FG jaarrapport 2022

Gemeente Deurne

Inleiding

- De Functionaris Gegevensbescherming (FG) houdt zich binnen de gemeente bezig met de bescherming van persoonsgegevens van inwoners, werknemers en relaties. Dat doet hij door onder andere toezicht te houden op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

- Via dit jaarlijks rapport brengt de FG verslag uit aan het hoogste leidinggevende niveau van de gemeente, zijnde de gemeentesecretaris, het college van Burgemeester en Wethouders en de gemeenteraad.

- In dit rapport laat de FG zien wat zijn bevindingen zijn over 2022 en geeft hij aanbevelingen. Het rapport is opgesteld in januari 2023.

Bijlagen

1. Overzicht datalekken 2022
2. Overzicht DPIA's*
3. Opvallende nieuwsfeiten 2022

* *Een DPIA (Data Protection Impact Assessment) is een hulpmiddel om privacyrisico's voor de start van een gegevensverwerking uitgebreid in kaart te brengen, zodat maatregelen genomen kunnen worden om deze risico's te beperken.*

Deel 1

Terugblik op 2022

Voorbeelden van positieve ontwikkelingen in 2022:

- Diverse DPIA's zijn uitgevoerd in 2022. Zie bijlage 2.
- Sinds 1 juli 2022 is een Technisch Security Specialist in vaste dienst. Hij houdt zich bezig met het verhogen van de Cyber Security weerbaarheid en het beheren van de netwerkinfrastructuur.
- Sinds 31 oktober 2022 is een procesadviseur in dienst getreden. De procesadviseur is enerzijds verantwoordelijk voor het uitdragen van procesmatig werken in de organisatie en voor de inrichting. Anderzijds traint en faciliteert hij de proceseigenaren bij het optimaliseren van hun processen.
- Er is een protocol cybercrisis opgesteld in 2022 en intern besproken.
- De verplichte externe Wpg-audit-rapportage is op tijd ingeleverd bij de Autoriteit Persoonsgegevens.
- Het melden van datalekken en andere beveiligingsincidenten door medewerkers werd in 2022 gestimuleerd. Zo werden enkele stripalbums met kwinkslagen over informatiebeveiliging verloot onder melders. Medewerkers maakten ook regelmatig gebruik van de phishing-meldknop in Outlook.

Bevindingen en aanbevelingen van de FG

Beleid

- Het privacybeleid is vastgesteld in mei 2018. Deze dient geactualiseerd te worden. Zo ontbreekt bijvoorbeeld hierin het beleid over de gemeentelijke verwerking van politiegegevens (Wpg).

Aanbeveling 1 **Actualiseer het privacybeleid**

- Herzie het privacybeleid. Vul dat aan met het beleid met betrekking tot de gemeentelijke verwerking van politiegegevens (Wpg).

Processen

Nieuwe en gewijzigde processen met persoonsgegevens

Standaard werkwijze bij het toetsen en vastleggen van nieuwe en gewijzigde processen

- Alle plannen voor nieuwe of gewijzigde processen waarin persoonsgegevens worden verwerkt, dienen zo snel mogelijk voorgelegd te worden aan de Privacy Officer door de proceseigenaar. Zodat de Privacy Officer (kort) kan toetsen of het proces voldoet aan de privacyregels en kan adviseren of er maatregelen nodig zijn om persoonsgegevens beter te beschermen. De proceseigenaar zorgt er daarom voor dat de Privacy Officer op tijd betrokken wordt. De proceseigenaar neemt vervolgens een besluit over het wel/niet accepteren van de geadviseerde risicobeperkende maatregelen en zorgt voor de eventuele uitvoering daarvan voordat met het proces wordt gestart. De Privacy Officer zorgt dat de toetsing en het besluit vastgelegd worden en dat het proces geregistreerd wordt in het verwerkingsregister. Zo zorgt de gemeente dat het proces getoetst en geregistreerd is.
- Sinds enkele jaren bestaat er een werkwijze voor het toetsen van processen en de vastlegging van de toetsing. Proceseigenaren vragen in de prakijk vaak medewerkers om hun taken uit te voeren en dat werkt volgens de Privacy Officer prima.
- Het beeld van de FG is ook dat de Privacy Officer op tijd wordt betrokken bij nieuwe of gewijzigde processen en dat er dan getoetst wordt. De uniforme vastlegging van de toetsing kan verbeterd worden. Daarnaast worden deze processen nog niet standaard geregistreerd in het verwerkingsregister.

