## DPIA informatie Inburgeringswet 2021

**DPIA**

Inburgeringswet 2021

**Auteursnaam**

Johannes Homan

**Naam van de beoordelaar**

VNG projectgroep

**Aanmaakdatum**

10/03/2021

## Context

**Overzicht**

**Welke gegevensverwerking wordt overwogen?**

Gegevensuitwisseling en -verwerking ten behoeve van inburgering van inburgeringsplichtigen

**Wat zijn de doeleinden van de gegevensverwerkingen?**

Mogelijk maken dat nieuwkomers zelfstandig kunnen deelnemen aan de Nederlandse samenleving.

**Waar vinden de gegevensverwerkingen plaats?**

Binnen de systemen van de IND en binnen de systemen van individuele gemeenten. In principe binnen de EER, als daarvan wordt afgeweken is het vermeld in de dataleveringsovereenkomsten/verwerkingsovereenkomsten tussen betrokken partijen (IND, DUO, Gemeenten, leveranciers van cursussen)

**Welke verantwoordelijkheden zijn verbonden aan de gegevensverwerking?**

COA
Verantwoordelijke voor eigen verwerking van de gegevens van nieuwkomers in heel Nederland.

Gemeenten
Verantwoordelijke voor registratie van gevenens van nieuwkomers tbv inburgeringstaken.

DUO
Voert taken minister SZW uit en is daarmee een verwerker voor registratie van gegevens van nieuwkomers tbv registratie diploma's/certificaten.

Leveranciers van cursussen
Door gemeenten ingehuurde organisaties voor het verzorgen van cursussen aan nieuwkomers.

**Welke wet- en regelgevingen hebben betrekking op de gegevensverwerkingen?**

Wet inburgering 2021(Nog niet van kracht)
Besluit inburgering
Regeling inburgering

**Zijn er normen van toepassing op de gegevensverwerking?**

Geen specifieke gedragscodes van toepassing

## Gegevens, processen en de levenscyclus ondersteunende systemen

**Welke persoonsgegevens worden verwerkt?**

Arbeidsgegevens
Contactgegevens
Identiteitsgegevens
Persoonlijke gegevens

**Welke bijzondere persoonsgegevens worden verwerkt?**

|  |  |
| --- | --- |
|

|  |
| --- |
| Religieuze of levensbeschouwelijke overtuigingen |

 |
| Gezondheidsgegevens |

**Hoe werkt de levenscyclus van persoonsgegevens en processen?**

50 jaar voor de volgende gegevens:

a)     burgerservicenummer;

b)     naamgegevens;

c)     adresgegevens;

d)     woonplaats;

e)     geboortedatum;

f)       gegevens die betrekking hebben op gehele of gedeeltelijke vrijstelling van de inburgeringsplicht;

g)     gegevens die betrekking hebben op een ontheffing van de inburgeringsplicht;

h)     de datum en de wijze waarop aan de inburgeringsplicht is voldaan.

Andere gegevens worden vijf jaar na beëindiging inburgeringsplicht verwijderd, of na overlijden inburgeringsplichtige.

**Beschrijf de systemen, technieken en methoden voor gegevensverwerking.**

**Wat zijn de persoonsgegevens ondersteunende systemen?**

COA: TVS

Gemeenten: Specifiek inburgeringssysteem /BRP

DUO: Portaal inburgering

**Welke technieken en methoden worden gebruikt voor de gegevensverwerking?**

Er worden geen bijzondere technieken en methoden zoals profiling e.d. gebruikt.

## Fundamentele principes

**Evenredigheid en noodzaak**

**Zijn de verwerkingsdoeleinden gespecificeerd, expliciet en legitiem?**

De doelen zijn expliciet genoemd in wet en besluit. De verwerking gaat niet verder dan de taken die wet en besluit worden genoemd.

