

DPIA (Compact)

Inleiding

Dit document is voor het uitvoeren van een compacte DPIA (Data Protection Impact Assessments). Bepaal vooraf met behulp van de BBN-toets en Pre-DPIA of een PDIA noodzakelijk is en welk model je moet toepassen (compact of uitgebreid). Dit is het compacte DPIA-model. Het is een volwaardig DPIA en is opgebouwd uit de door de AVG (art. 35 lid 7) voorgeschreven onderdelen:

- Een systematische beschrijving van de verwerkingen en de verwerkingsdoelen;
- Een beoordeling van de noodzaak en evenredigheid;
- Een risicobeoordeling;
- Beheersmaatregelen.

Voor het invullen van dit document is een toelichting beschikbaar. Daarin wordt elke vraag wordt uitgelegd.

Project/proces/verwerking:	Fraudebestrijding balie Burgerzaken
Ingevuld door:	
Betrokken Informatiebeveiligingsadviseur(s):	
Betrokken Privacy Officer(s):	
Status:	Definitief
Datum:	23 maart 2026
Documentnummer (Corsa registratienummer):	2500010994

Advies FG en vaststelling

□ **Advies FG:** geadviseerd door op 28-5-2026.

Toelichting:

Zorgvuldig uitgevoerde DPIA op dit proces. Goede beschrijving van het proces en de bijbehorende verwerkingen met duidelijke scope. De verwerkingsdoelen en de grondslagen zijn goed uitgewerkt en de proportionaliteit en subsidiariteit hebben daarbij voldoende aandacht gekregen. Risico's zijn beschreven maar de werking daarvan moet in de praktijk nog worden getoetst. Bovendien is het een nieuwe werkwijze binnen de gemeente. Ik zou daarom de DPIA na 1 jaar nogmaals voorgelegd willen krijgen met daarbij een beoordeling van de werking in de praktijk van de mitigerende maatregelen.

DPIA (Compact)

□ **Vaststelling:** vastgesteld door **Klik of tik om tekst in te voeren.** op **Klik of tik om een datum in te voeren..**

Toelichting:

Klik of tik om tekst in te voeren.

PDCA

DPIA moet herzien worden voor:

28-5-2027

Systematische beschrijving verwerkingen en de verwerkingsdoelen

Dit eerste onderdeel dient, net als bij de Pre-DPIA, om voldoende inzicht te krijgen in de verwerking. Maak zoveel mogelijk gebruik van de informatie uit de Pre-DPIA.

Algemeen

De vragen uit dit onderdeel zijn gelijk aan de vragen uit de Pre-DPIA. Neem de antwoorden uit de Pre-DPIA over, controleer en vul waar nodig aan.

PD.A.1. Algemene vragen

Organisatie (Enschede / Losser):	Enschede en Losser
Organisatieonderdeel:	Afdeling Burgerzaken.
Proces:	Fraudebestrijding
Proceseigenaar (naam en functie):	teamleider Burgerzaken
Eindverantwoordelijke (naam en functie):	clustermanager Dienstverlening

PD.A.2. Procesbeschrijving

Beschrijf in het kort wat de nieuwe gegevensverwerking (proces/wijziging/project/initiatief) inhoudt. Waarom wil de organisatie deze verwerking gaan uitvoeren?

DPIA (Compact)

Het vaststellen van de identiteit aan de hand van het reisdocument gebeurt nu door de medewerker aan de balie. Daarvoor worden de fysieke gegevens op het reisdocument vergeleken met de persoon aan de balie.

Met de aanschaf van apparatuur voor fraudebestrijding wordt het nieuwe proces:

1. Aanvrager komt aan de balie en geeft het document (paspoort, identiteitskaart, rijbewijs en dergelijke) aan de baliemedewerker.
2. De baliemedewerker legt het document in de documentscanner en start de controle.
3. De apparatuur scant beide zijdes van het document.
4. De apparatuur controleert het document op echtheid. Het scherm toont een scan van het document.
5. De baliemedewerker start de gezichtsvergelijking. Dit geldt alleen voor vrouwen ouder dan 16 en mannen ouder dan 18. Onder deze leeftijden veranderen gezichten nog te veel om een gezichtsvergelijking uit te kunnen voeren. Vrouwen zijn eerder uitgegroeid dan mannen, vandaar het verschil in minimum leeftijd.
6. De camera op de balie maakt een foto van de aanvrager. De foto op het document en de foto van de camera worden in het scherm getoond.
7. De apparatuur vergelijkt de foto's op en in het document en de foto van de camera op gelijkenis. Daarvoor gebruikt de apparatuur biometrische gegevens die van de foto's worden afgeleid. De biometrische gegevens staan alleen op de computer en zijn niet voor de baliemedewerker inzichtelijk.
8. De apparatuur genereert een rapport dat wordt opgeslagen in iBurgerzaken, zie bijlage A. Hier staan geen biometrische gegevens in maar alleen foto's en persoonsgegevens die ook in iBurgerzaken staan.
9. De biometrische gegevens worden van de apparatuur verwijderd.
10. De apparatuur toont op het scherm het advies van de documentcontrole en de gezichtsvergelijking.
11. Als beide adviezen positief zijn controleert de baliemedewerker of deze het eens is met het advies. Zo ja dan kan verder worden gegaan met de aanvraag. Zo nee dan wordt een collega gevraagd mee te kijken.
Als één van beide adviezen negatief is bespreekt de baliemedewerker dit met de aanvrager. Er kan een oorzaak zijn dat de foto's niet overeenkomen, zoals een operatie. De baliemedewerker vraagt een collega mee te kijken.
Besluiten de baliemedewerkers dat het document echt is en van de aanvrager is dan kan verder worden gegaan met de aanvraag. Bij aanhoudende twijfel of constatering van fraude wordt de politie ingeschakeld.

In bijlage B is te zien wat de baliemedewerker te zien krijgt bij dit proces.

Bij de fraudebestrijding met gezichtsvergelijking en echtheidscontrole van het document wordt geen gebruik gemaakt van de vingerafdrukken op de chip van het document.

DPIA (Compact)

PD.A.3. Geef aan van welke categorie(ën) van betrokkenen persoonsgegevens worden verwerkt. Geef daarbij aan wat de relatie is tot de betrokkenen.

- ☐ Aanvragers
- ☐ Belanghebbenden
- ☐ Belastingplichtigen
- ☐ Betrokkenen
- ☐ Cliënten
- ☐ Contactpersonen
- ☐ Eigenaren
- ☐ Inwoners
- ☐ Jeugdigen
- ☐ Klagers/Bezwaarmakers

- ☐ Leerplichtigen
- ☐ Melders
- ☐ Ouders
- ☐ Overig
- ☐ Personeelsleden
- ☐ Politieke ambtsdragers
- ☐ Vergunninghouders
- ☐ Anders, namelijk:
Klik of tik om tekst in te voeren.

Toelichting: De echtsheidscontrole van het document kan voor aanvragers van alle leeftijden. De gezichtsvergelijking is alleen voor vrouwen ouder dan 16 jaar en mannen ouder dan 18 jaar.

Aanvragers zijn iedereen die bij aan de balie van burgerzaken komt. Dit kunnen zijn inwoners van Enschede, personen die zich willen vestigen in Enschede en Nederlanders in het buitenland.

PD.A.4. Geef aan welke categorieën van persoonsgegevens worden verwerkt.

- ☐ Burgerservicenummer
- ☐ Basispersoonsgegevens
- ☐ Gegevens m.b.t. kind(eren)
- ☐ Ras of etnische afkomst
- ☐ Religieuze of levensbeschouwelijke overtuiging
- ☐ Gezondheid

- ☐ Strafrechtelijke veroordelingen en strafbare feiten
- ☐ Seksuele identiteit en oriëntatie
- ☐ Inkomensgegevens
- ☐ Politieke opvattingen
- ☐ Genetische of biometrische gegevens
- ☐ Lidmaatschap van een vakbond

PD.A.5. Wat is de herkomst van de persoonsgegevens?

Identiteitsdocument, aangeleverde foto en camera.

DPIA (Compact)

PD.A.6. Aan welke categorieën ontvangers worden de persoonsgegevens verstrekt? Zijn deze als verwerker te kwalificeren?

	Verwerker?
☐ Externe dienstverlener Oribi, wordt niet verstrekt is alleen de leverancier van de apparatuur	Nee
☐ ...	Kies een item.

PD.A.7. In welke landen vindt de verwerking plaats? Worden persoonsgegevens aan derde landen (= landen buiten de EER) of aan internationale organisaties doorgegeven? Zo ja, zijn er passende waarborgen, en zo ja, welke zijn dat?

De verwerking vindt plaats in:	Op de NUC (mini computer) die door Oribi wordt meegeleverd. Elke balie heeft een eigen NUC. Zie bijlage C voor een weergave van de opstelling.	
Is dit een derde land (buiten de EER)?	☐ Nee	☐ Ja
Zo ja, zijn er passende waarborgen?	☐ Nee	☐ Ja (vul toelichting in)
Toelichting:		

Klik of tik om tekst in te voeren.

PD.A.8. Bepaal welke bewaartermijnen voor deze persoonsgegevens van toepassing zijn.

De biometrische-, persoons- en documentgegevens die gebruikt worden voor de controles worden slechts enkele seconden bewaart op de NUC. Na de controle en vergelijking worden deze direct verwijderd.

