DATUM: 25 MEI 2022

De staat van privacy bij gemeenten

Een onderzoek naar de naleving van de Algemene verordening gegevensbescherming onder de tien grootste gemeenten van Nederland.

Door Nadia Benaissa.

SAMENVATTING

De gemeenten hebben, vier jaar nadat de privacywetgeving werd herzien, hun gegevensbescherming nog altijd niet op orde. Dat blijkt uit onderzoek van digitale burgerrechtenbeweging Bits of Freedom.

We onderzochten hoe goed de tien grootste gemeenten van Nederland de Algemene verordening gegevensbescherming (AVG) naleven. In dit rapport beschrijven we onze bevindingen. We keken vooral naar onderwerpen die de meeste impact hebben op burgers en de maatschappij. Hebben gemeenten het overzicht van de gegevens die zij verwerken? Hoe gaan zij om met het recht op inzage van burgers? Is de naleving van deze wet voldoende geprioriteerd? Hoe is de interne toezichthouder, de Functionaris Gegevensbescherming, gepositioneerd? En legt de gemeente wel verantwoording aan de gemeenteraad af? Ook hebben we gekeken naar de mate waarin Rekenkamers onderzoek hebben gedaan naar de opvolging van de AVG.

Voor ons onderzoek vroegen we de gemeenten om alle relevante documenten openbaar te maken. Daarvoor beriepen we ons op de Wet openbaarheid van bestuur (Wob). Ook analyseerden we de informatie op de websites van de gemeenten, de gemeenteraden en de Rekenkamers. Dit zijn de belangrijkste bevindingen:

- Gemeenten hebben de basis gegevenshuishouding nog niet goed op orde. Verwerkingsregisters zijn niet compleet en actueel, waardoor ge-

meenten niet voldoende weten welke gegevens ze verwerken, met welk doel, of dat rechtmatig en veilig is en met wie er wordt samengewerkt.

- Gemeenten tonen zich tegelijkertijd wel ambitieus en blijken datagedreven te willen werken en nieuwe technologieën te willen uitproberen. Dat is onverstandig als de basis nog niet op orde is, omdat de gegevens waarvan de rechtmatigheid, betrouwbaarheid en actualiteit nog niet gecontroleerd zijn, vervolgens gebruikt worden als input bij het gebruik van bijvoorbeeld big data of algoritmen.
- Burgers die hun AVG-rechten inzetten, bijvoorbeeld door inzage te verzoeken, moeten vaak te lang wachten. Processen zijn niet overal op orde en wettelijke termijnen worden zonder legitieme reden verlengd en overschreden.
- Bij vrijwel alle gemeenten is er sprake van een capaciteitsprobleem, doordat er onvoldoende middelen worden vrijgemaakt voor gegevensbescherming. Dit wekt de indruk dat verantwoordelijke bestuurders en directies dit onvoldoende prioriteren.
- Op grond van artikel 60 van de Gemeentewet moeten burgemeesters en wethouders verantwoording afleggen aan de gemeenteraad over het gevoerde bestuur. De meerderheid van de gemeenten legt echter niet actief verantwoording af aan de gemeenteraad door de AVG-rapportages van de Functionaris Gegevensbescherming met hen te delen.

INHOUDSOPGAVE

INLEIDING

Vier jaar geleden, op 25 mei 2018, trad de nieuwe Europese privacywet, de Algemene verordening gegevensbescherming (AVG) in werking. Deze wet verving de Wet bescherming persoonsgegevens. Er kwamen meer regels voor organisaties om zichzelf te verantwoorden over de manier waarop ze omgaan met persoonsgegevens. Ook moest de privacywet meer zeggenschap en controlemogelijkheden geven aan betrokkenen, bijvoorbeeld door middel van inzageverzoeken. De wet voorziet in een Functionaris Gegevensbescherming die toeziet op de naleving van de AVG. Als organisaties niet goed met persoonsgegevens omgaan, kan deze toezichthouder de verantwoordelijken terecht roepen en adviseren. Ook is er een externe toezichthouder, de Autoriteit Persoonsgegevens, die kan handhaven, desnoods met miljoenenboetes.

We vroegen ons af hoe goed de wet in de praktijk werkt. We besloten onderzoek te doen onder gemeenten. Dat zijn immers bij uitstek dé organisaties die veel verschillende en heel gevoelige persoonsgegevens verwerken van burgers, vaak zonder dat burgers daar een keuze in hebben. Gemeenten mogen en moeten persoonsgegevens immers vaak verwerken op grond van een wettelijke taak of plicht.