Bestaande processen met persoonsgegevens

- Het is voor de gemeente nog onduidelijk of privacy in alle bestaande processen voldoende is ingericht.

Aanbeveling 2 **Herzie de huidige werkwijze bij het toetsen en vastleggen van nieuwe en gewijzigde processen**

- Herzie de huidige werkwijze voor het toetsen en vastleggen van nieuwe en gewijzigde processen met persoonsgegevens zodat het toetsen en het vastleggen van de toetsing op een meer uniforme manier gebeurd. Zorg dat de processen geregistreerd worden in het verwerkingsregister.

Aanbeveling 3 **Breng de bestaande processen op orde** **Prioriteit**

- Zorg dat elk bestaand proces met persoonsgegevens aantoonbaar en op een uniforme manier getoetst wordt. Te beginnen met de processen met waarschijnlijk een hoog privacyrisico. Voer daarover DPIA's uit want pas als de hoge risico's in beeld zijn, kunnen er maatregelen worden genomen om deze risico's te verkleinen.

Organisatorische inbedding

Proceseigenaarschap

- Een proces binnen de gemeente dient belegd te zijn bij een proceseigenaar. Niet elke proceseigenaar weet echter wat van hem of haar precies verwacht wordt op het gebied van gegevensbescherming. Het in 2021 geïntroduceerde managementsysteem CyberManager kan hierbij ondersteunen. Via het systeem kunnen managers beter monitoren en bijsturen op het gebied van privacy en informatieveiligheid. In 2022 zijn de privacynormen uit het AVG-borgingsdocument van de Informatiebeveiligingsdienst (IBD) toegevoegd in het systeem. Verdere implementatie daarvan is nodig.

Bewustwording voor medewerkers

- Nieuwe medewerkers kregen in 2022 binnen 2 maanden na indiensttreding een bewustwordingstraining van de Privacy Officer/CISO over gegevensbescherming.
- In 2022 werden via de gemeentelijke leeromgeving voor medewerkers (BROS-academie) diverse e-learnings aangeboden over gegevensbescherming.
- Eind 2022 is een enquête gehouden door het bedrijf Brooklyn partners genaamd Cyber Barometer. Dit is een nulmeting voor de start van een nieuw bewustwordingsprogramma. Vanaf 2023 gaat dit programma zich richten op bepaalde doelgroepen. Aan de enquête deden 170 medewerkers mee, dat is zo'n 58% van alle medewerkers.
- Uit de enquête bleek o.a. dat enkele onderwerpen organisatiebreed meer aandacht nodig hebben, zoals het voorkomen van phishing, wachtwoordgebruik en "overweeg alvorens te handelen". Brooklyn partners neemt deze onderwerpen mee in het bewustwordingsprogramma. 19 Medewerkers hebben aangegeven ambassadeur te willen worden voor gegevensbescherming.

Opschonen gegevens

- Wat er niet is, kan ook niet gelekt worden. Na ontdekking van de hack in april 2022 moest de gemeente Buren midden in een crisis nagaan wat er precies in de systemen stond en wat dus mogelijk gelekt kon zijn. De gemeente constateerde dat veel gegevens onnodig bewaard werden op het netwerk.

Aanbeveling 4 Verbeter het proceseigenaarschap

- Zorg dat elke proceseigenaar bekend is met diens taken, verantwoordelijkheden en bevoegdheden op het gebied van gegevensbescherming. Zo kan deze binnen het proces gaan sturen op het zorgvuldig omgaan met persoonsgegevens. Trek hierin samen op met de aangetrokken procesadviseur. Ga verder met de implementatie van de privacynormen via Cybermanager.

Aanbeveling 5 Zorg voor het opschonen van onnodige gegevens

- Ga periodiek na welke gegevens noodzakelijk zijn om te bewaren op het netwerk. Zorg dat de overige gegevens worden gearchiveerd of vernietigd. Breng het periodiek opschonen onder de aandacht van medewerkers in het bewustwordingsprogramma.

Rechten van betrokkenen

Inwoners, werknemers en relaties van de gemeente (betrokkenen) hebben het recht om na te gaan wat de gemeente doet met hun persoonsgegevens. De gemeente informeert hen hierover en zorgt ervoor dat zij controle kunnen houden over deze gegevens. Bijvoorbeeld door op verzoek inzage te bieden.

