bij lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is).

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 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 burgerservicnummer 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 versleuteling. 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 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 BSN 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-Koppelregister (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 BSN 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.

Transparantie
In de memorie van toelichting bij het wetsvoorstel digitale overheid is reeds 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 al 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 worden vastgelegd in op te stellen privacyverklaringen die op de betrokken websites zullen worden geplaatst.

Privacy impact assessments
Gedurende het proces om te komen tot elektronische identificatie terzake 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 14 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 artikel 19 van 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.

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 (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. Het nemen van veiligheidsmaatregelen en vooral het monitoren en verantwoorden is voor hen nieuw; naleving hiervan betekent voor hen administratieve lasten en kosten.

6.3 Resultaten uitvoeringstoetsen (tijdens consultatie)

- In welke mate is te verwachten dat de toepassing van het Besluit voor (welke?) normadressaten aanleiding geeft tot conflicten;

- Kwantificering: wat zijn de ingeschatte kosten op jaarbasis;
- Kan men uit de voeten met de invoeringstermijn 1 januari 2019.

PM

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). Voor wat betreft het 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 15, zesde lid, en de artikelen 16 en 17 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 terzake van de bepalingen inzake monitoring en 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

Ingevolge artikel 21 van het wetsvoorstel digitale overheid zendt de minister binnen vijf jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag 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 Consultatie en advies

Gedurende de (internet)consultatie, die plaats had van …. maart - ….april 2018, is een ieder in de gelegenheid geweest input te leveren op het besluit. Op hoofdlijnen houden de ontvangen reacties het volgende in…..
Hieraan is gevolg gegeven in die zin, dat...

Advies Adviescollege Toetsing Regeldruk (ATR)

Advies Autoriteit persoonsgegevens

PM

10 Inwerkingtreding

Beoogd moment van inwerkingtreding is 1 januari 2019; parallel aan inwerkingtreding van de wet digitale overheid en ervan uitgaand dat de voorzieningen, waarin ingevolge dit besluit gegevens worden verwerkt, dan daadwerkelijk functioneren. Ook de informatieveiligheidsbepalingen behoeven vanaf dat moment toepassing door de dienstverleners. 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.

Wat betreft de beschrijving van de afnemer van een routeringsvoorziening wordt erop gewezen dat het daarbij gaat om de verlening van toegang met zowel toegelaten identificatiemiddelen voor burgers als, op de langere termijn, voor bedrijven en ondernemingen, vandaar dat 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.

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 persoon 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 die zaak runt, reden waarom bij de verwerking van persoonsgegevens over eenmanszaken sprake is van persoonsgegevens.

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, Nederlandse paspoort of Nederlandse identiteitskaart zoals geldigheidsdata en het documentnummer van het rijbewijs paspoort of identiteitskaart. 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 de versleutelde BSN, volgnummer en document type. Deze verwerking is noodzakelijk omdat het rijbewijs geïntroduceerd zal worden bij 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.

Ten derde wordt artikel 2, onderdeel c, onder 6°, uitgebreid met de categorie gegevens noodzakelijk voor de administratie van DigiD. 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. 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: versleutelde BSN, documentnummer en documentcode. De gegevens op de chip van het paspoort, de identiteitskaart en het rijbewijs worden na verificatie van de identiteit van de gebruiker direct verwijderd. 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 vorm daarvan gaat verwerken. Om die reden is die versleutelde 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. Tot slot 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.

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 terzake niet langer bewerkersovereenkomsten (de AVG spreekt van verwerkersovereenkomsten) tussen de minister en de afnemers behoeven te worden gesloten. Tot slot 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 van de afnemers 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.

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-Koppelregister 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 daarvan afgeleid nummer verwerkt kan worden door de minister van BZK als verantwoordelijke voor het BSN-K. De verschillende functionaliteiten van het BSN-K maken gebruik van versleutelde burgerservicenummers van gebruikers om de koppeling te maken tussen het elektronische identificatiemiddel waarmee authenticatie plaatsvindt en de gebruiker van het middel. Onder bepaalde omstandigheden, namelijk bij misbruik, kan het van het BSN afgeleide versleutelde gegeven door de minister van BZK echter wel degelijk 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 d 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. Tot slot 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.