**Wat is de wettelijke basis om de gegevensverwerking rechtmatig te maken?**

AVG artikel 6.1(f) + wet inburgering 2021 en besluit inburgering

**Zijn de persoonsgegevens adequaat, relevant en beperkt tot wat nodig is met betrekking tot de doeleinden waarvoor ze worden verwerkt ('gegevensminimalisatie')?**

Arbeidsgegevens; voor inburgering op maat en bepaling eventuele aangepaste leerroute
Contactgegevens;
Identiteitsgegevens;
Persoonlijke gegevens;

|  |  |
| --- | --- |
|

|  |
| --- |
| Religieuze of levensbeschouwelijke overtuigingen: Uitsluitend van betrokkenen die een geestelijk bedienaar zijn |

 |
| Gezondheidsgegevens: Het college mag gezondheidsgegevens verwerken als dat noodzakelijk is voor de beoordeling van gehele of gedeeltelijke ontheffing van de inburgeringsplicht en de verlenging van de termijn en bij de brede intake , de vaststelling van het PIP en de ondersteuning en begeleiding t.b.v. de leerroute (art. 37 lid 2 Wet). |
|   |

**Zijn de persoonsgegevens juist en worden ze up-to-date gehouden?**

Te beschrijven door iedere betrokken partij:

COA

Gemeenten

DUO

**Wat is de bewaartermijn van de persoonsgegevens?**

Bewaartermijnen (art. 9.9 Besluit)

50 jaar voor de volgende gegevens:

a)     burgerservicenummer;

b)     naamgegevens;

c)     adresgegevens;

d)     woonplaats;

e)     geboortedatum;

f)       gegevens die betrekking hebben op gehele of gedeeltelijke vrijstelling van de inburgeringsplicht;

g)     gegevens die betrekking hebben op een ontheffing van de inburgeringsplicht;

h)     de datum en de wijze waarop aan de inburgeringsplicht is voldaan.

Andere gegevens worden vijf jaar na beëindiging inburgeringsplicht verwijderd, of na overlijden inburgeringsplichtige

## Hoe geregeld wordt dat betrokkenen hun persoonlijke rechten kunnen uitoefenen.

**Hoe worden de betrokkenen geïnformeerd over de gegevensverwerking?**

Bij de brede intake door gemeenten worden ze mondeling geïnformeerd over de gegevensverwerking. (folder?)

**Hoe wordt de toestemming van betrokkenen verkregen?**

Toestemming is niet van toepassing want de grondslag is "Uitvoering taak openbaar gezag" (AVG 6.1.f en inburgeringswet).

**Hoe kunnen betrokkenen hun recht op toegang en overdraagbaarheid van persoonsgegevens uitoefenen?**

Zie privacyverklaring op website gemeente voor rechten van betrokkenen (meenemen in folder bij brede intake).

**Hoe kunnen betrokkenen hun recht op rectificatie en verwijdering uitoefenen?**

Zie privacyverklaring op website gemeente voor rechten van betrokkenen (meenemen in folder bij brede intake).

**Hoe kunnen betrokkenen hun recht op beperking uitoefenen en bezwaar maken?**

Zie privacyverklaring op website gemeente voor rechten van betrokkenen (meenemen in folder bij brede intake).

**Zijn de verplichtingen van de verwerkers duidelijk geïdentificeerd en geregeld in een (verwerkers)overeenkomst?**

Wordt geregeld (meeleveren in pakketje informatie voor gemeenten).

**Zijn de persoonsgegevens in het geval van gegevensoverdracht buiten de Europese Unie voldoende beschermd?**

In te vullen door individuele verantwoordelijken(basisdocumentatie meegeleverd in pakketje informatie voor gemeenten (standaard verwerkersovereenkomst en dataleveringsovereenkomst zelfstandig verwerkingsverantwoordelijke).