- In 2022 zijn geen AVG-verzoeken ontvangen en geregistreerd in het gemeentelijk zaaksysteem.
- De privacyverklaring op de gemeentelijke website bevat nog geen informatie over de gemeentelijke verwerking van politiegegevens.
- Een interne privacyverklaring is opgesteld in 2022. Deze wordt nog voorgelegd aan de OR.

Aanbeveling 6 **Herzie de privacyverklaring op de gemeentelijke website en stel een interne privacyverklaring op**

- Herzie de privacyverklaring op de gemeentelijke website zodat informatie over de gemeentelijke verwerking van politiegegevens (Wpg) is opgenomen.
- Stel de interne privacyverklaring vast na goedkeuring van de OR. Maak het intern bekend.

Samenwerking

De gemeente werkt veel samen met derde partijen. Daarbij worden persoonsgegevens gedeeld. Het buiten de eigen deur plaatsen van taken ontslaat de gemeente niet van verantwoordelijkheid voor de gegevens. Het is belangrijk dat ook derde partijen zorgvuldig omgaan met verstrekte gegevens en dat daar afspraken over worden gemaakt. Zo is een verwerkersovereenkomst verplicht bij verstrekking van persoonsgegevens aan een verwerker.

- Een overzicht met gemaakte afspraken ontbreekt. Onduidelijk is of afspraken nog actueel zijn, of er afspraken ontbreken en of ze worden nageleefd.
- Door beperkte capaciteit en het ontbreken van centrale regie op contractbeheer bij de gemeente is het beheer voornamelijk reactief. Er is met name aandacht voor het maken van privacy-afspraken met derde partijen bij nieuwe of gewijzigde processen met persoonsgegevens.

Aanbeveling 7 **Breng afspraken met derde partijen op orde**

- Zorg voor een actueel totaaloverzicht van afspraken met derde partijen. Maak afspraken met derde partijen als deze ontbreken. Actualiseer bestaande afspraken met derde partijen indien nodig. Controleer periodiek of de afspraken op papier in de praktijk worden nagekomen. Laat de derde partij periodiek verantwoording afleggen over informatiebeveiliging en privacy.

Beveiliging

Passende technische en organisatorische maatregelen zijn nodig om (persoons)gegevens te beveiligen. Daarmee worden datalekken voorkomen en de impact van een cyberaanval verkleind.

	Maatregel	Beeld van de CISO (Chief Information Security Officer) eind 2022
	Hard- en software up-to-date houden	✓ Dat heeft de aandacht van systeem- en functioneel beheerders. Veel extern bereikbare software binnen de gemeente is uitbesteed. Leveranciers houden deze software goed bij.
	Meerfactor-authenticatie	✓ Gebruik van meerfactorauthenticatie is ingevoerd voor alle toegang buiten het eigen netwerk.
	Netwerk-segmentatie	Het netwerk is logisch in “kamers” verdeeld maar alle “deuren” daartussen staan nog open. Een aanvaller kan eenmaal binnen overal rondlopen. Sinds 1 juli 2022 is een Technisch Security Specialist in vaste dienst. Deze houdt zich bezig met het verhogen van de Cyber Security weerbaarheid en het beheren van de netwerk-infrastructuur.
	Robuuste back-ups	Back-up voorzieningen zijn waarschijnlijk in orde maar overzicht, controle en beleid hierover ontbreken. Verbeteren van back-up beleid staat ingepland voor 2023.
	Oefenen ICT-crisisplan	De gemeente heeft een protocol cybercrisis opgesteld in 2022 en intern besproken. Er is nog niet mee geoefend. Gepland is om mee te doen aan de landelijke cybercrisisoefening in oktober 2023. In 2023 verwacht de gemeente een bedrijfscontinuïteitsplan (BCP) gereed te hebben.
	Monitoring, Detection & Response	Het detecteren en signaleren van verboden en ongewenste acties en gedrag op de ICT-infrastructuur is onvoldoende. Zowel van buiten het gemeentelijk netwerk als van binnenuit. Zo kan een aanvaller langere tijd ongemerkt binnen zijn. In 2023 wordt deze dienst uitbesteed aan een leverancier en geïmplementeerd. Daarvoor is geld gereserveerd.
	Logging	Een loggingbeleid en uitvoering daarvan ontbreekt. Loggegevens worden zelden gecontroleerd.