We kozen voor de tien grootste gemeenten van Nederland: de gemeenten Amsterdam, Rotterdam, Den Haag, Utrecht, Eindhoven, Groningen, Tilburg, Almere, Breda en Nijmegen. Ten eerste omdat deze tien gemeenten bij elkaar opgeteld de gegevens verwerken van zo'n 3,8 miljoen mensen. Ten tweede besteden kleine gemeenten regelmatig werkzaamheden uit aan grote gemeenten, en is de stand van zaken bij de grote gemeenten ook relevant voor de kleinere gemeenten. Ten derde vervullen grote gemeenten een voorbeeldfunctie voor kleinere gemeenten. We hebben bij de tien grootste gemeenten een Wob-verzoek ingediend met de vraag ons alle rapportages van de Functionarissen Gegevensbescherming op te sturen vanaf 2017 tot op heden, samen met alle rapportages over de informatiebeveiliging. Ook hebben we gevraagd de interne reacties daarop met ons te delen.

Als de rapportages goed zijn geschreven, geven ze een helder beeld over waar gemeenten staan, wat er goed gaat en waar nog uitdagingen liggen. Ook zou je in de rapportages willen teruglezen of en hoe eerdere adviezen zijn opgevolgd en of gemeenten een stijgende lijn laten zien in het voldoen aan de privacywetgeving. Dat is voor de organisatie belangrijk om te weten, maar ook voor de mensen om wie het gaat. Daarom zou het uitgangspunt moeten zijn dat deze informatie openbaar gemaakt wordt. We zijn hierbij niet op zoek gegaan naar kwetsbaarheden binnen de organisaties. We wilden niet weten welke beveiligingslekken zich zouden kunnen voordoen en waar de grootste kans op datalekken bestaat. Dat is weliswaar

belangrijke informatie, maar het openbaar maken hiervan brengt risico's voor de gemeenten, en vooral voor de burgers met zich mee.

We hebben (uiteindelijk) van alle gemeenten de stukken mogen ontvangen. De gemeente Almere heeft echter een groot deel van de stukken zwart gelakt. De gemeente Tilburg bleek geen AVG-rapportages te hebben. Door verschillende omstandigheden was het hen niet gelukt om te rapporteren. Wel was ten tijde van het schrijven van dit rapport de rapportage over het jaar 2020 in voorbereiding, maar nog niet af. Dit wordt ons alsnog nagestuurd wanneer het gereed is.

Toen de Europese privacywet in werking trad gingen veel organisaties aan de slag met het tienstappenplan van de Autoriteit Persoonsgegevens. Deze stappen waren gericht op: bewustwording, rechten van betrokkenen, overzicht verwerkingen, Data Protection Impact Assessments, privacy by design en privacy by default, Functionaris Gegevensbescherming, meldplicht datalekken, verwerkersovereenkomsten, leidende toezichthouder en tot slot toestemming.[1]

Op basis van deze stappen rapporteerden veel interne toezichthouders van de door ons onderzochte gemeenten over wat zij binnen de gemeenten zagen. De rapportages zijn steeds verder uit elkaar gaan liggen, waarschijnlijk door een ontbrekend format. Daarnaast constateren we dat er veel verschil is in stijl, diepgang en woordkeuze. Zo nemen sommige toezichthouders de vrijheid alarmerend te waarschuwen als de situatie daar om vraagt, waar andere toezichthouders hun woorden heel voorzichtig lijken te kiezen.

In dit rapport richten we ons op onderwerpen die voor burgers en de maatschappij het meest relevant zijn. In hoofdstuk 1 gaan we in op de vraag in hoeverre gemeenten de basis gegevenshuishouding op orde hebben. Weten ze welke gegevens ze verwerken, met welk doel en is de verwerking rechtmatig? Hoofdstuk 2 gaat over de rechten van betrokkenen. Kunnen burgers bij gemeenten terecht met bijvoorbeeld inzageverzoeken en hoe worden deze verzoeken door gemeenten opgepakt? Het derde hoofdstuk richt zich op de positionering van de Functionaris Gegevensbescherming die vanuit een onafhankelijke rol diens werk moet kunnen doen. Ook hebben we in dit hoofdstuk gekeken naar de capaciteit die gemeenten beschikbaar stellen om aan de AVG te voldoen. In het vierde hoofdstuk gaan we in op de mate waarin gemeenten transparantie bieden op hun website, en of ze zich verantwoorden naar de gemeenteraad. Daarnaast hebben we gekeken naar de mate waarin Rekenkamers onderzoek hebben gedaan naar de bescherming van persoonsgegevens. Tot slot doen we aanbevelingen om tot een hoger beschermingsniveau van persoonsgegevens te komen.