Onderdeel F

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 het burgerservicenummer of een afgeleide versleutelde vorm daarvan, de naam van de gebruiker en de noodzakelijke gegevens om deze correct weer te geven, de geboortedatum en de datum van overlijden. Het gaat daarbij om gebruikers van een toegelaten publiek of privaat identificatiemiddel of erkend bedrijfs- of organisatiemiddel. Op dit moment wordt primair gebruik van de routeringvoorziening ten behoeve van toegelaten publieke en private identificatiemiddelen door burgers beoogd, maar met het oog op toekomstige ontwikkelingen wordt tevens gebruik ten behoeve van erkende identificatiemiddelen door bedrijven mogelijk gemaakt.

Van degene die wordt vertegenwoordigd door een gemachtigde met DigiD Machtigen wordt ook het burgerservicenummer of een afgeleide versleutelde 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.
Daarnaast wordt door middel van het invoeren van een nieuw artikel 5b de persoonsgegevensverwerking geregeld die plaatsvindt door de aanbieder van een toegelaten privaat identificatiemiddel als bedoeld in artikel 9 van de Wet digitale overheid voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de voorziening voor de uitgifte en authenticatie van het toegelaten privaat identificatiemiddel. Aangezien voorzien wordt dat de werking van deze voorziening 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 formuleert gegevens die kunnen worden verwerkt door de erkende private partijen die betrokken zijn bij het aanbieden van elektronische identificatiemiddelen voor bedrijven. 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. Zo is in onderdeel a, onder 2°, als categorie gegevens opgenomen een 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. Onder de in onderdeel a, onder 4°, genoemde gegevens vallen 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. 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.
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. 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 – onder de verantwoordelijkheid van de minister uitgevoerde - koppeling van uit een andere lidstaat binnenkomende gegevens, onder meer naam, geboortedatum en uniek identificerend nummer in geval van authenticatie buiten Nederland ('uniquenessID') aan een burgerservicenummer en een versleutelde vorm daarvan ('pseudoID'). 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.
Onderdeel F regelt tot slot dat een nieuw artikel 5e 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. 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,

beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de voorzieningen binnen de generieke digitale infrastructuur en de gegevens en inlichtingen, bedoeld in artikel 17 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.
Voor de volledigheid wordt hier nog 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 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).
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. 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 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 verwerkt).
Onderdeel H
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 vorm van het BSN van gebruikers van bedrijfs-en organisatiemiddelen vanuit het BSN-K aan bestuursorganen en aangewezen organisaties en erkende ontsluitende diensten. 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 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.
Onderdeel I
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.
De verstrekkingen in verband met het toegelaten private identificatiemiddel (artikel 9b) zijn beperkt. De aanbieder van het middel verstrekt – vergelijkbaar met hetgeen terzake van het publieke middel geldt - aan bestuursorganen en aangewezen organisaties (publieke dienstverleners) die elektronische diensten verlenen slechts het (versleutelde) burgerservicenummer 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.
Ook de verstrekkingen in verband met een bedrijfs- en organisatiemiddel (artikel 9c) zijn beperkt. Erkende (private) partijen verstrekken aan de minister, verantwoordelijk voor de eidas-voorziening, de (versleutelde) eidas-gegevens (zie artikel 5d), opdat identificatie van bedrijven ten behoeve van grensoverschrijdende elektronische dienstverlening binnen de EU kan plaatsvinden. Erkende ontsluitende diensten (ook wel 'makelaars' genoemd) verstrekken aan publieke dienstverleners in verband met hun elektronische dienstverlening aan bedrijven een 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.
Voor wat betreft verstrekkingen in de eidas-voorziening (artikel 9d), verstrekt de minister aan het BSN-K (dus: aan zichzelf, als verantwoordelijke voor die 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 routeringsdienst (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 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. Deze inperking is nu uitgebreid tot de gebruikers van de overige voorzieningen en middelen, zoals de routeringsvoorziening en de authenticatiemiddelen. In twee gevallen is en blijft die toestemming niet nodig. 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 door een. 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 J
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.
Onderdeel K
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 kvk nummer 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.
Onderdeel L
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.
Onderdeel M
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 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.Ten slotte 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.
Onderdeel N 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 terzake van het (versleutelde) burgerservicenummer 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 vijfjaarstermijn 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.
De bewaartermijnen zoals die gelden ten aanzien van DigiD alsmede de – door de betreffende verwerkingsdoelen ingegeven - onderbouwing daarvoor zijn leidend voor de bewaartermijnen terzake 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 terzake een gelijkwaardig veiligheids- en betrouwbaarheidsniveau geldt en aan dezelfde eisen moet worden voldaan (gelijk speelveld).