Aanbeveling 8 **Verklein de impact van een cyberaanval** — Prioriteit

- Bereid een cyberaanval voor want 100% veilig bestaat niet. Zorg voor overzicht en controle over back-ups. Houd een crisisoefening. Zorg voor een loggingbeleid en uitvoering daarvan. Implementeer Monitoring, Detection & Response in 2023.

Verantwoording

- Op dit moment kan de gemeente onvoldoende aantoonbaar maken dat zij voldoet aan haar AVG-verplichtingen (verantwoordingsplicht). Zo wordt het verwerkingsregister onvoldoende onderhouden waardoor het register onbetrouwbaar is.

Prioriteit

Aanbeveling 9 **Actualiseer het verwerkingsregister**

- Inventariseer welke processen met persoonsgegevens in huis zijn. Ga vervolgens aan de slag met het actualiseren en volledig maken van het verwerkingsregister. Borg het beheer ervan. Zorg dat nieuwe en gewijzigde verwerkingen na aantoonbare toetsing opgenomen worden in het register. Zorg voor een overzicht van verwerkingen met een hoog privacyrisico in het verwerkingsregister.

Wet Politiegegevens (Wpg)

De gemeente is werkgever van buitengewoon opsporingsambtenaren (BOA's) in het domein Onderwijs. Deze verwerken politiegegevens bij de uitvoering van hun opsporingstaak. De gemeente moet daarom rekening houden met de verplichtingen uit de Wet Politiegegevens (Wpg).

- Eén van de Wpg-verplichtingen is een externe audit laten uitvoeren om de 4 jaar. De gemeente heeft dat in 2022 gedaan en het Wpg-auditrapport is ingeleverd bij de toezichthouder, de Autoriteit Persoonsgegevens.
- Jaarlijks dient ook een interne Wpg-audit uitgevoerd te worden.
- Uit de externe Wpg-audit bleek dat de Wpg nog verder geïmplementeerd dient te worden.

Prioriteit

Aanbeveling 10 **Implementeer de Wet Politiegegevens (Wpg)**

- Voer een verbeterplan uit voor de Wpg-implementatie in 2023. Zorg daarna dat er in 2023 een hercontrole plaatsvindt. Stuur de rapportage hiervan naar de Autoriteit Persoonsgegevens. Voer de interne Wpg-audit uit.

Vooruitkijken naar 2023

- Er is meer zicht en grip nodig op de processen waarin persoonsgegevens en politiegegevens worden verwerkt. Niet alleen vanuit privacy-oogpunt maar ook om als organisatie intern beter te gaan werken en om weerbaarder te worden voor cyberaanvallen. Als de processen op orde zijn dan kan de gemeente ook beter samenwerken, transparant en betrouwbaar zijn.

- De FG heeft 10 aanbevelingen gedaan in deel 1. Het is realistisch dat niet alles in 2023 opgepakt kan worden. Voor 2023 ziet de FG 4 prioriteiten.

Prioriteiten 2023

1. Breng de bestaande processen op orde

Zorg dat elk bestaand proces met persoonsgegevens aantoonbaar en op een uniforme manier getoetst wordt. Te beginnen met de processen met waarschijnlijk een hoog privacyrisico. Voer daarover DPIA's uit want pas als de hoge risico's in beeld zijn, kunnen er maatregelen worden genomen om deze risico's te verkleinen.

2. Verklein de impact van een cyberaanval

Bereid een cyberaanval voor want 100% veilig bestaat niet. Zorg voor overzicht en controle over back-ups. Houd een crisisoefening. Zorg voor een loggingbeleid en uitvoering daarvan. Implementeer Monitoring, Detection & Response in 2023.

3. Actualiseer het verwerkingsregister

Inventariseer welke processen met persoonsgegevens in huis zijn. Ga vervolgens aan de slag met het actualiseren en volledig maken van het verwerkingsregister. Borg het beheer ervan. Zorg dat nieuwe en gewijzigde verwerkingen na aantoonbare toetsing opgenomen worden in het register. Zorg voor een overzicht van verwerkingen met een hoog privacyrisico in het verwerkingsregister.

4. Implementeer de Wet Politiegegevens (Wpg)

Voer een verbeterplan uit voor de Wpg-implementatie in 2023. Zorg daarna dat er in 2023 een hercontrole plaatsvindt. Stuur de rapportage hiervan naar de Autoriteit Persoonsgegevens. Voer de interne Wpg-audit uit.