## Risico's

**Geplande of bestaande maatregelen**

**6.1.2 Scheiding van taken**

**7.1.2 Beveiliging in arbeidsvoorwaarden**

**7.1.1 Screening personeel**

**6.2.2 Telewerkbeleid**

**8.3.1 Beheer van verwijderbare media**

**8.2.1 Classificatie van informatie**

**8.2.3 Procedures voor behandelen van bedrijfsmiddelen**

**9.4.3 Systeem voor wachtwoordbeheer**

**8.3.2 Procedures voor verwijderen van media**

**9.1.2 Alleen bevoegde toegang tot netwerken en netwerkdiensten**

**9.4.2 Beveiligde inlogprocedures**

**8.3.3 Bescherming media bij fysiek overdragen**

**9.1.1 Beleid voor toegangsbeveiliging**

**9.2.2 Procedure voor toegang verlenen gebruikers**

**9.2.1 Registratie en afmelden van gebruikers**

**9.4.1 Beperking toegang tot informatie**

**9.2.6 Toegangsrechten intrekken of aanpassen bij beëindigen werkzaamheden**

**10.1.2 Sleutelbeheer**

**10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen**

**11.1.1 Gebruik fysieke beveiligingszones**

**11.2.9 ‘Clear desk’- en ‘clear screen’-beleid**

**11.2.8 Bescherming onbeheerde gebruikersapparatuur**

**12.4.2 Beschermen van informatie in logbestanden**

**13.2.1 Beleid en procedures voor informatietransport**

**13.2.2 Overeenkomsten over informatietransport**

**13.2.3 Bescherming elektronische berichten**

**14.1.2 Toepassingen op openbare netwerken beveiligen**

**14.1.3 Transacties van toepassingen beschermen**

**13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst**

**18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen**

**Encryptie**

**Logische toegangscontrole**

**Minimaliseren van de hoeveelheid persoonsgegevens**

**Traceerbaarheid (logging)**

**Archiveren**

**Operationele beveiliging**

**Vasthouden aan schadelijke software**

**Website beveiliging**

**Werkstations beheren**

**Onderhoud**

**Verwerkingsovereenkomsten**

**Backups**

**Netwerk veiligheid**

**Privacyrisico's beheren**

**Fysieke toegangscontrole**

### Onrechtmatige toegang tot persoonsgegevens

**Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?**

Discriminatie, stigmatisering, Fysieke bedreiging aan huis

**Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?**

Systemen gecompromiteerd, Afluisteren, gegevens onderschept tijdens transport, gegevens onrechtmatig gedeeld met derden

**Wat zijn de risicobronnen?**

Medewerkers betrokken instanties, Criminelen, Tegenstanders immigratie

**Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?**

Privacyrisico's beheren, Fysieke toegangscontrole, Netwerk veiligheid, Verwerkingsovereenkomsten, Website beveiliging, Werkstations beheren, Operationele beveiliging, Logische toegangscontrole, Encryptie, 18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen, 14.1.3 Transacties van toepassingen beschermen, Minimaliseren van de hoeveelheid persoonsgegevens, 13.2.1 Beleid en procedures voor informatietransport, 13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst, 11.2.9 ‘Clear desk’- en ‘clear screen’-beleid, 10.1.2 Sleutelbeheer, 14.1.2 Toepassingen op openbare netwerken beveiligen, 13.2.3 Bescherming elektronische berichten, 13.2.2 Overeenkomsten over informatietransport, 12.4.2 Beschermen van informatie in logbestanden, 11.2.8 Bescherming onbeheerde gebruikersapparatuur, 11.1.1 Gebruik fysieke beveiligingszones, 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen, 9.4.3 Systeem voor wachtwoordbeheer, 9.4.2 Beveiligde inlogprocedures, 9.4.1 Beperking toegang tot informatie, 9.2.6 Toegangsrechten intrekken of aanpassen bij beëindigen werkzaamheden, 9.2.2 Procedure voor toegang verlenen gebruikers, 9.2.1 Registratie en afmelden van gebruikers, 9.1.2 Alleen bevoegde toegang tot netwerken en netwerkdiensten, 9.1.1 Beleid voor toegangsbeveiliging, 8.3.3 Bescherming media bij fysiek overdragen, 8.3.2 Procedures voor verwijderen van media, 8.3.1 Beheer van verwijderbare media, 8.2.3 Procedures voor behandelen van bedrijfsmiddelen, 7.1.2 Beveiliging in arbeidsvoorwaarden, 7.1.1 Screening personeel, 6.2.2 Telewerkbeleid, 6.1.2 Scheiding van taken, 8.2.1 Classificatie van informatie