1. HEBBEN GEMEENTEN DE BASIS OP ORDE?

Met de komst van de AVG werden gemeenten verplicht overzicht te krijgen in de persoonsgegevens die ze verwerken en dit overzicht vast te leggen in een verwerkingsregister. Welke persoonsgegevens zijn dat? Waarom worden die verwerkt? Hoe lang mogen die gegevens bewaard worden? En hoe worden ze beveiligd? Dat zijn vragen die beantwoord moeten worden in het verwerkingsregister.[2]

Het doel van zo'n verwerkingsregister is om meer grip te krijgen op de verwerkingen van persoonsgegevens. Door dat overzicht is het makkelijker om te controleren of er op de juiste manier met persoonsgegevens wordt omgegaan en of de verwerkingen rechtmatig zijn. Ook kunnen gemeenten mogelijke risico's voor betrokkenen of de organisatie eenvoudiger opsporen. Wanneer gemeenten datagedreven willen werken en gebruik willen maken van nieuwe technologieën, is het enorm van belang dat de gegevens actueel en betrouwbaar zijn, maar ook dat je ze überhaupt (nog) mag verwerken. Gemeenten noemen dit ook wel 'de basis op orde'.

HOE DOEN GEMEENTEN HET OP DIT VLAK?

Uit de documenten blijkt dat alle gemeenten van start zijn gegaan met het vullen van een verwerkingsregister. De gemeente Utrecht publiceerde al in 2018 haar verwerkingsregister online.[3] [4] Met een projectteam werd er tussen 2016 en 2018 gewerkt aan het voldoen aan de AVG die in 2018 in werking zou treden. Daarmee was de gemeente Utrecht de uitzondering. Hoewel meerdere gemeenten stappen hadden gezet om overzicht te krijgen in de gegevenshuishouding, kregen veel gemeenten het niet voor elkaar om hier voldoende voortgang in te krijgen. Zo bleef de gemeente Eindhoven in 2021 nog steeds achter in het volledig krijgen van het verwerkingsregister en was vijftien procent van de verwerkingen hier nog niet compleet in opgenomen.[5] In de gemeente Almere bleken afdelingen niet bekend te zijn met de inspanningen die ze moeten leveren om het register actueel te houden.[6] In de gemeente Breda werd in 2018 geadviseerd 'de basis op orde' als hoofdprioriteit te nemen[7], maar dat advies werd herhaald in 2019, 2020 en 2021. Ook de Functionaris Gegevensbescherming van de gemeente Rotterdam gaf in 2018 aan dat nog niet alle verwerkingen in beeld zijn.[8] In 2019 werd opnieuw aangegeven dat de kwaliteit van het register onvoldoende is.[9] De concerndirectie besloot dat dit prioriteit moest krijgen en in de rapportage die daarop volgt later in 2019[10] is een voortgang te zien en in 2020[11] is het verwerkingsregister af. De gemeente Amsterdam werd in 2020 door de Functionaris Gegevensbescherming opgeroepen het verwerkingsregister te actualiseren.[12] Ook werd er in datzelfde jaar op gewezen

dat er nog onvoldoende zicht is op de beveiliging van apparatuur en informatie.[13] Of en hoe dat is opgevolgd, blijkt niet uit de ontvangen stukken. In de gemeente Den Haag zou het verwerkingsregister in 2020 afgerond worden, volgens het Jaarplan privacy 2020.[14] In de rapportage van 2018 geeft de Functionaris Gegevensbescherming van de gemeente Groningen aan dat de kwaliteit van het verwerkingsregister omhoog moet. Of en hoe dit is opgevolgd, blijkt niet uit de ontvangen stukken.[15]

WAAROM MOET DIT BETER?

Dat gemeenten moeite hebben met het volbrengen van deze taak, is niet heel vreemd. Gemeenten verwerken een enorme hoeveelheid persoonsgegevens en hebben heel veel processen, verspreid over verschillende afdelingen, gekoppeld aan verschillende taken en wettelijke bevoegdheden. Het is dan ook een uitdaging om daar overzicht in te krijgen, zeker als gemeenten daar voor de inwerkingtreding van de AVG nog weinig aandacht voor hadden. Toch lukt het sommige gemeenten eerder dan anderen om er voortgang in te krijgen en uiteindelijk de klus te klaren. Dat lijkt volgens de rapportages te liggen aan prioritering door de verantwoordelijke directies en het wel of niet vrijmaken van capaciteit.

Het gebrek aan overzicht, ofwel het niet op orde hebben van de basis gegevenshuishouding, brengt risico's met zich mee. Als verwerkingsprocessen niet in beeld zijn, kan ook niet getoetst worden of de verwerking rechtmatig is en rechten van betrokkenen voldoende beschermd worden. Er kan niet gecontroleerd worden of de gegevens voldoende beveiligd worden.