De rapportage, zie bijlage A, met daarin persoonsgegevens, documentgegevens en scans van document met foto van de aanvrager worden in iBurgerzaken opgeslagen in de zaak van de aanvraag. De bewaartermijn in iBurgerzaken is afhankelijk van het type zaak. De langste bewaartermijn is 110 jaar. In bijlage D staat een overzicht van de bewaartermijnen per zaaktype per status. In iBurgerzaken worden geen biometrische gegevens opgeslagen.

PD.A.9. Beschrijf de doel(en) van verwerking (meerdere antwoorden mogelijk).

DPIA (Compact)

1. Vaststellen of het document (paspoort, identiteitskaart, rijbewijs en dergelijke) echt is.
2. Vaststellen of de gegevens op de chip van het document, de fysieke gegevens op het document en de persoon aanwezig met elkaar overeenkomen.

Indien één van beide of beide controles negatief zijn dan wordt door de baliemedewerker en een collega de controle visueel gedaan. Bij blijvende twijfel of fraude wordt de politie ingeschakeld.

PD.A.10. Beschrijf de rechtsgrond(en) van verwerking (meerdere antwoorden mogelijk).

- ☐ Toestemming van betrokkene
- ☐ Uitvoering van een overeenkomst
- ☐ Voldoen aan wettelijke verplichting
- ☐ Bescherming van een vitaal belang van betrokkene of andere natuurlijke persoon
- ☐ Vervulling van een taak in algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag
- ☐ Behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde.

Toelichting

Volgens de Wet BRP artikel 2.4 lid 3, en wet op de identificatieplicht artikel 1 zijn wij als gemeente verplicht om de identiteit van een aanvrager deugdelijke vast te stellen. Dit gebeurt momenteel handmatig, door middel van een visuele beoordeling. Echter de technieken om een document te vervalsen worden steeds complexer en daardoor moeilijker visueel te detecteren. Ook alle echtheidskenmerken op documenten zijn steeds moeilijker alleen visueel te verifiëren, zie bijlage G voor een voorbeeld van de echtheidskenmerken op een Nederlands paspoort. Wij vinden het daarom noodzakelijk dat apparatuur voor fraudebestrijding de baliemedewerker kan ondersteunen bij het vaststellen van de identiteit van de aanvrager en de controle op echtheid van het document.

Bij de aanvraag van identiteitsdocumenten is identiteitsfraude één van de grootste risico's. Dit zien we concreet in de zaak Taghi maar ook in andere grote ondermijningszaken. Criminele activiteiten worden daarbij mogelijk gemaakt door het aannemen van valse identiteiten.

Het aantal bekende gevallen van fraude met identiteitsdocumenten is niet heel groot maar de gevolgen zijn wel heel groot. De inzet van fraudebestrijdingsapparatuur is volgens ons dus te verantwoorden. Ook werkt de inzet van fraudebestrijdingsapparatuur preventief.

PD.B.2. Is/zijn er een of meerdere categorieën van de lijst van de Autoriteit Persoonsgegevens van toepassing? Zo ja, welke en licht dit toe.

Antwoord:

Argumentatie:

DPIA (Compact)

1. Heimelijk onderzoek	Nee	Klik of tik om tekst in te voeren.
2. Zwarte lijsten	Nee	Klik of tik om tekst in te voeren.
3. Fraudebestrijding	Ja	Klik of tik om tekst in te voeren.
4. Creditscores	Nee	Klik of tik om tekst in te voeren.
5. Financiële situatie	Nee	Klik of tik om tekst in te voeren.
6. Genetische persoonsgegevens	Nee	Klik of tik om tekst in te voeren.
7. Gezondheidsgegevens	Nee	Klik of tik om tekst in te voeren.
8. Samenwerkingsverbanden	Nee	Klik of tik om tekst in te voeren.
9. Cameratoezicht	Nee	Klik of tik om tekst in te voeren.
10. Flexibel cameratoezicht	Nee	Klik of tik om tekst in te voeren.
11. Controle werknemers	Nee	Klik of tik om tekst in te voeren.
12. Locatiegegevens	Nee	Klik of tik om tekst in te voeren.
13. Communicatiegegevens	Nee	Klik of tik om tekst in te voeren.
14. Internet of things	Nee	Klik of tik om tekst in te voeren.
15. Profilerings	Nee	Klik of tik om tekst in te voeren.
16. Observatie en beïnvloeding van gedrag	Nee	Klik of tik om tekst in te voeren.
17. Biometrische gegevens	Ja	Bij gezichtsvergelijking worden kenmerken van het gezicht gebruikt, zoals de afstanden tussen ogen, neus, mond en kaaklijn, evenals textuurkenmerken van de huid.
Eén of meerdere vragen met JA beantwoord?	Ja	Klik of tik om tekst in te voeren.

PD.B.3. Zijn er twee of meer criteria van de lijst van de WP29 van toepassing? Zo ja, welke (vink aan) en licht dit toe.

	Antwoord:	Argumentatie:
--	-----------	---------------

DPIA (Compact)

1. Beoordelen van mensen op basis van persoonskenmerken/ profilering	Ja	Het vaststellen van de identiteit van de aanvrager en de controle van de echtheid van het document is niet alleen meer mogelijk met visuele controles. De technieken om fraude te plegen en fraude tegen te gaan in het document worden steeds complexer. Dit is met alleen een visuele controle onvoldoende te controleren. De gevolgen van identiteitsfraude kunnen heel groot zijn en nemen de laatste jaren steeds verder toe. Het is daarom noodzakelijk om fraudebestrijdingsapparatuur in te zetten bij de bestrijding van identiteitsfraude.
2. Geautomatiseerde beslissingen, want Stelselmatige en grootschalige monitoring	Nee	Klik of tik om tekst in te voeren.
3. Gevoelige gegevens	Nee	Klik of tik om tekst in te voeren.
4. Grootschalige gegevensverwerkingen	Nee	Klik of tik om tekst in te voeren.
5. Gekoppelde databases	Nee	Klik of tik om tekst in te voeren.
6. Gegevens over kwetsbare personen	Nee	Klik of tik om tekst in te voeren.
7. Gebruik van nieuwe technologieën	Ja	Het vaststellen van de identiteit van de aanvrager en de controle van de echtheid van het document is niet alleen meer mogelijk met visuele controles. De technieken om fraude te plegen en fraude tegen te gaan in het document worden steeds complexer. Dit is met alleen een visuele controle onvoldoende te controleren. De gevolgen van identiteitsfraude kunnen heel groot zijn en nemen de laatste jaren steeds verder toe. Het is daarom noodzakelijk om fraudebestrijdingsapparatuur in te zetten bij de bestrijding van identiteitsfraude. Gezichtsvergelijking met OriBi apparatuur is één van de meest effectieve manieren om frauduleuze aanvragen te detecteren voordat een document wordt uitgegeven
8. Blokkering van een recht, dienst of overeenkomst	Nee	Klik of tik om tekst in te voeren.

DPIA (Compact)

9. Eén of meerdere vragen met JA beantwoord?

Ja

Klik of tik om tekst in te voeren.

Aanvullende vragen

CD.AV.1. Beschrijf het juridische en beleidsmatige kader.

Welke wet- en regelgeving is naast de AVG en de UAVG van toepassing op de verwerking? Benoem de wet of norm met het bijbehorende artikel.

DPIA (Compact)

- Wet BRP artikel 2.4 lid 3: Inschrijving geschiedt niet dan nadat de identiteit van de betrokkene deugdelijk is vastgesteld.
- Wet BRP Artikel 2.19 lid 5: De gegevens worden niet opgenomen dan nadat de identiteit van de betrokkene deugdelijk is vastgesteld.
- Wet op de identificatieplicht artikel 1: Als documenten waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld, worden aangewezen: reisdocument en rijbewijs.
- Paspoortwet Artikel 26 en 28: De aanvraag moet persoonlijk worden ingediend en De autoriteit (artikel 26) verschaft zich de nodige zekerheid over de identiteit en de nationaliteit van de aanvrager.
- Paspoortuitvoeringsregeling Nederland 2001: Voor het verkrijgen van de nodige zekerheid over de identiteit van de aanvrager, alsmede over zijn Nederlandschap dan wel zijn behandeling als Nederlander, indien het een persoon betreft op wie de [Wet betreffende de positie van Molukkers](#) van toepassing is, wordt gebruik gemaakt van het door de aanvrager overgelegde Nederlandse reisdocument, de door de aanvrager bij de aanvraag verstrekte gegevens, alsmede van de in de basisadministratie dan wel de in het basisregister reisdocumenten opgenomen gegevens of van overige bij de tot uitreiking bevoegde autoriteit aanwezige documenten.
- Reglement rijbewijzen Artikel 33, lid 1 onder b I : Dit specifieke lid bepaalt dat een rijbewijs ongeldig wordt indien het is afgegeven op basis van vervalste of onjuiste documenten [bronnen gecombineerd op basis van structuur Reglement rijbewijzen].

Het vaststellen van iemands identiteit is een essentiële eerste stap in de dienstverlening van een gemeente. De wet (BRP, bijvoorbeeld art. 1.8, 2.4, 2.55) eist daarvoor van het college een 'deugdelijke identiteitsvaststelling', maar geeft verder geen invulling van het begrip 'deugdelijk'. Iemands identiteit bestaat uit persoonsgegevens en fysieke kenmerken. De identiteit wordt vastgesteld door een echt, eigen, geldig en gekwalificeerd identiteitsdocument (met de persoonsgegevens en fysieke kenmerken) te vergelijken met de persoon in kwestie.