Bijlage 1 Overzicht datalekken 2022

	Datalek
1	Twee cliëntbrieven zijn in 1 envelop gedaan en verzonden.
2	Een mail met een WMO onderzoeksverslag is verzonden naar een verkeerde cliënt.
3	Een mail over een promotiebladtekst is verzonden naar een verkeerde ontvanger.
4	Onbevoegde medewerkers hadden toegangsrechten tot persoonsgegevens over agressie-incidenten.
5	Een mail met bijlage is verzonden naar een verkeerde ontvanger.
6	Een mail is verzonden naar een verkeerde collega.
7	Twee uittreksels BRP zijn verwisseld en per post verstuurd.
8	Een mail met als bijlage een brief over een betalingsregeling voor huur is verzonden naar een verkeerde ontvanger.
9	Publiekszaken stuurde onnodig via mail persoonsgegevens naar de VNG (Vereniging Nederlandse Gemeenten).
10	Twee cliëntbrieven zijn in 1 envelop gedaan en verzonden.
11	Een verzendlijst werd per ongeluk als bijlage verzonden in een mail naar genodigden voor het Participatiecafé Deurne.
12	Een publicatie van een ingestuurde inwonersbrief was onvoldoende geanonimiseerd.

Datalekken	2018	2019	2020	2021	2022
Gemeld aan de gemeente	8	10	15	13	12
Gemeld aan de Autoriteit Persoonsgegevens	3	5	4	4	4

Bijlage 2 Overzicht DPIA's

Onderwerp DPIA	Status eind 2022
Wvggz (Wet verplichte geestelijke gezondheidszorg)	DPIA uit 2019. **Aanbeveling: evalueren/herzien in 2023**
Zorg- en veiligheidshuis (ZVH)	DPIA uit 2019. **Aanbeveling: evalueren/herzien in 2023**
Cameratoezicht Parkeergarage Wolfsberg	DPIA uit 2020. Afgerond in 2020. **Aanbeveling: evalueren/herzien in 2023**
Cameratoezicht gemeentehuis	DPIA uit 2021. Afgerond in 2021.
Jongeren in kwetsbare posities (JIKP)	DPIA uit 2021. Afgerond in 2021.
Agressieprotocol	DPIA uit 2021. Afgerond in 2022.
GPS tracker op voertuigen buitendienst	DPIA uit 2021. Afgerond in 2022.
Nieuwe Wet inburgering	DPIA uit 2022. Afgerond in 2022.
Beschermd Wonen / Beschermd Thuis	DPIA uit 2022. Afgerond in 2022. Uitgevoerd door de Gemeenschappelijke Regeling Peelgemeenten.
Grip op Schuld	DPIA uit 2022. Is in behandeling
Jeugdhulpverlening	DPIA uit 2022. Is in behandeling.
Financieel systeem ERPx	DPIA uit 2022. Is in behandeling.
Powerbrowser	DPIA uit 2022. Is in behandeling.
Leerplicht	DPIA wordt nog gestart.
Bibob verwerkingen	DPIA wordt nog gestart.
Nieuw zaaksysteem	DPIA wordt nog gestart.