Maar ook is het moeilijk te controleren of de gegevens nog wel kloppen en nog bewaard mogen worden. Denk daarbij bijvoorbeeld aan de Belastingdienst die gegevens had over de dubbele nationaliteit van mensen. Die gegevens moesten in 2014 al verwijderd worden[16], maar dat werd niet gedaan, waarna de Belastingdienst deze gegevens gebruikte om etnisch te profileren.[17] Het onrechtmatig hebben van persoonsgegevens opent deuren naar verdere onrechtmatige praktijken met die gegevens.

Bij de inzet van nieuwe technologiën en datatoepassingen, waaronder big data, algoritmen, machine learning en kunstmatige intelligentie, is het van cruciaal belang dat de gegevens die daarvoor gebruikt worden, kloppen en rechtmatig zijn. De uitkomsten kunnen immers behoorlijke impact hebben op het leven van mensen. Toch lijkt dat besef nog niet volledig doorgedrongen bij gemeenten. Hoewel ze de basis nog lang niet altijd op orde hebben, weerhoudt dat ze er niet van met spannende technologieën en datatoepassingen aan de slag te gaan. Maar als gemeenten hun datahuishouding niet op orde hebben, maar wel datagedreven gaan werken, ondersteund door technologieën, willen gemeenten gaan rennen nog voordat ze kunnen lopen.

Zoals helder verwoord in een rapportage van de gemeente Den Haag:

> ***"In maart heeft de gemeente Den Haag de ambitie verwoord om het zogenaamde tien stappenplan van de Autoriteit Persoonsgegevens te implementeren om de Algemene verordening gegevensbescherming uit te voeren. Nu, twee jaar later, stel ik als Functionaris Gegevensbescherming vast dat de gemeente deze tien stappen nog niet volledig heeft doorlopen. (...) Inmiddels zijn de ambities van de Gemeente Den Haag op bijvoorbeeld het gebied van datagedreven werken en smart cities alleen maar gegroeid en profileert Den Haag zich als de stad van vrede en recht én veiligheid."*** [18]

En daarmee is de gemeente Den Haag geen uitzondering. Zo blijkt uit onderzoek van de NOS dat zeker 25 gemeenten gebruik maken van voorspellende systemen en algoritmen om bijvoorbeeld bijstandsfraude op te sporen, of burgers met schulden te kunnen helpen.[19]

AANBEVELINGEN

- Prioriteer het vullen en actueel houden van het verwerkingsregister. Zie dit niet als een eenmalige klus, maar als een doorlopend proces waarbij kritisch gekeken wordt naar welke verwerkingen nog noodzakelijk en rechtmatig zijn, en welke verwerkingen gestopt kunnen worden.
- Publiceer het verwerkingsregister op de website. Dit is welliswaar geen

verplichting vanuit de AVG, maar het biedt wel transparantie.

- Verwerk geen gegevens op een manier die niet te verantwoorden is, bijvoorbeeld door algoritmen geautomatiseerde beslissingen te laten maken die niet transparant en motiveerbaar zijn. Houd ten alle tijden de algemene beginselen van behoorlijk bestuur voor ogen.
- Zorg ervoor dat in beeld wordt gebracht met welke partijen samenwerkingen zijn aangegaan en vanuit welke hoedanigheid en bevoegdheid. Is er sprake van (gedeelde) verwerkingsverantwoordelijkheid of van een verwerker? Documenteer de daarbij behorende overeenkomsten centraal.
- Begin niet aan ‘datagedreven werken’ met behulp van nieuwe technologieën en datatoepassingen zoals big data en algoritmen als de basis niet op orde is.

2. HOE GAAN GEMEENTEN OM MET AVG-VERZOEKEN?

Burgers hebben recht op transparantie, inzage, rectificatie en gegevenswissing.[20] Gemeenten zijn verplicht binnen een maand na ontvangst van een verzoek de informatie te verstrekken waar om gevraagd wordt. Deze termijn mag met twee maanden verlengd worden afhankelijk van de complexiteit van de verzoeken en het aantal verzoeken.[21] [22]

Een doel van deze rechten is om mensen meer controle te geven over hun persoonsgegevens. Zo kunnen mensen te weten komen welke gegevens van hen verwerkt worden en of die gegevens wel kloppen. Ook worden organisaties gedwongen verantwoording af te leggen en openheid te geven over de wijze waarop ze met persoonsgegevens omgaan.