**Hoe schat u de ernst van het risico, rekening houdend met de potentiële effecten en geplande maatregelen?**

Verwaarloosbaar, Verwaarloosbaar gezien genomen maatregelen

**Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?**

Beperkt, Niet verwaarloosbaar gezien de diverse uitwisselingen van gegevens

### Ongewenste wijziging van persoonsgegevens

**Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?**

Ontercht een boete krijgen, in verkeerde inburgeringstraject terecht komen

**Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?**

Systemen gecompromiteerd, Gegevens gewijzigd tijdens transport, Invoerfouten

**Wat zijn de risicobronnen?**

Medewerkers betrokken instanties, Criminelen, Tegenstanders immigratie

**Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?**

Privacyrisico's beheren, Fysieke toegangscontrole, Netwerk veiligheid, Verwerkingsovereenkomsten, Website beveiliging, Werkstations beheren, Vasthouden aan schadelijke software, Operationele beveiliging, Minimaliseren van de hoeveelheid persoonsgegevens, Logische toegangscontrole, Encryptie, 18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen, 14.1.3 Transacties van toepassingen beschermen, 14.1.2 Toepassingen op openbare netwerken beveiligen, 13.2.3 Bescherming elektronische berichten, 13.2.1 Beleid en procedures voor informatietransport, 13.2.2 Overeenkomsten over informatietransport, 11.2.9 ‘Clear desk’- en ‘clear screen’-beleid, 12.4.2 Beschermen van informatie in logbestanden, 11.1.1 Gebruik fysieke beveiligingszones, 11.2.8 Bescherming onbeheerde gebruikersapparatuur, 9.4.3 Systeem voor wachtwoordbeheer, 10.1.2 Sleutelbeheer, 9.4.2 Beveiligde inlogprocedures, 9.4.1 Beperking toegang tot informatie, 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen, 9.2.6 Toegangsrechten intrekken of aanpassen bij beëindigen werkzaamheden, 9.2.2 Procedure voor toegang verlenen gebruikers, 9.2.1 Registratie en afmelden van gebruikers, 9.1.2 Alleen bevoegde toegang tot netwerken en netwerkdiensten, 9.1.1 Beleid voor toegangsbeveiliging, 8.3.3 Bescherming media bij fysiek overdragen, 8.3.2 Procedures voor verwijderen van media, 8.2.3 Procedures voor behandelen van bedrijfsmiddelen, 8.3.1 Beheer van verwijderbare media, 8.2.1 Classificatie van informatie, 7.1.1 Screening personeel, 6.2.2 Telewerkbeleid, 6.1.2 Scheiding van taken

**Hoe schat u de ernst van het risico, met name op basis van de potentiële effecten en geplande maatregelen?**

Verwaarloosbaar, Gezien de uitgebreide set aan maatregelen

**Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?**

Verwaarloosbaar, Gezien de uitgebreide set aan maatregelen

### Verdwijnen van persoonsgegevens

**Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?**

Opnieuw moeten aanleveren persoonsgegevens, vertraging in inburgeringsproces

**Wat zijn de belangrijkste dreigingen die tot het risico kunnen leiden?**

systemen gecompromiteerd, brand, ongelukken nabij locatie

**Wat zijn de risicobronnen?**

medewerkers betrokken instanties, tegenstanders migratie, criminelen

**Welke van de geïdentificeerde maatregelen dragen bij aan het mitigeren van het risico?**

Fysieke toegangscontrole, Netwerk veiligheid, Verwerkingsovereenkomsten, Onderhoud, Backups, Website beveiliging, Werkstations beheren, Vasthouden aan schadelijke software, Operationele beveiliging, Archiveren, Traceerbaarheid (logging), Logische toegangscontrole

**Hoe schat u de ernst van het risico, met name op basis van de potentiële effecten en geplande maatregelen?**

Verwaarloosbaar, Gevolgen beperken zich tot irritatie bij betrokkenen

**Hoe schat u de waarschijnlijkheid van het risico, vooral met betrekking tot dreigingen, risicobronnen en geplande maatregelen?**

Beperkt, Beperkt gezien de genomen maatregelen