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. Dat vertaalt zich voor de verschillende gegevens die in het kader van het bedrijfs- en organisatiemiddel worden verwerkt in de aangegeven bewaartermijnen.
De bewaartermijn van de gegevens die worden verwerkt in de eidas-voorziening is ingevolge artikel 14d maximaal een week, met uitzondering van uniek identificerende nummers, burgerservicenummers en de versleutelde vormen daarvan, welke voor maximaal vijf jaar worden bewaard. Reden hiervoor is dat de minister omwille van veiligheid en betrouwbaarheid, enige tijd de mogelijkheid moet houden een koppeling ongedaan te maken.
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 O
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 van 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 per dienstverlener kan verschillen; het betreft immers maatwerk. De ruimte die individuele dienstverleners hebben, wordt – om redenen van goede werking, veiligheid en betrouwbaarheid van de toegang tot elektronische dienstverlening in Nederland - door dit Besluit in zekere mate geüniformeerd en ingeperkt. Het door dienstverleners op te stellen informatieveiligheidsbeleid en de in dat verband te nemen maatregelen dienen in ieder geval de aspecten te behelzen, zoals aangegeven in de (hierna volgende) 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 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:
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 continue proces; in dit verband is sprake van een 'Plan-Do-Check-Act' cyclus.

Lid 4:
Dit lid geeft de minister de bevoegdheid om nadere regels te stellen met betrekking tot de werking, betrouwbaarheid 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.

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 terzake 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 14, 16-17 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 in den brede 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 (het rechtstreeks werkende) 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.

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. 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 terzake 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 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. 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 diensteverlening. Het onderhavige artikel verplicht dienstverleners in dit verband te voldoen aan de door de minister gestelde testcriteria voor aansluiting op de voor hen 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, welke 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, 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. 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 16 -17 van de wet. Zie in dit verband ook artikel 5e 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 terzake van de toegang tot elektronische dienstverlening laten beoordelen. Dit geschiedt door de uitvoering van een technische controle van hun informatiesystemen; de resultaten moeten bij een jaarlijks uit te voeren audit worden betrokken. De op basis hiervan opgestelde rapportage dient onderdeel uit te maken van de reguliere verantwoording (planning en control-cyclus) en dient daarnaast jaarlijks via de voorgeschreven gestandaardiseerde methode, 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. Elementen van het assessment zijn onder meer netwerkveiligheid (systeem- en infrastructuurkoppelingen) besturingssysteem, basisbeveiliging, applicatiebeveiliging en penetratietest. Het gaat hierbij primair 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. Op basis van opgedane ervaringen (binnen vijf jaar na de inwerkingtreding van de wet dient er 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 terzake, afhankelijk van aard, ernst en omvang van niet-naleving en mits proportioneel, (interbestuurlijke) maatregelen nemen. Hij is immers verantwoordelijk voor toezicht terzake (artikel 15, zesde 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 16 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 terzake 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 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" in de zin van bijvoorbeeld de NOREA-beroepsregels, of een certificaat inzake het managementsysteem voor informatiebeveiliging (ISO/NEN 27001/27002). 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 kan hiertoe een *assurance*verklaring bevatten: aanvullende zekerheid (een zogeheten *Third Party*-mededeling) van een derde inzake de desbetreffende beheerprocessen. 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 terzake 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 terzake 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.
De minister kan beleidsregels stellen met betrekking tot de wijze van beoordeling en rapportage. Het kan daarbij 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 etc.
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 (eigen P&C-cyclus) alsmede aan de Minister kan plaatsvinden.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,