Gemeenten kunnen verspreid over verschillende afdelingen allerlei persoonsgegevens verwerken. Om dat allemaal naar boven te halen is het meestal nodig om die verschillende afdelingen te benaderen met de vraag of er gegevens over een persoon beschikbaar zijn. Om dat in goede banen te leiden is er een goed proces nodig waarbij de verantwoordelijkheden belegd zijn.

HOE DOEN GEMEENTEN HET OP DIT VLAK?

De gemeente Nijmegen is tijdig begonnen met het ontwikkelen van een

proces en bleek in staat de verzoeken af te handelen.[23] [24] In de gemeente Amsterdam zijn er in 2020 120 verzoeken in behandeling genomen en in 2019 130 verzoeken.[25] In de rapportage wordt echter niets vermeld over de kwaliteit of tijdigheid van de behandeling. In de gemeente Groningen geeft de Functionaris Gegevensbescherming aan dat de rechten van betrokkenen "redelijk geborgd" zijn.[26] In de gemeente Utrecht was er weliswaar een proces, maar bleek er onvoldoende capaciteit om de verzoeken tijdig te behandelen. Dat werd opgelost door het bij een andere afdeling onder te brengen.[27]

In de gemeente Breda schreef de Functionaris Gegevensbescherming een stuk waarin wordt ingegaan op de juridische invulling van het recht op inzage. Ook werden er praktische adviezen gegeven voor een goede behandeling van de verzoeken.[28] In de rapportage van 2019 wordt aangegeven dat uit een evaluatie van de behandeling van de verzoeken bleek dat dit "uiterst moeizaam" verliep. Termijnen werden overschreden, de communicatie met betrokkenen verliep moeizaam en het ontbrak aan een proces, technische ondersteuning en sturing. De gemeentesecretaris heeft vervolgens opdracht gegeven een proces te ontwikkelen en te zorgen voor technische ondersteuning, dat uiterlijk eind 2019 afgerond moest worden.[29] In de jaarrapportage van 2020 wordt aangegeven dat er beperkte voortgang is geboekt op de verbeterpunten die in het voorgaande jaar geadviseerd waren.[30] In de jaarrapportage van 2021 is wederom weinig vooruitgang zichtbaar.[31] Ook in Rotterdam vond er een evaluatie plaats waaruit bleek dat het proces herzien moest worden en de uitvoering elders belegd moest worden.[32] In een volgende rapportage in 2019 wordt wederom geadviseerd beter om te gaan met de verzoeken van burgers, omdat de Functionaris Gegevensbescherming nog onvoldoende verbetering ziet in de afwikkeling. In bijna de helft van de aanvragen wordt de behandeltermijn overschreden.[33] Eind 2019 is er wel een verbetering zichtbaar, maar wordt nog altijd 30% van de aanvragen te laat afgehandeld.[34] In 2020 wordt gerapporteerd dat het proces van de rechten van betrokkenen is verbeterd en van de 153 verzoeken, 77% tijdig werd afgehandeld, waar dit in 2019 nog maar 45% was.[35]

De Functionaris Gegevensbescherming benadrukt in de rapportage van 2020 hoe belangrijk het is aan de verplichtingen van de AVG te voldoen:

> **"Vertrouwen van de burger in de overheid is essentieel, aangezien burgers voor veel processen wettelijk verplicht zijn hun persoonsgegevens ter beschikking te stellen. Door de toeslagenaffaire is nog eens pijnlijk duidelijk geworden wat er mis kan gaan. De AVG reikt praktische handvatten aan voor verantwoord omgaan met data. De overheid moet open zijn en zich kunnen verantwoorden aan de burger."**

WAAROM MOET DIT BETER?

Burgers bevinden zich ten opzichte van gemeenten in een afhankelijke en onevenwichtige machtsrelatie. De rechten van betrokkenen uit de AVG vormen een belangrijk middel om die disbalans meer in evenwicht te brengen. Gemeenten zouden er dan ook een prioriteit van moeten maken ervoor te zorgen dat ze de processen en de uitvoering goed op orde hebben, zodat ze naar behoren kunnen voldoen aan de verzoeken van burgers.

AANBEVELINGEN

- Zorg voor een goed proces voor AVG-verzoeken van burgers, waarbij de verantwoordelijkheden goed belegd zijn.
- Evalueer het proces voor AVG-verzoeken periodiek om te controleren of het proces effectief is en verzoeken tijdig en naar behoren worden afgehandeld.