Bijlage 3 Opvallende nieuwsfeiten 2022

	Nieuwsfeiten
1 april 2022 **Gemeente Buren**	Gemeente Buren (27.000 inwoners) werd gehackt, 5 terabytes (30 miljoen bestanden) aan (persoons)gegevens werden gestolen. Waaronder kopieën van 1.331 geldige identiteitsbewijzen. Deze identiteitsbewijzen moesten allemaal vervangen worden na de hack. De aanvallers waren maandenlang ongemerkt binnen geweest. Een les uit deze aanval: zorg voor vroegtijdige detectie.
12 april 2022 **Boete Belastingdienst**	De belastingdienst kreeg een **boete** van **3,7 miljoen euro** voor een zwarte lijst FSV (Fraude Signalering Voorziening). Dat is de hoogste boete ooit opgelegd door de Autoriteit Persoonsgegevens dat tot nu toe openbaar is gemaakt.
25 mei 2022 **Onderzoek Bits of Freedom**	Onderzoek Bits of Freedom naar de staat van privacy bij de top 10 gemeenten. Conclusie: • "Gemeenten hebben de basis nog niet goed op orde" • "Bij vrijwel alle gemeenten is er sprake van een capaciteitsprobleem, doordat er onvoldoende middelen worden vrijgemaakt voor gegevensbescherming."
18 juli 2022 **Gemeente Eindhoven**	De Autoriteit Persoonsgegevens maakt zich zorgen over de privacycultuur binnen de gemeente Eindhoven.
27 juli 2022 **Gemeenten Eijsden-Margraten, Gulpen-Wittem, Kerkrade, Meerssen en Vaals**	De softwareleverancier van de vijf Zuid-Limburgse gemeenten werd getroffen door een cyberaanval. Daarbij werd de administratie van het sociaal domein vergrendeld. Hierdoor waren gegevens over onder meer bijstandsuitkeringen, jeugdzorg, de WMO en energietoeslagen niet meer toegankelijk.
10 september 2022 **Gemeente Hof van Twente**	Bericht van de woordvoerder van gemeente Hof van Twente (35.000 inwoners) over de kosten van de hack eind 2020: "De kosten zijn uitgekomen op **4,2 miljoen euro**. Daarnaast zijn onze structurele ict-uitgaven verhoogd."
20 oktober 2022 **IBD Dreigingsbeeld 2023/2024**	De Informatiebeveiligingsdienst (IBD) constateert in haar Dreigingsbeeld informatiebeveiliging 2023/2024 o.a.: groeiende dreiging van ransomware-aanvallen en gemeenten hebben onvoldoende aandacht voor informatiebeveiliging en privacy bij samenwerking met derde partijen.
November 2022 **NIS2-richtlijn is door het Europees Parlement en de Raad van de EU aangenomen** NIS2 wordt in Nederland ook wel NIB2 genoemd (netwerk- en informatiebeveiliging 2 richtlijn**)**	De NIS2-richtlijn (Network and Information Security 2 directive) is door het Europees Parlement en de Raad van de EU aangenomen. Nu moet de richtlijn nog worden omgezet in nationaal recht. De nieuwe wet moet zorgen voor een betere weerbaarheid tegen cybercriminaliteit in Europa. Ingang wordt verwacht in 2024. NIS2 leidt er o.a. toe dat ook decentrale overheden zoals gemeenten aan de Europese verplichtingen op het gebied van cybersecurity moeten voldoen. Zo zullen organisaties meer maatregelen moeten nemen om hun ICT te beveiligen tegen incidenten. En informatie delen over dreigingen wat het mogelijk maakt om betere bescherming en detectie te kunnen bieden, maar ook om sneller te kunnen handelen tijdens een incident. In de NIS2 staat dat de nationale autoriteiten strenger moeten handhaven op het naleven van deze regels. Er zal sprake zijn van een proactief beleid waarbij controles steekproefsgewijs worden uitgevoerd. Mogelijke boetes en een bestuurder kan verantwoordelijk worden gesteld met een mogelijke schorsing als gevolg.
1 december 2022 **Aangepaste Wbni is van kracht**	De aangepaste Wet beveiliging netwerk- en informatiesystemen (Wbni) is nu van kracht, waardoor o.a. het Nationaal Cyber Security Centrum (NCSC) dreigings- en incidentinformatie ook mag delen met organisaties die niet tot de vitale organisaties of de Rijksoverheid behoren, zoals gemeenten.

Bijlage 3 Opvallende nieuwsfeiten 2022

	Nieuwsfeiten
21 december 2022 **Algoritmeregister**	Staatssecretaris Alexandra van Huffelen (Digitalisering) heeft het Algoritmeregister gelanceerd. De nieuwe site moet zorgen voor **meer transparantie over de algoritmes die overheden inzetten**, omdat dit nu nog vaak tekort schiet. Een algoritme is een stappenplan dat een computersysteem uitvoert. Met algoritmes wordt onder andere bepaald of iemand recht heeft op bepaalde toeslagen. Ze worden gebruikt om processen sneller te laten verlopen. Verkeerde inzet van algoritmes kan leiden tot discriminatie. Een voorbeeld daarvan is de toeslagenaffaire, waarbij mensen met een laag inkomen door een algoritme automatisch in het vizier van de Belastingdienst kwamen voor een fraudecontrole. Ministeries, **gemeenten** en andere takken van de overheid kunnen hun algoritmes delen op het Algoritmeregister, maar dat is nog niet verplicht. De Tweede Kamer wil wel dat dit gebeurt. Van Huffelen wil hier werk van maken en verwacht dat zo'n verplichting op zijn vroegst in 2024 van kracht wordt.