De gemeente is dus verplicht om de identiteit van een persoon die een aanvraag doet bij de balies deugdelijk vast te stellen. De fraudebestrijdingsapparatuur is een hulpmiddel om dit te ondersteunen. De gemeente versterkt documenten waarmee de identiteit van de persoon vastgesteld kan worden. Ook daarvoor is het noodzakelijk om de identiteit van de persoon deugdelijk vast te stellen voordat het document wordt versterkt. Ook hierbij ondersteunt de fraudebestrijdingsapparatuur.

CD.AV.2. Beschrijf de aard en de inhoud van de verwerking.

DPIA (Compact)

De software leest de chip van het document, scant de fysieke gegevens van het document en maakt een foto van de persoon aan de balie. Van de foto's worden biometrische gegevens afgeleid. De biometrische- en persoonsgegevens van de verschillende bronnen worden door de apparatuur met elkaar vergeleken. De bevindingen van de vergelijking worden weergegeven in een rapport, zie bijlage A. In dit rapport staan geen biometrische gegevens maar alleen foto's. Dit rapport wordt opgeslagen in iBurgerzaken.

De vergelijking van de biometrische- en persoonsgegevens van de verschillende bronnen wordt door de apparatuur gedaan op basis van AI. Alle kenmerken worden één voor één vergeleken voor de verschillende bronnen. Dit geeft per kenmerk een score. Alle scores per kenmerk worden samengevoegd tot een geïntegreerde eindscore. Als deze eindscore boven de 70% ligt volgt een positief advies aan de baliemedewerker.

De resultaten AI-verordening Beslishulp van de overheid geeft aan dat het gaat om een AI-systeem met hoog risico, maar zonder transparantieplichtingen, zie bijlage I.

Informatie over het algoritme is te vinden op de website: <https://pages.nist.gov/frvt/html/frvt11.html>. Hier staan de NIST rapportages volledig openbaar. De fraudebestrijdingsapparatuur maakt gebruik van de SDK van het Cognitec FaceVACS 1:1.

CD.AV.3. Beschrijf de scope van de verwerking.

De fraudebestrijdingsapparatuur zal worden ingezet bij iedereen die zich aan de balie van burgerzaken moet identificeren. Dat is voor de volgende processen:

- Het aanvragen en afhalen van een paspoort of identiteitskaart
- Het aanvragen en afhalen van een rijbewijs
- Het regelen van een huwelijk of geregistreerd partnerschap
- De aangifte van een pasgeboren kind
- Het doorgeven van een overlijden
- Uw inschrijving in de gemeente
- Het doorgeven van een verhuizing
- Het aanvragen van een naturalisatie
- Het aanvragen van een uittreksel

CD.AV.4. Beschrijf de context van de verwerking.

Verwachten betrokkenen deze verwerking en bestaan hierover zorgen?

DPIA (Compact)

Het gebruik van gezichtsvergelijking voor identificatie bij de gemeente is de laatste jaren veelvuldig in het nieuws geweest en wordt al bij heel vele gemeenten ingezet. Ook de marechaussee maakt gebruik van gezichtsvergelijking op de luchthavens. De verwachting is dus dat het voor inwoners niet een geheel nieuw fenomeen is.

In de afspraakbevestiging die de inwoners ontvangen na het maken van een afspraak bij burgerzaken zal worden aangegeven dat bij de balie gebruik gemaakt wordt van gezichtsvergelijking. In deze afspraakbevestiging wordt verwezen naar een website waarop uitgebreide informatie staat over het gebruik van de fraudebestrijdingsapparatuur, zie bijlage E.

In de wachtruimte van de balies zullen we flyers plaatsen waarin kort het gebruik van de camera's wordt aangegeven. Hierop zal ook een verwijzing naar de website staan.

De verwachting is niet dat het gebruik van fraudebestrijdingsapparatuur veel problemen gaat geven. Wel hebben we te maken met de verwarring tussen gezichtsvergelijking en gezichtsherkenning. Het kan dus zijn dat inwoners bezwaar maken of vragen hebben als ze aan de balie komen omdat ze veel negatieve berichten hebben gehoord over het gebruik van gezichtsherkenning. Om vervelende discussies tussen de baliemedewerker en de inwoner te voorkomen zullen we zorgen dat goede informatie voorhanden is.

CD.AV.5. Beschrijf het doel en het belang van de verwerking.

Wet BRP artikel 2.4 lid 3: Inschrijving geschiedt niet dan nadat de identiteit van de betrokkene deugdelijk is vastgesteld.

Wet op de identificatieplicht artikel 1: Als documenten waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld, worden aangewezen: reisdocument en rijbewijs.

De gemeente is dus verplicht om de identiteit van een persoon die zich wil inschrijven in de BRP deugdelijk vast te stellen. Omdat identiteitsfraude steeds complexer wordt en moeilijker vast te stellen achten wij het noodzakelijk om voor een deugdelijke vaststelling van de identiteit fraudebestrijdingsapparatuur in te zetten.

De gemeente verstrekt documenten (paspoorten, identiteitskaarten en rijbewijzen) waarmee de identiteit van de persoon vastgesteld kan worden. Ook verstrekken wij documenten met gegevens uit de BRP.

De documenten met gegevens uit de BRP worden door de inwoners gedeeld met andere instanties, die deze informatie gebruiken als onderdeel van hun besluitvorming, zoals bij het verstrekken van een huurwoning. Het is daarom noodzakelijk om de identiteit van de persoon deugdelijk vast te stellen voordat het document wordt verstrekt. Ook hierbij ondersteunt de fraudebestrijdingsapparatuur.

CD.AV.6. Transparantie.

Hoe voldoe je aan de wettelijke (privacy)informatieverplichtingen tegenover betrokkenen?

Inwoners worden in de afspraakbevestiging geïnformeerd over het gebruik van gezichtsvergelijking. Het komt op de website, zie bijlage E en er wordt een flyer geplaatst in de wachtruimte met een verwijzing naar de website.

DPIA (Compact)

CD.AV.7. Rechten betrokkenen.

Hoe geef je invulling aan de rechten van betrokkenen en aan privacyvragen/-verzoeken?

De gemeente Enschede heeft een vastgesteld procedure voor de afhandeling van rechten van betrokkene zoals het inzage recht.

Voor deze verwerking gelden de volgende aanvullende afspraken t.a.v. rechten van betrokkenen:
Omdat geen gegevens worden opgeslagen is het niet mogelijk om inzage te geven in de gebruikte gegevens.

Aanvragers zijn verplicht om mee te werken aan de echtsheidscontrole van de documenten en de gezichtsvergelijking. Als een aanvrager dit weigert dan kan geen gebruik gemaakt worden van de diensten van Burgerzaken.

CD.AV.8. Kennis & awareness.

Hoe houd je de privacykennis van medewerkers op het benodigde niveau?

Vanuit de bewustwordingscampagne "Veilig werken. Zo doe je dat!" worden alle medewerkers van de gemeente Enschede gewezen op het belang om veilig en zorgvuldig om te gaan met persoonsgegevens. Dit doen we met verschillende bewustwordingsactiviteiten waaronder met verplichte e-learning die medewerkers met een vaste regelmaat moeten doorlopen.

De baliemedewerkers werken de hele dag door met persoonsgegevens, gegevens van documenten en foto's. De verwerking in het kader van de fraudebestrijdingsapparatuur is daarin niet anders dan bij andere werkzaamheden, vooral omdat de baliemedewerker geen toegang heeft tot biometrische gegevens. Wij hoeven dus geen aanvullende activiteiten te ondernemen om de baliemedewerker er bewust van te maken dat zij veilig en zorgvuldig moeten omgaan met gegevens.

CD.AV.9. Verwerkersovereenkomsten.

Heb je met verwerkers verwerkersovereenkomsten afgesloten die voldoen aan de AVG-eisen? Dezelfde vraag voor (joint) controllerovereenkomsten bij (joint) controllers (= gezamenlijke verwerkingsverantwoordelijken).

De verwerkingsovereenkomst is opgenomen in Bijlage F.

CD.AV.10. Autorisaties.

Heb je de autorisaties ingericht op basis van 'need to know'? (role based access)?

Het rapport met het resultaat van de vergelijkingen komt in de zaak in iBurgerzaken. iBurgerzaken is altijd al zo ingericht dat alleen medewerkers van de afdelingen Burgerzaken, Ontvangst, Handhaving BRP en KCC toegang hebben tot de zaakgegevens. Inloggen in iBurgerzaken gebeurt met inlognaam en wachtwoord en is alleen mogelijk vanuit de werkomgeving waarin ingelogd wordt met 2FA.

Directe toegang tot de gezichtsvergelijking is ook mogelijk. Daarvoor dient direct ingelogd te worden op de apparatuur. Dit gebeurt via een link op een sharepoint-pagina. Alleen medewerkers van de afdeling Burgerzaken die aan de balies van Burgerzaken werken krijgen toegang tot deze sharepoint-pagina. Dit zijn er ongeveer 50.

DPIA (Compact)

CD.AV.11. Informatiebeveiliging.

Welke (soorten) beveiligingsmaatregelen heb je getroffen bij deze verwerking? Welke specifieke beveiligingsnormen gelden er voor dit proces? Wordt daaraan voldaan?

In bijlage H staat aangegeven aan welke bio-normen de leverancier en de apparatuur voor fraudebestrijdingsapparatuur voldoen.

Daarnaast hebben we de volgende beveiligingsmaatregelen genomen:

- Het gebruik van de apparatuur via iBurgerzaken wordt gelogd in iBurgerzaken. Daar kunnen we zien wie de betreffende aanvraag heeft afgehandeld. Alleen in iBurgerzaken worden gegevens van de fraudebestrijdingsapparatuur opgeslagen.
- De camera is niet toegankelijk als er geen medewerker bij de balie aanwezig is. Dit doen we door een pakje over de camera te plaatsen.
- Alleen geautoriseerde gebruikers hebben toegang tot de opgeslagen gegevens in iBurgerzaken, zie CD.AV.10. Autorisaties van deze DPIA.
- De resultaten AI-verordening Besliahulp van de overheid geeft aan dat het gaat om een AI-systeem met hoog risico, maar zonder transparantieplichtingen.