3. MAKEN GEMEENTEN VOLDOENDE MIDDELEN EN CAPACITEIT VRIJ?

Elke gemeente is verplicht een Functionaris Gegevensbescherming aan te stellen.[36] Dat is een interne toezichthouder die controleert of de gemeente zich houdt aan de AVG en daarover adviseert.[37] Om volledig onafhankelijk toezicht te kunnen houden, moet een Functionaris Gegevensbescherming goed gepositioneerd zijn in de organisatie. Management- en directielagen boven een toezichthouder zijn niet wenselijk omdat dat de onafhankelijkheid in gevaar kan brengen. Een toezichthouder moet zich vrij door de organisatie kunnen bewegen en op het hoogste niveau kunnen rapporteren en adviseren. De Functionaris Gegevensbescherming mag geen instructies ontvangen over de uitvoering van diens taken en mag niet worden ontslagen voor de uitvoering van diens taken. Daarnaast moet een Functionaris Gegevensbescherming tijdig en naar behoren worden betrokken als het om de bescherming van persoonsgegevens gaat.[38]

Omdat een Functionaris Gegevensbescherming toezicht moet houden, is het niet wenselijk dat deze persoon ook belast wordt met uitvoerende taken. Dan moet de Functionaris Gegevensbescherming immers het eigen vlees gaan keuren. Daarom is het noodzakelijk dat er naast de toezichthouder ook privacy- en informatiebeveiliging medewerkers zijn die uitvoerende taken kunnen oppakken. Daar moet een gemeente financiële middelen voor vrij maken.

HOE DOEN GEMEENTEN HET OP DIT VLAK?

In de gemeente Rotterdam werd begin 2019 om voldoende middelen gevraagd door de toezichthouder.[39] Ook vanuit de concerndirectie wordt gelijktijdig benadrukt dat er extra capaciteit nodig is om voor de AVG-werkzaamheden de basis op orde te krijgen.[40] De vraag om geld beschikbaar te maken, wordt door het College van B&W grotendeels afgewezen.[41] In 2021 wordt nog eens benadrukt hoe belangrijk het is om voldoende capaciteit en kwaliteit beschikbaar te hebben.[42]

In de gemeente Utrecht geeft de Functionaris Gegevensbescherming in de rapportage van 2019/2020 aan dat hij goed gepositioneerd is en zijn onafhankelijke rol in voldoende mate kan uitvoeren. Er is echter maar weinig ondersteuning, waardoor hij belast wordt met veel administratieve taken.[43] In 2020 maakte de gemeente Utrecht geld vrij om 5 nieuwe privacy en security officers en een Chief Privacy Officer aan te nemen.[44]

In de gemeente Breda wordt in 2018 gewaarschuwd dat er vrijwel geen

capaciteit beschikbaar is, met alle risico's van dien.[45] Begin 2019 wordt het privacyteam uitgebreid naar 3,5 fte, maar door uitval is dat weer teruggebracht naar 1,5 fte. Ook worden de privacymedewerkers niet gekoppeld aan een teamleider, waardoor de Functionaris Gegevensbescherming informeel als teamleider werd gezien. In haar rapportage geeft ze aan dat dit onverenigbaar is met haar rol als toezichthouder.[46] In de rapportage van 2020 wordt aangegeven dat er beperkte voortgang zit in de beschikbaarheid van voldoende capaciteit.[47] In de voortgangsrapportage van 2021 wordt de directie opnieuw herinnerd aan de noodzaak voldoende capaciteit beschikbaar te stellen.[48]

In de gemeente Den Haag wordt eveneens door de Functionaris Gegevensbescherming aangegeven dat de gemeente niet beschikt over een toereikende privacy organisatie.[49] In 2020 wordt een uitgewerkt plan voorgelegd aan het managementteam om het privacyteam uit te breiden. Daarin wordt door de Functionaris Gegevensbescherming juist voorgesteld dat de Functionaris Gegevensbescherming de privacy officers functioneel aanstuurt (in tegenstelling tot de gemeente Breda).[50] Begin 2021 wordt een principebesluit genomen tot de oprichting van een centrale privacy organisatie. Daarbij wordt ook besloten de toezichthoudende rol van de Functionaris Gegevensbescherming te scheiden van het maken van beleid en de coördinatie op de uitvoering, inclusief de functionele aansturing van de privacy organisatie.[51]

De gemeente Tilburg heeft naast een Functionaris Gegevensbescherming drie privacy officers, maar door uitval van meerdere medewerkers is er feitelijk heel weinig capaciteit.[52]

In de gemeente Eindhoven is de beschikbaarheid van voldoende capaciteit eveneens een probleem. Uit een rapportage uit 2017 van de Chief Information Security Officer blijkt dat de gemeente onvoldoende voorbereid is op de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG), dat de verantwoordelijkheden hiervoor niet belegd zijn en dat er ook geen capaciteit voor aanwezig is.[53] In 2018 wordt het team uitgebreid met een aantal medewerkers.[54] In een rapportage over de jaarrekeningcontrole van Deloitte wordt aangegeven dat belangrijke doelstellingen niet behaald zijn door "frequente wisselingen op de CIO en CISO posities", en dat deze posities in 2019 tijdelijk niet ingevuld waren. Geadviseerd wordt om een succesieplan op te stellen voor cruciale posities binnen de organisatie.[55]