CD.AV.12. Datalekkenbeleid.

Beschik je over datalekkenbeleid, een effectieve procedure en een datalekkenregister?

De gemeente Enschede heeft een vastgesteld beleid en procedure voor de afhandeling van datalekken. De datalekken worden in een centraal register bijgehouden. Voor het proces geldt het vastgesteld beleid.

CD.AV.13. Kwaliteit.

Beschik je over procedures om de kwaliteit van de gegevens te waarborgen? Met andere woorden: hoe zorg je ervoor dat de gegevens actueel, juist en volledig zijn en blijven?

De gegevens die gebruikt worden voor de gezichtsvergelijking worden op het moment verzameld en verwerkt. Het rapport dat wordt opgeslagen in iBurgerzaken wordt later niet meer gebruikt.

CD.AV.14. Afstemming met betrokkenen.

Heb je bij het uitvoeren van de DPIA de betrokkenen om hun mening gevraagd over de verwerking, en zo ja, op welke wijze wordt deze meegenomen in de DPIA?

Er is geen contact geweest met betrokkenen.

Beoordeling van de rechtmatigheid, noodzaak en evenredigheid van de verwerking

Beoordeel aan de hand van de antwoorden op de inventarisatie, zoals vastgesteld in A tot en met E, de noodzaak en de evenredigheid van de (voorgenomen) gegevensverwerking. Is de verwerking rechtmatig?

DPIA (Compact)

Bereik je daarmee het beoogde doel? Is er geen andere, minder belastende manier om het resultaat te bereiken?

CD.B.1. Rechtmatigheid.

Beoordeel aanvullend op wat hierboven al is uitgewerkt de rechtmatigheid van de verwerking.

DPIA (Compact)

De Autoriteit Persoonsgegevens heeft een juridisch kader voor het gebruik van gezichtsherkenning gepubliceerd: <https://www.autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning>. Aangezien de AP niets zegt over het gebruik van gezichtsvergelijking gebruiken we het kader voor gezichtsherkenning.

Uit dit kader volgt:

Het verwerken van biometrische gegevens met het oog op de unieke identificatie van een persoon valt onder het verwerkingsverbod van artikel 9, eerste lid, van de AVG. Dit verwerkingsverbod wordt alleen doorbroken als een uitzonderingsgrond van toepassing is uit artikel 9, tweede lid, van de AVG. Naast een uitzonderingsgrond moet voor de verwerking ook altijd voldoen worden aan de beginselen van gegevensbescherming uit artikel 5 AVG en moet de verwerkingsverantwoordelijke een grondslag uit artikel 6 AVG hebben. Er zijn 2 mogelijke uitzonderingen voor gezichtsherkenning: uitdrukkelijke toestemming van de betrokkenen en een zwaarwegend algemeen belang.

Een van de uitzonderingen op het verwerkingsverbod is 'uitdrukkelijke toestemming'. Daar is geen sprake van bij het gebruik van fraudebestrijding aan de balies want de aanvrager is verplicht mee te werken. Anders kan de aanvrager geen diensten afnemen bij de balies van Burgerzaken.

De tweede uitzondering is als er sprake is van een in een wettelijke bepaling verankerd zwaarwegend algemeen belang.

Is er sprake van wetgeving die voldoet aan de voorwaarden van artikel 9, tweede lid, onderdeel g, AVG?

Dan is het verbod om biometrische gegevens te verwerken niet van toepassing. Deze voorwaarden zijn:

- de verwerking is noodzakelijk 'om redenen van zwaarwegend algemeen belang';
- dit zwaarwegende algemene belang is vastgelegd in de wettelijke bepaling;
- de evenredigheid met het nagestreefde doel wordt gewaarborgd;
- de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd; en
- passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

Het zwaarwegende belang is vastgelegd in de wetgeving zoals aangegeven in "CD.AV.1. Beschrijf het juridische en beleidsmatige kader."

Daarnaast geldt:

- Bijzondere Persoonsgegevens / Biometrische gegevens

Op grond van art. 29 UAVG is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Dat is het geval, want het proces is bedoeld om de identiteit van een persoon te verifiëren. Conclusie: er kan een beroep gedaan worden op een uitzondering.

- Bijzondere Persoonsgegevens / Ras of Etnische Afkomst gegevens

Artikel 25 onder a UAVG geeft aan dat het verbod niet van toepassing is als de gegevens over iemands ras of etnische afkomst worden gebruikt met het oog op de identificatie van de betrokkene, en alleen als het gebruik voor dat doel onvermijdelijk is. Gezien de vele verschillende identiteitsdocumenten die gemeente moet controleren, is het ondoenlijk om de echtheidscontroles van deze documenten handmatig uit te voeren. Bovendien zijn sommige

DPIA (Compact)

echtheidskenmerken alleen met hulpmiddelen als UV-licht, infraroodlicht of een RFID-scanner te controleren. Een visuele controle voldoet daarom niet. Om deze reden wil de gemeente als hulpmiddel de scanapparatuur gaan gebruiken.

Conclusie: er kan een beroep gedaan worden op een uitzondering.

- Bijzondere Persoonsgegevens / Religieuze of Levensbeschouwelijke Overtuiging gegevens

Van de foto kunnen religieuze persoonsgegevens worden afgeleid (namelijk hoofdbedekkingen: keppeltje, tulband, hoofddoek), maar wij doen niets met deze gegevens. Aangezien men niet als doel heeft om religieuze persoonsgegevens te verwerken, kan niet gezegd worden dat deze worden verwerkt. Zo'n grondslag is namelijk ook niet nodig voor cameratoezicht, aldus de Guidelines 3/2019 on processing of personal data through video devices.

Conclusie: een wettelijke grondslag is niet nodig.

Daarnaast hebben we er voor gezorgd dat de biometrische gegevens voor niemand inzichtelijk zijn. De biometrische gegevens worden niet bewaard. En de gegevens die wel worden opgeslagen zijn alleen voor daartoe bevoegde personen inzichtelijk, CD.AV.10. Autorisaties.

Wij achten de inzet van fraudebestrijdingsapparatuur bij de balies van burgerzaken daarmee rechtmatig.

CD.B.2. Noodzaak.

Zijn alle verwerkingen noodzakelijk voor het bereiken van het doel? Licht het antwoord toe.

DPIA (Compact)

Om aan de wettelijke taken van de gemeente te voldoen is het noodzakelijk is om apparatuur in te zetten. Fraude en technieken om fraude tegen te gaan wordt steeds geavanceerder en met alleen een visuele controle onvoldoende te controleren. Door het niet opslaan van de gegevens is de verwerking van vertrouwelijke gegevens minimaal en dus ook minimaal belastend voor de inwoner.

Bij vermoeden van fraude met documenten bij een gemeente wordt dit landelijk doorgestuurd naar de Marechaussee. In 2024 werd door de Marechaussee 2.183 valse (identiteits)documenten vastgesteld. In 2023 was dit 2.223.

(https://www.marechaussee.nl/binaries/marechaussee/documenten/publicaties/2025/04/07/statistisch-jaaroverzicht-van-identiteits--en-documentfraude-in-2024/ECID+Jaaroverzicht_2024.pdf)

Software die ondersteuning biedt bij het maken van de gezichtsvergelijking kan in die gevallen als noodzakelijk worden beschouwd. Zeker bij belangrijke processen, zoals de aanvraag van een (nieuw) identiteitsdocument en/of een (her)inschrijving in de gemeente, is de identiteitscontrole van groot belang. Zo ontstaat de identiteit met de registratie in de BRP. De BRP is een basisregistratie. Dat betekent dat de BRP-informatie binnen de hele overheid gebruikt wordt, bijvoorbeeld bij het verlenen van zorg, toegang tot opleidingen of toekennen van uitkeringen. Juiste registratie is de toegangspoort om voor voorzieningen in aanmerking te komen om zo volwaardig mee te kunnen doen in onze maatschappij. Het is dus van groot belang dat de gegevens in de BRP correct zijn. Met de uitgifte van een identiteitsdocument kan de ontvanger in het maatschappelijke verkeer zijn of haar identiteit aantonen. Ook de uitgifte van een paspoort, rijbewijs, identiteitskaart moet daarom correct zijn.

De door software ondersteunde gezichtsvergelijking biedt de mogelijkheid om de kans op fouten in het verificatieproces zoveel mogelijk te beperken. Onderzoek heeft uitgewezen dat de combinatie van ondersteunende software als hulpmiddel bij het menselijke oordeel succesvol is.¹ Het werk van de behandelend ambtenaar wordt door de software niet vervangen, maar wordt aangevuld met een extra controle.² Door deze combinatie is de kans op fouten bij de identiteitsvaststelling kleiner.

De balanstest: tegenover de verwerking staat de inbreuk van de inwoner. De inbreuk vinden wij minimaal omdat er geen biometrische gegevens worden opgeslagen of zichtbaar zijn voor de werknemer. Alle gegevens worden alleen verwerkt door de software en direct verwijderd na enkele seconden. De medewerker ziet hierdoor niet meer gegevens dan in de huidige situatie.

¹ 'Retrospectief zaakonderzoek heeft aangetoond dat er een goede correlatie is tussen de automatische gezichtsbeeldvergelijking en de vergelijkingen uitgevoerd door de NFI-onderzoekers. De uitkomsten van deze twee methoden kunnen worden samengenomen tot één eindconclusie resulterend in een betere berouwbaarheid van de uitspraak dan de onafhankelijke oordelen'. Zie voor het gehele onderzoek: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKewidpIW20dmMAxVmg_0HHf5sK1sQFnoECBYQAQ&url=https%3A%2F%2Fwww.forensischinstituut.nl%2Fbinaries%2Fni%2Fdocumenten%2Fpublicaties%2F2022%2F09%2F21%2Fvakbijlage-automatische-gezichtsbeeldvergelijking%2F220921%2BVakbijlage_automaat_gezicht_Versie_1.0.pdf&usg=AOvVaw22GJ-v5nBWKOwYluPNyhee&opi=89978449

² Zie voor concrete handvatten bij het inrichten van een betekenisvolle menselijke tussenkomst het consultatiedocument '[Betekenisvolle Menselijke Tussenkomst](#)' van de Autoriteit Persoonsgegevens.

DPIA (Compact)

CD.B.3. Dataminimalisatie en doelbinding.

Zijn alle persoonsgegevens strikt noodzakelijk voor het bereiken van het doel? Wordt aan de eis van doelbinding voldaan? Licht het antwoord toe.

De gegevens worden alleen gebruikt tijdens de duur van de vergelijking (enkele seconden). Alleen het rapport, zie bijlage A, wordt opgeslagen.

CD.B.4. Proportionaliteit.

Staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoelen? Licht het antwoord toe.

In overweging nemende dat:

- In "CD.B.1. Rechtmatigheid" van deze DPIA we hebben aangegeven dat wij vinden dat de inzet fraudebestrijdingsapparatuur aan de balies van burgerzaken rechtmatig is.
- In "CD.B.2. Noodzaak" van deze DPIA we aangeven dat de inzet fraudebestrijdingsapparatuur aan de balies van burgerzaken volgens ons noodzakelijk is.
- In "PD.A.10. Beschrijf de rechtsgrond(en) van verwerking" we aangeven dat de gevolgen van identiteitsfraude heel groot kunnen zijn.
- Geen personen toegang hebben tot de biometrische gegevens.
- Er geen biometrische gegevens bewaard worden.
- De toegang tot de persoonsgegevens die wel worden opgeslagen in iBurgerzaken doormiddel van autorisatie (zie CD.AV.10. Autorisaties van deze DPIA) beveiligd zijn.

Zijn wij van mening dat de inzet van fraudebestrijdingsapparatuur aan de balie van burgerzaken proportioneel is.

CD.B.5. Subsidiariteit.

Is er geen andere, voor betrokkene minder belastende manier om hetzelfde doel te bereiken? Licht het antwoord toe.

Op dit moment wordt de identiteit met een visuele controle door de baliemedewerker vastgesteld. Dit is veel minder nauwkeurig dan dat de fraudebestrijdingsapparatuur dat kan. Door veranderingen in het gezicht zoals gewichtstoename en -afname, plastische chirurgie en verandering van de haardracht is het in sommige gevallen heel lastig om te kunnen zien of degene op de foto dezelfde is als die aan de balie. Doordat de apparatuur gebruik maakt van biometrische gegevens is dit volgens ons een noodzakelijke aanvulling.

Voorafgaande raadpleging AP

Bepaal en omschrijf aan de hand van de restrisico's of de verwerking mag worden gestart of dat een voorafgaande raadpleging bij de AP nodig is.

CD.V1. Is voorafgaande raadpleging AP nodig?**Nee****Toelichting:**

Er is uitgebreid contact geweest met de AP. Zij geven aan dat gezichtsvergelijking toegestaan is omdat de gegevens niet worden opgeslagen.

De restrisico's zijn ook zo klein dat verder overleg met de AP niet nodig is.

DPIA (Compact)

Bijlage A: Rapport in iBurgerzaken

Om privacy redenen zijn de persoonsgegevens geanonimiseerd. Dit is niet zo in het werkelijke rapport.

DPIA (Compact)

Foto vergelijking (Chip - Visueel)

Chip

Visueel

Data vergelijking

	MRZ	Chip	Visuele Controle Zone
Achternaam	:		
Voornamen	:		
Documentnummer	:		
Persoonlijk nummer	:		
Geboortedatum	:		
Geldigheidsdatum	:		
Geslacht	:		
Nationaliteit	:	NLD	Nederland
CSO locatiecode	:		

Document resultaat

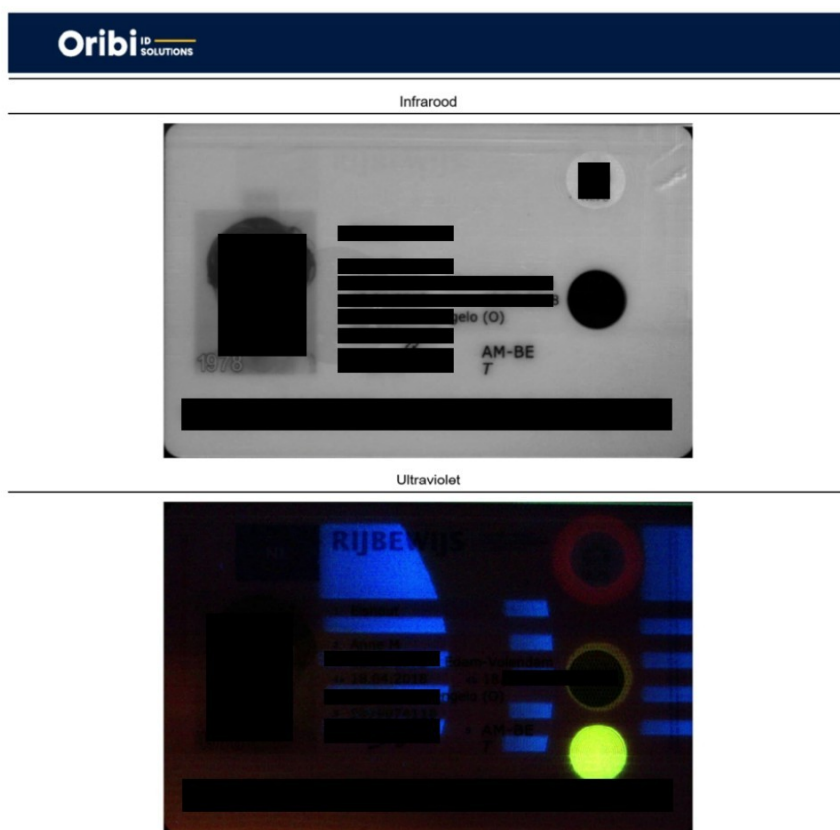
Authenticaties

Verificaties

Kruiscontrole
 : Er is maar 1 zijde van het document geclassificeerd.

Belichtingen

DPIA (Compact)



DPIA (Compact)



DPIA (Compact)

Bijlage B: Procestappen

Om privacy redenen zijn de persoonsgegevens geanonimiseerd. Dit is niet zo in het werkelijke rapport.

DPIA (Compact)

DOCUMENTSCAN

Start nieuwe ID scan
Voeg pagina toe
Orbi Scanserver formulier
Rapport

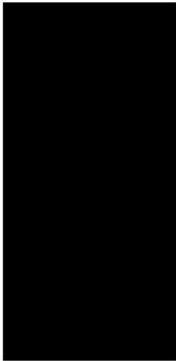
SCANNEN

Scan status: Klaar

RESULTAAT



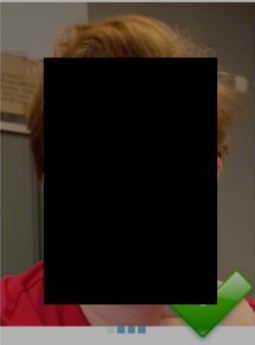
Voornamen
Voorvoegsel
Geslachtsnaam
Geboortedatum (dag/maand/jaar)
Geslacht
Nationaliteit
Geboorteplaats
Persoon identificatie nummer
Documentnummer
Document type
Afgiftedatum
Vervaldatum
Land van afgifte
Valide



Bevestigen
Annuleren

Document

Contact



PERSOONSGEGEVENS

Voornamen

Gezichtsvergelijking

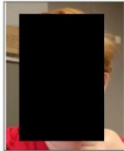
Referentieafbeelding

Contact



Vergelijkingsafbeelding

Foto 12:04:23



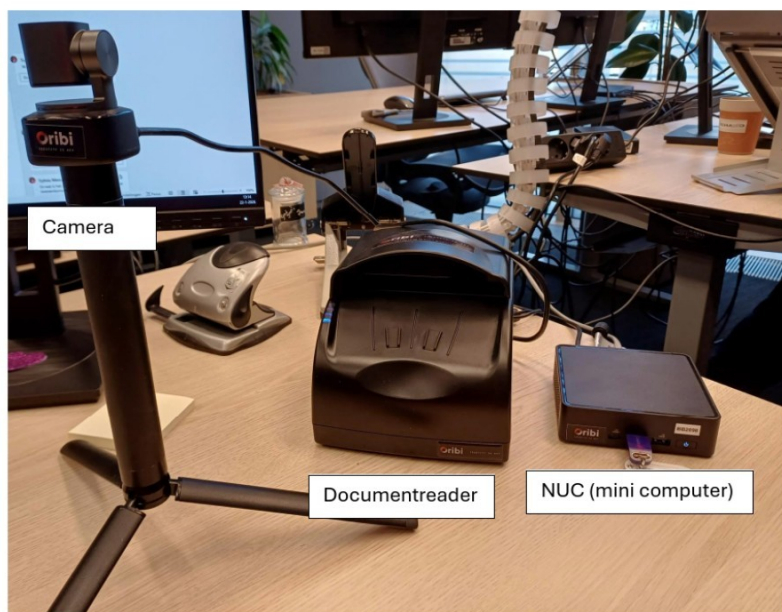
Vergelijken



Sluiten

Bijlage C: weergave opstelling

DPIA (Compact)