In de gemeente Groningen wordt in het jaarverslag van 2018 geadviseerd de formatie van het privacyteam te herzien omdat de beschikbare capaciteit niet toereikend is.[56] In de gemeente Almere wordt het privacyteam in 2021 uitgebreid.[57] In de gemeente Nijmegen wordt in 2018 de functie van de Chief Information Security Officer gecombineerd met die van de Functionaris Gegevensbescherming.[58] Dat is een opmerkelijke combinatie aangezien de Functionaris Gegevensbescherming ook toezicht moet houden op het werk van de Chief Information Security Officer. In de rapportage van 2019 wordt aangegeven dat in 2020 onderzocht zal worden of de positionering van de Functionaris Gegevensbescherming logisch en functioneel is.[59] Of en hoe hier opvolging aan is gegeven blijkt niet uit de ontvangen stukken.

WAAROM MOET DIT BETER?

In vrijwel elke gemeente blijkt het beschikbaar stellen van voldoende middelen een probleem. Privacyteams blijken onderbezet waardoor er onvoldoende geadviseerd kan worden over gegevensbescherming en -beveiliging. Ook geven verschillende toezichthouders aan dat dit er in resulteert dat afdelingen de motivatie verliezen om aandacht te hebben voor privacy, omdat ze daarin te weinig ondersteund worden. Deze keuzes vragen om problemen.

Zoals de Functionaris Gegevensbescherming van de gemeente Breda verwoordt:

> **"Onvoldoende expertise leidt ertoe dat afdelingen en projecten onvoldoende geadviseerd kunnen worden in de juiste toepassing van de AVG. Dit resulteert in onvoldoende bescherming van persoonsgegevens – een grondrecht waarvan de overheid de borging moet garanderen aan haar burgers. Wat de risico's van het beperken van grondrechten zijn, wordt pas duidelijk als het recht geschonden wordt. Als je niet meer**

vrijuit kunt spreken, voel je het belang van de vrijheid van meningsuiting. Als je een baan geweigerd wordt omdat je de verkeerde afkomst hebt, begrijp je het verbod op discriminatie. Wanneer gegevens over je gezondheid of financiën op straat liggen, realiseer je je dat je toch iets te verbergen hebt. Schendingen van het recht op privacy kunnen een enorme impact hebben op het leven van mensen, met verstrekkende gevolgen." [60]

Op landelijk niveau zien we dat de overheid graag voorop wil lopen met digitale innovatie[61], maar niet wil investeren in passend en effectief toezicht daarop.[62] De politieke keuze om wel geld te besteden aan de inzet van innovatieve technologieën, maar te weinig aan de borging van rechten van betrokkenen, lijken we ook bij lokale overheden terug te zien. Het is eenvoudig om te stellen dat men privacy belangrijk vindt, maar het vrijmaken en inzetten van middelen toont of gemeenten daad bij woord voegen.

AANBEVELINGEN

- Maak voldoende middelen vrij voor één van de belangrijkste kerntaken die een gemeente heeft: de verwerking en bescherming van persoonsgegevens. Zonder voldoende capaciteit op het gebied van gegevensbescherming en -beveiliging kan de rest van de gemeentelijke organisatie niet gefaciliteerd worden, met alle gevolgen van dien. Het gaat hier niet om een 'nice to have' maar om een 'need to have'.
- Gegevensbescherming en -beveiliging is niet een taak van een klein groepje medewerkers, maar een gezamenlijke verantwoordelijkheid voor alle afdelingen binnen de organisatie. Beleg de verantwoordelijkheden dan ook op de juiste plekken binnen de organisatie.
- Zorg ervoor dat de Functionaris Gegevensbescherming goed gepositioneerd is in de organisatie, zodat diens taken op onafhankelijke wijze uitgevoerd kunnen worden. Hiervoor is nodig dat er geen managementlagen zitten boven de toezichthouder en dat de toezichthouder rechtstreeks kan rapporteren aan de directie en wethouder. Ook is het van belang dat de Functionaris Gegevensbescherming geen taken krijgt die niet verenigbaar zijn met diens functie, zoals management- of uitvoerende taken.
- Reageer op de rapportages van de Functionaris Gegevensbescherming door aan te geven welke adviezen op welke wijze worden opgevolgd. Geef daarbij ook aan van welke adviezen er wordt afgeweken en met welke reden.