Bijlage D: overzicht bewaartermijnen zaken in iBurgerzaken

Zaaktypenaam	Zaakresultaat	Bewaartermijn in jaren
Aanmaken generiek document	Afgewezen	1
Aanmaken generiek document	Niet nodig	1
Aanmaken generiek document	Verwerkt	1
Aanvraag adresonderzoek	Verwerkt	10
Aanvraag afschrift burgerlijke stand	Afgewezen	1
Aanvraag afschrift burgerlijke stand	Niet nodig	1
Aanvraag afschrift burgerlijke stand	Verwerkt	1
Aanvraag bewijs van in leven zijn	Afgewezen	1
Aanvraag bewijs van in leven zijn	Niet nodig	1
Aanvraag bewijs van in leven zijn	Verwerkt	20
Aanvraag bewijs van in leven zijn	Verwerkt	20
Aanvraag bewijs van Nederlanderschap	Afgewezen	1
Aanvraag bewijs van Nederlanderschap	Niet nodig	1
Aanvraag bewijs van Nederlanderschap	Verwerkt	20
Aanvraag stempas	Afgewezen	1
Aanvraag stempas	Niet nodig	1

DPIA (Compact)

Aanvraag stempas	Verwerkt	5
Actualisering PL	Afgewezen	5
Actualisering PL	Niet nodig	1
Actualisering PL	Verwerkt	10
Adoptie	Afgewezen	1
Adoptie	Verwerkt	1,5
Adresonderzoek	Afgerond	10
Adresonderzoek	Afgewezen	1
Adresonderzoek	Niet nodig	1
Adresonderzoek	Verwerkt	10
Benoemen openbare ruimte	Afgewezen	1
Benoemen openbare ruimte	Verwerkt	10
Bijhouding PL	Afgewezen	5
Bijhouding PL	Niet nodig	1
Bijhouding PL	Verwerkt	1
Bijhouding PL	Verwerkt	10
Bijhouding Verwijsgegevens	Verwerkt	10
Brondocument vervangen	Afgewezen	5
Brondocument vervangen	Niet nodig	5
Brondocument vervangen	Verwerkt	1,5
Controle briefadres	Afgewezen	1

DPIA (Compact)

Controle briefadres	Niet nodig	1
Controle briefadres	Verwerkt	10
Echtscheiding of ontbinding partnerschap	Afgerond	1,5
Echtscheiding of ontbinding partnerschap	Afgewezen	5
Echtscheiding of ontbinding partnerschap	Niet nodig	1
Echtscheiding of ontbinding partnerschap	Verwerkt	110
Eerste inschrijving	Afgerond	110
Eerste inschrijving	Afgewezen	5
Eerste inschrijving	Niet nodig	5
Eerste inschrijving	Verwerkt	110
Eerste inschrijving	Verwerkt	110
Erkenning kind	Afgewezen	5
Erkenning kind	Niet nodig	1
Erkenning kind	Verwerkt	110
Erkenning ongeboren vrucht	Afgewezen	5
Erkenning ongeboren vrucht	Niet nodig	1
Erkenning ongeboren vrucht	Verwerkt	110
Geboorte	Afgewezen	5
Geboorte	Niet nodig	1
Geboorte	Verwerkt	110
Geheimhouding	Afgewezen	1

DPIA (Compact)

Geheimhouding	Niet nodig	1
Geheimhouding	Verwerkt	5
Generieke akte of Latere vermelding	Afgewezen	5
Generieke akte of Latere vermelding	Niet nodig	1
Generieke akte of Latere vermelding	Verwerkt	110
Geslachtsnaamwijziging	Afgewezen	5
Geslachtsnaamwijziging	Niet nodig	1
Geslachtsnaamwijziging	Verwerkt	110
Hernoemen openbare ruimte	Afgewezen	1
Hernoemen openbare ruimte	Niet nodig	1
Hernoemen openbare ruimte	Verwerkt	10
Hervestiging	Afgewezen	5
Hervestiging	Niet nodig	1
Hervestiging	Verwerkt	5
Huwelijk of Partnerschap	Afgewezen	5
Huwelijk of Partnerschap	Niet nodig	1
Huwelijk of Partnerschap	Verwerkt	110
Indienen toestemmingsformulier reisdocument	Afgewezen	1
Indienen toestemmingsformulier reisdocument	Niet nodig	1
Indienen toestemmingsformulier reisdocument	Verwerkt	16

DPIA (Compact)

Infrastructurele wijziging	Afgewezen	5
Infrastructurele wijziging	Niet nodig	1
Infrastructurele wijziging	Verwerkt	10
Lijkvinding	Afgewezen	5
Lijkvinding	Niet nodig	1
Lijkvinding	Verwerkt	110
Naamgebruik wijzigen	Afgewezen	5
Naamgebruik wijzigen	Niet nodig	1
Naamgebruik wijzigen	Verwerkt	5
Naamskeuze	Afgewezen	5
Naamskeuze	Niet nodig	1
Naamskeuze	Verwerkt	5
Naamskeuze na geboorte	Afgewezen	5
Naamskeuze na geboorte	Verwerkt	5
Naturalisatie	Afgewezen	5
Naturalisatie	Niet nodig	1
Naturalisatie	Verwerkt	10
Nieuwe verkiezing	Afgewezen	1
Nieuwe verkiezing	Niet nodig	1
Nieuwe verkiezing	Verwerkt	20
Omzetting partnerschap in huwelijk	Afgewezen	5

DPIA (Compact)

Omzetting partnerschap in huwelijk	Niet nodig	1
Omzetting partnerschap in huwelijk	Verwerkt	110
Optieverzoek	Afgewezen	5
Optieverzoek	Niet nodig	1
Optieverzoek	Verwerkt	12
Overlijden	Afgerond	1,5
Overlijden	Afgewezen	5
Overlijden	Niet nodig	1
Overlijden	Verwerkt	110
Registratie beëindiging huwelijk of partnerschap	Verwerkt	1,5
Registratie huwelijk of partnerschap	Afgewezen	5
Registratie huwelijk of partnerschap	Verwerkt	1,5
Reisdocument inname	Afgewezen	5
Reisdocument inname	Niet nodig	1
Reisdocument inname	Verwerkt	11
Reisdocument inname	Verwerkt	11
Reisdocument nieuw	Afgewezen	1
Reisdocument nieuw	Niet nodig	1
Reisdocument nieuw	Verwerkt	11
Reisdocument nieuw	Verwerkt	16

DPIA (Compact)

Rijbewijs aanvraag	Afgewezen	1
Rijbewijs aanvraag	Niet nodig	1
Rijbewijs aanvraag	Verwerkt	11
Rijbewijs bijzondere aanvraag	Afgewezen	1
Rijbewijs bijzondere aanvraag	Niet nodig	1
Rijbewijs bijzondere aanvraag	Verwerkt	11
Rijbewijs ongeldig verklaren	Afgewezen	1
Rijbewijs ongeldig verklaren	Niet nodig	1
Rijbewijs ongeldig verklaren	Verwerkt	1
Rijbewijs registratie vermissing	Afgewezen	1
Rijbewijs registratie vermissing	Niet nodig	1
Rijbewijs registratie vermissing	Verwerkt	1
Rijbewijs uitreiken	Afgewezen	1
Rijbewijs uitreiken	Niet nodig	1
Rijbewijs uitreiken	Verwerkt	11
Samenvoeging	Verwerkt	10
Sloop	Afgewezen	1
Sloop	Verwerkt	10
Splitsing	Afgewezen	1
Splitsing	Verwerkt	10

DPIA (Compact)

Toevoegen brondocument	Afgewezen	5
Toevoegen brondocument	Afgewezen	1
Toevoegen brondocument	Niet nodig	1
Toevoegen brondocument	Verwerkt	1,5
Uittreksel BRP	Afgewezen	1
Uittreksel BRP	Niet nodig	1
Uittreksel BRP	Verwerkt	20
Verhuizing binnen Nederland	Afgerond	5
Verhuizing binnen Nederland	Afgewezen	5
Verhuizing binnen Nederland	Niet nodig	1
Verhuizing binnen Nederland	Verwerkt	5
Verhuizing buitenland	Afgewezen	5
Verhuizing buitenland	Niet nodig	1
Verhuizing buitenland	Verwerkt	10
Verklaring omtrent gedrag	Afgewezen	1
Verklaring omtrent gedrag	Niet nodig	1
Verklaring omtrent gedrag	Verwerkt	7
Verklaring voor stemmen Europees Parlement in Nederland	Verwerkt	10
Voornaam- of Geslachtswijziging	Afgewezen	5
Voornaam- of Geslachtswijziging	Niet nodig	1
Voornaam- of Geslachtswijziging	Verwerkt	5

DPIA (Compact)

--	--	--

Bijlage E Website fraudebestrijding

Camera met gezichtsvergelijking

Op elke balie van burgerzaken staat een camera met gezichtsvergelijking. Deze camera gebruiken we om fraude met identiteitsdocumenten tegen te gaan, bijvoorbeeld een paspoort, identiteitskaart of rijbewijs. Het is voor ons belangrijk dat wij zeker weten dat u bent wie u zegt dat u bent. Daarom gebruiken wij de camera met gezichtsvergelijking.

U kunt het gebruik van gezichtsvergelijking niet weigeren. Zonder gezichtsvergelijking kunnen wij u niet helpen.

Zo werkt de camera

Bij de balie geeft u uw identiteitsdocument aan de balied medewerker. De balied medewerker legt het document in de scanner. De scanner controleert de gegevens die op uw document staan, bijvoorbeeld uw naam, geboortedatum en de datum waarop het document verloopt. Daarna maakt de camera een foto van u.

De computer doet een gezichtsvergelijking met uw biometrische gegevens zoals de stand van uw ogen en de vorm van uw neus. Na de gezichtsvergelijking geeft de computer aan of de 3 foto's van dezelfde persoon zijn. Dat zijn de foto op uw document, de foto in de chip en de foto van de camera. Ook kan de balied medewerker zien hoe goed de gezichten op elkaar lijken.

Gegevens voor gezichtsvergelijking niet bewaard

Uw gegevens worden direct na het maken van de vergelijking automatisch van de computer verwijderd. Uw gegevens staan dus maar een aantal seconden op de computer. Niemand kan uw gegevens zien, ook de balied medewerker niet. Wij geven uw gegevens niet door aan andere instanties.

Camera's bij alle balies van burgerzaken

We gebruiken de camera voor:

-  Het aanvragen en afhalen van een paspoort of identiteitskaart
-  Het aanvragen en afhalen van een rijbewijs
-  Het regelen van uw huwelijk
-  De aangifte van uw pasgeboren kind
-  Het doorgeven van een overlijden
-  Uw inschrijving in de gemeente
-  Het doorgeven van uw verhuizing
-  Het aanvragen van uw naturalisatie

Gezichtsvergelijking om fraude tegen te gaan

Er is steeds meer fraude met identiteitsdocumenten. De gemeente is wettelijk verplicht om goed vast te stellen dat de persoon die een document aanvraagt ook echt deze persoon is. Dit staat in Artikel 28 Paspoortwet, Artikel 22 en artikel 39, lid 1 Paspoortuitvoeringsregeling Nederland 2001 (PUN). Camera's met gezichtsvergelijking helpen ons hierbij.

Voordat wij uw gegevens veranderen in de Basisregistratie Personen (BRP), willen wij zeker weten dat u het bent. Ook dat zijn wij wettelijk verplicht. Dit staat in Artikel 2.4, lid 3 en Artikel 2.19, lid 5 Wet Basisregistratie Personen (Wet BRP) en Algemene Verordening Gegevensbescherming (AVG) Artikel 6 lid 1 sub C. Ook hierbij helpen de camera's met gezichtsvergelijking.

DPIA (Compact)

Negatieve uitslag gezichtsvergelijking

Als de gezichtsvergelijking negatief is bespreekt de baliemedewerker dit met u. Er kan een reden zijn waardoor uw foto's niet voldoende op elkaar lijken. De baliemedewerker vraagt altijd een collega om mee te kijken. Zijn er twijfels of er sprake is van fraude, dan bellen wij de politie.

Heeft u vragen

Wij helpen u graag als u vragen heeft. U bereikt ons van maandag tot en met vrijdag van 09.00 tot 17.00 uur via telefoonnummer 14 053.

DPIA (Compact)

Bijlage G

Alle echtheidskenmerken van een Nederlands paspoort zijn hier te vinden:

<https://www.rvig.nl/kenmerkenbrochure-identiteitskaart-model2024>

DPIA (Compact)

Bijlage H: Bionormen

BIO Nummer	Control /Beveiligingsmaatregel	Aanwezig
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Ja
6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	Gedeeltelijk
6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	Nee
6.2.1.1	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	Niet van toepassing
6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a. In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b. Het device maakt deel uit van patchmanagement en hardening. c. Er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d. Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. e. Periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd	Niet van toepassing
8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	Ja

DPIA (Compact)

8.3.2.1	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	Ja
8.3.2.2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	Ja
8.3.2.3	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	Ja
8.3.3.1	Er is een vastgestelde procedure voor het fysiek transport van media.	Ja
8.3.3.2	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	Niet van toepassing
9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Ja
9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Ja
9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Ja
9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Ja
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	Ja
9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	Ja
9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Ja
9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Gedeeltelijk
9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	Ja

DPIA (Compact)

9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	Ja
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Ja
9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Ja
9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Ja
9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Ja
9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Gedeeltelijk
9.4.2.2	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Ja
9.4.3.1	Als er geen gebruik wordt gemaakt van two factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	Ja
9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	Gedeeltelijk
9.4.3.3	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	Gedeeltelijk
9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Ja
9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Gedeeltelijk
9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Ja

DPIA (Compact)

9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Niet van toepassing
10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	Niet van toepassing
10.1.2.2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Niet van toepassing
11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	Ja
11.1.4.1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	Ja
11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	Ja
11.2.9.1	Een onbemende werkplek is altijd vergrendeld.	Ja
11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	Ja
11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	Ja
11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	Ja
11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	Niet van toepassing
12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	Ja
12.1.3.1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service) te signaleren en hierop te reageren.	Ja

DPIA (Compact)

12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	Ja
12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	Ja
12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	Ja
12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	Ja
12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Ja
12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; (b) bijlagen en downloads vóór gebruik.	Ja
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	Ja
12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	Ja
12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	Ja
12.3.1.3	In het back-up beleid staan minimaal de volgende eisen: (a) dataverlies bedraagt maximaal 28 uur; (b) hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	Ja
12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Ja
12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Ja

DPIA (Compact)

12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	Ja
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Ja
12.4.1.3	De informatie verwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectievoorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties), die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	Niet van toepassing
12.4.1.4	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Niet van toepassing
12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Niet van toepassing
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	Ja
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	Gedeeltelijk
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	Niet van toepassing
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	Ja
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een	Ja

DPIA (Compact)

	expliciete risicoafweging mitigerende maatregelen getroffen.	
12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Ja
13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Ja
13.1.2.2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Niet van toepassing
13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Niet van toepassing
13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Niet van toepassing
13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Ja
13.2.3.1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.	Ja

DPIA (Compact)

13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling	Niet van toepassing
13.2.3.3	Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontleen.	Niet van toepassing
13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Niet van toepassing
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	Ja
14.2.5.1	Zie Rijksmaatregel 14.2.1.1	Niet van toepassing
14.2.6.1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging	Ja
14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Gedeeltelijk
14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	Ja
15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	Niet van toepassing
15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	Niet van toepassing
15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	Ja
15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	Ja
15.1.2.5	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	Ja

DPIA (Compact)

15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	Ja
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Onbekend
15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	Onbekend
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	Ja
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Ja
16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	Ja
16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	Ja
16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	Ja
16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Ja
16.1.2.7	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.	Niet van toepassing
16.1.3.1	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.	Niet van toepassing
16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	Niet van toepassing
16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.	Ja

DPIA (Compact)

16.1.6.2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	Gedeeltelijk
16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	Gedeeltelijk
17.1.3.1	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	Ja
17.1.3.2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	Ja
17.1.3.3	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	Niet van toepassing
18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Ja
18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	Ja
18.1.4.2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en –procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Ja
18.2.1.1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	Ja
18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Gedeeltelijk
18.2.2.1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, Generieke verantwoording.	Ja
18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Ja

Bijlage I

Resultaten AI-verordening Beslischulp

Fraudebestrijding door gezichtsvergelijking bij de balies

Biometrische verificatie met als doel te bevestigen dat een specifieke natuurlijke persoon de persoon is die hij of zij beweert te zijn)

Gegenereerd op vrijdag 6 maart 2026 om 10:17

Bron: [AI-verordening Beslischulp](#)

Versie: development

Belangrijke informatie

Dit rapport bevat de resultaten van de AI-verordening Beslischulp. Het geeft een overzicht van uw antwoorden en de daaruit voortvloeiende conclusies.

Let op: bij het interpreteren van de resultaten zijn de volgende punten van belang:

- De AI-verordening beslischulp is een betaversie: de informatie is niet compleet en er kunnen fouten in staan. Kom je iets tegen? Mail naar: ai-verordening@minbzk.nl
- Je doorloopt de AI-verordening beslischulp op basis van je eigen antwoorden. De AI-verordening beslischulp kan niet vaststellen of jouw antwoorden waar zijn of niet.
- De AI-verordening beslischulp is geen check op jouw eigen kennis en inzichten en je blijft zelf verantwoordelijk voor de informatie die je gebruikt.
- Wij adviseren de uitkomsten van de AI-verordening beslischulp met andere experts in jouw organisatie te delen en te bespreken.
- Dit rapport is een momentopname en weerspiegelt de antwoorden die zijn gegeven tijdens het doorlopen van de AI-verordening beslischulp.
- Dit rapport is bedoeld als een hulpmiddel en dient niet als juridisch advies te worden beschouwd.
-

DPIA (Compact)

AI-verordening Profiel

Categorie	Resultaat
Verantwoordelijkheid	gebruiksverantwoordelijke
Operationeel	in gebruik
Soort toepassing	AI-systeem
Risicogroep	hoog-risico AI
Transparantieverplichting	geen transparantieverplichting

DPIA (Compact)

Antwoorden

Vraag 1.1: Bevat de (beoogde) toepassing een algoritme?

Antwoord: Ja

Vraag 1.2: Ontwikkelen jullie de toepassing in eigen beheer of is/wordt deze ontwikkeld door een andere partij?

Antwoord: We gebruiken een extern ontwikkelde toepassing zonder aanpassingen

Vraag 1.3: Is de toepassing al in gebruik of niet?

Antwoord: In gebruik

Opmerking: Bij verschillende gemeenten in gebruik, ook vermelding in algoritmeregister.

Vraag 1.4.1: Is jouw (beoogde) toepassing een AI-systeem?

Antwoord: Ja, het is een AI-systeem

Vraag 1.5: Is er voor de (beoogde) toepassing sprake van een uitzonderingsgrond? Antwoord: Nee

Vraag 2.0: Op basis van de ingevulde antwoorden is de AI-verordening op jou van toepassing.

Antwoord: Naar risicogroep bepaling

Vraag 2.1: Valt de toepassing onder een van de verboden systemen uit Artikel 5 van de Alverordening?

Antwoord: Nee

Vraag 2.3: Is het AI-systeem bedoeld om te worden gebruikt als een veiligheidscomponent van een product dat valt onder de lijst in Bijlage I? Antwoord: Geen van beide

Vraag 2.4: Valt het AI-systeem onder een van de hoog-risico systemen uit Bijlage III van de Alverordening? Antwoord: Ja

Opmerking: 1. Nee, omdat:

Systemen voor biometrische identificatie op afstand (dit geldt niet voor AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie met als enig doel te bevestigen dat een specifieke natuurlijke persoon de persoon is die hij of zij beweert te zijn).

2. Ja, omdat:

DPIA (Compact)

AI-systemen die bedoeld zijn om door of namens overheidsinstanties te worden gebruikt om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en diensten, waaronder gezondheidsdiensten, of om dergelijke uitkeringen en diensten te verlenen, te beperken, in te trekken of terug te vorderen.

Als een inwoner wordt verplicht om aan gezichtsvergelijking mee te werken bij het aanvragen van een paspoort, zonder alternatief, raakt dit mogelijk aan fundamentele rechten. De AI act zegt, als biometrische herkenning wordt ingezet om toegang te bepalen tot essentiële diensten zoals overheidsdiensten, kan het systeem alsnog onder de hoog-risico regels vallen. Een paspoort is een essentieel identiteitsdocument, zonder paspoort kan een inwoner niet reizen, zich niet identificeren bij bepaalde diensten, etc.

Vraag 2.7.2: Is het verplicht om de conformiteitsbeoordeling door een derde partij, zoals een conformiteitsbeoordelingsinstantie, uit te laten voeren? Antwoord: Nee

Vraag 2.5: Voert het AI-systeem profilering van natuurlijke personen uit?

Antwoord: Nee

Vraag 2.6: Is er sprake van een uitzondering op de lijst van hoog-risico AI-systemen (uit bijlage III)?

Antwoord: Nee

Vraag 2.9: Moet het AI-systeem voldoen aan de transparantieplichtingen?

Antwoord: Nee

Conclusie

Op basis van de ingevulde antwoorden is de AI-verordening op jou van toepassing. Je bent een gebruiksverantwoordelijke van een hoog-risico AI-systeem.

DPIA (Compact)

Verplichtingen

Verplichtingen voor alle AI-systemen:

- AI-geletterdheid (Artikel 4)
- Gedragscodes voor vrijwillige toepassing van specifieke voorschriften (Artikel 95)

Geldig vanaf:

- AI-geletterdheid (Artikel 4) gaat vanaf februari 2025 in werking.
- Gedragscodes (Artikel 95) zijn vrijwillig en kunnen op elk moment na de inwerkingtreding van de Alverordening worden opgesteld en toegepast.

Verplichtingen van gebruiksverantwoordelijken van AI-systemen met een hoog risico (Artikel 26 en Artikel 27):

- Het nemen van passende technische en organisatorische maatregelen om te waarborgen dat dergelijke systemen in overeenstemming met de gebruiksaanwijzingen die bij de systemen zijn gevoegd worden gebruikt
- Het opdragen van menselijk toezicht aan natuurlijke personen die over de nodige bekwaamheid, opleiding en autoriteit beschikken en de nodige ondersteuning krijgen
- Het ervoor zorgen dat, voor zover de gebruikersverantwoordelijke controle heeft over de inputdata, de inputdata relevant en voldoende representatief zijn voor het beoogde doel van het AI-systeem met een hoog risico
- Het monitoren van de werking van het AI-systeem met een hoog risico op basis van de gebruiksaanwijzingen en in voorkomend geval het in kennis stellen van de aanbieders overeenkomstig Artikel 72.
- Het bewaren van de logs die automatisch worden gegenereerd door dat AI-systeem met een hoog risico voor zover dergelijke logs onder controle van de gebruiksverantwoordelijke vallen gedurende een periode die passend is voor het beoogde doel van het AI-systeem met een hoog risico, of ten minste zes maanden
- Voordat een AI-systeem met een hoog risico op de werkplek in gebruik wordt gesteld of wordt gebruikt, delen gebruiksverantwoordelijken die werkgever zijn werknemersvertegenwoordigers en de betrokken werknemers mee dat zij zullen worden onderworpen aan het gebruik van het AI-systeem met een hoog risico
- Gebruiksverantwoordelijken van AI-systemen met een hoog risico die de hoedanigheid van overheidsinstanties of instellingen, organen of instanties van de Unie hebben, leven de in Artikel 49 bedoelde registratieverplichtingen na. Wanneer deze gebruiksverantwoordelijke vaststellen dat het AI-systeem met een hoog risico dat zij voornemens zijn te gebruiken niet in de in Artikel 71 bedoelde

DPIA (Compact)

EU-databank is geregistreerd, gebruiken zij dat systeem niet en stellen zij de aanbieder of de distributeur daarvan in kennis

- Indien van toepassing, gebruiken gebruiksverantwoordelijken van AI-systemen met een hoog risico de informatie die op grond van Artikel 13 van deze verordening wordt verstrekt om hun verplichting na te komen om een gegevensbeschermingseffectbeoordeling uit te voeren
- De gebruiksverantwoordelijke van een AI-systeem met een hoog risico voor biometrische identificatie op afstand verzoekt achteraf in het kader van een onderzoek waarbij gericht wordt gezocht naar een persoon die wordt verdacht van of veroordeeld is voor het plegen van een strafbaar feit, vooraf of zonder onnodige vertraging en uiterlijk 48 uur na het feit, om toestemming van een gerechtelijke instantie of administratieve instantie, van wie de beslissing bindend is en onderworpen is aan rechterlijke toetsing, voor het gebruik van dat systeem, behalve wanneer het wordt gebruikt voor de initiële identificatie van een potentiële verdachte op basis van objectieve en verifieerbare feiten die rechtstreeks verband houden met het strafbare feit. Elk gebruik wordt beperkt tot hetgeen strikt noodzakelijk is voor het onderzoek naar een specifiek strafbaar feit
- Gebruiksverantwoordelijken van in bijlage III bedoelde AI-systemen met een hoog risico die beslissingen met betrekking tot natuurlijke personen nemen of helpen nemen, informeren de natuurlijke personen dat het AI-systeem met een hoog risico op hen wordt toegepast.
- Gebruiksverantwoordelijken werken samen met de relevante bevoegde autoriteiten bij alle door deze autoriteiten genomen maatregelen met betrekking tot een AI-systeem met een hoog risico met het oog op de uitvoering van deze verordening.
- Gebruiksverantwoordelijken die publiekrechtelijke organen zijn of particuliere entiteiten zijn die openbare diensten verlenen, en gebruiksverantwoordelijken van AI-systemen met een hoog risico gebruikt in krediet/verzekering (bijlage III, 5, c en d) een beoordeling uit van de gevolgen voor de grondrechten die het gebruik van een dergelijk systeem kan opleveren (Artikel 27).

Geldig vanaf (Artikel 111):

- Voor AI-systemen in ontwikkeling geldt dat de verordening volledig in werking treedt op 2 augustus 2026, wat betekent dat deze systemen vanaf die datum aan de voorschriften moeten voldoen.
- Voor AI-systemen in gebruik die vóór 2 augustus 2026 zijn geïntroduceerd, geldt dat de verordening alleen van toepassing is als ze significante wijzigingen ondergaan, maar voor AI-systemen met een hoog risico, met name die bedoeld voor overheidsgebruik, moeten aanbieders uiterlijk op 2 augustus 2030 aan alle vereisten voldoen, ongeacht ontwerp wijzigingen.

Bronnen

AI-verordening Beslischulp

<https://ai-verordening-beslischulp.apps.digilab.network>

AI-verordening Beslischulp Github <https://github.com/MinBZK/ai-verordening-beslischulp>

Tijddlijn AI-verordening Algoritmekader

DPIA (Compact)

<https://minbzk.github.io/Algoritmekader/voldoen-aan-wetten-en-regels/tijdlijn-aiverordening/>

Artikel 4 - AI-geletterdheid https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e2799-1-1

Artikel 26 - Verplichtingen van gebruiksverantwoordelijken van AI-systemen met een hoog risico https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e4350-1-1

Artikel 27 - Beoordeling van de gevolgen voor de grondrechten van AI-systemen met een hoog risico https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e4433-1-1

Artikel 72 - Monitoring door aanbieders na het in de handel brengen en plan voor monitoring na het in de handel brengen voor AI-systemen met een hoog risico https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e7075-1-1

Artikel 73 - Melding van ernstige incidenten https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e7117-1-1

Artikel 79 - Procedure op nationaal niveau voor de omgang met AI-systemen die een risico vormen https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e7480-1-1

Artikel 95 - Gedragscodes voor vrijwillige toepassing van specifieke voorschriften https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e8052-1-1

Artikel 111 - Reeds in de handel gebrachte of in gebruik gestelde AI-systemen https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689#d1e8928-1-1