4. LEGGEN GEMEENTEN VOLDOENDE VERANTWOORDING AF EN WORDEN GEMEENTEN TER VERANTWOORDING GEROEPEN?

Het College van Burgermeester & Wethouders is bestuurlijk verantwoordelijk voor de naleving van de privacywet binnen een gemeente. Op ambtelijk niveau is de gemeentesecretaris de hoogste leidinggevende. De gemeenteraad is het hoogste bestuursorgaan van een gemeente en controleert het College van B&W. Zij kan, bijvoorbeeld door middel van raadsvragen, bestuurders ter verantwoording roepen.[63] De burgemeester en wethouders zijn ieder afzonderlijk verantwoording schuldig over het gevoerde beleid aan de gemeenteraad.[64] Daarnaast hebben gemeenten een Rekenkamer die onderzoek doet naar de doelmatigheid, doeltreffendheid en rechtmatigheid van het gevoerde beleid.[65] De gemeenteraad en de Rekenkamer kunnen dus beiden vanuit hun taken en bevoegdheden informeren naar de manier waarop er wordt omgegaan met de bescherming van persoonsgegevens binnen de gemeente.

HOE DOEN GEMEENTEN HET OP DIT VLAK?

Van de tien gemeenten informeren slechts vier gemeenten de gemeenteraad actief door de AVG-rapportages met hen te delen. Dit zijn de gemeenten Amsterdam[66], Utrecht[67], Eindhoven[68] en Groningen[69]. In de gemeente Rotterdam is er in 2021 een motie aangenomen waarin de wethouder wordt gevraagd frequenter, periodiek en uitgebreider te rapporteren over de AVG.[70] In de gemeente Den Haag wordt er in 2021 een presentatie gehouden over de AVG, waarbij kort is ingegaan op de stand van zaken in de gemeente.[71] Ook in de gemeente Breda is er in 2022 een presentatie gehouden door de Functionaris Gegevensbescherming over de AVG, en beknopt over de stand van zaken binnen de gemeente.[72] In de gemeente Nijmegen werd er in jaarrekeningen een passage opgenomen over informatiebeveiliging en privacy.[73] In de gemeente Tilburg waren er geen AVG-rapportages om te delen met de gemeenteraad. In de gemeente Almere hebben we geen informatieverstrekking over AVG-rapportages kunnen vinden die gedeeld zijn met de gemeenteraad.

De gemeenten Amsterdam, Eindhoven en Groningen hebben de AVG-rapportages ook op hun website openbaar gemaakt. De gemeenten Amsterdam, Rotterdam, Utrecht, en Nijmegen hebben hun verwerkingsregister gepubliceerd op de website. De gemeente Amsterdam heeft daarnaast ook een algoritmeregister gepubliceerd.

Hoewel uit de ontvangen documenten blijkt dat een aantal gemeenten

transparantie en openheid over het bestuurshandelen duidelijk belangrijk vindt, geeft de meerderheid van de gemeenten minder openheid. Rapportages worden niet altijd gedeeld met de gemeenteraad, maar ook toen we de Wob-verzoeken indienden merkten we terughoudendheid om de openbaarheid van bestuur, waartoe gemeenten wettelijk verplicht zijn, te verschaffen. De gemeente Almere vond het zelfs nodig om grote delen weg te lakken. Dat staat in schril contrast met de gemeenten die de rapportages uit eigen beweging netjes en ongelakt op hun website publiceren.

Naast gemeenteraden hebben ook Rekenkamers een controlerende functie. De Rekenkamers van de tien grootste gemeenten hebben nog geen voltooid onderzoek gedaan naar de werking van de AVG. Wel deed een aantal Rekenkamers onderzoek naar informatiebeveiliging, soms in relatie tot de bescherming van persoonsgegevens. Dit zijn de Rekenkamers van Rotterdam[74], Utrecht[75], Eindhoven[76] en Breda[77]. De Rekenkamer van Nijmegen heeft momenteel een onderzoek lopen naar privacy en informatiebeveiliging.[78]

WAAROM MOET DIT BETER?

Burgers moeten er op kunnen vertrouwen dat hun persoonsgegevens op een rechtmatige en veilige manier verwerkt worden. Maar vertrouwen ontstaat niet uit het niets. Door verantwoording af te leggen en openheid te bieden over hoe er met persoonsgegevens wordt omgegaan, kan dat vertrouwen zowel bij controlerende organen als bij burgers groeien. Daarbij is het van belang dat gemeenten kunnen aantonen dat ze een lerende organisatie zijn en concrete stappen zetten om tot een goed niveau van be-

scherming te komen. Behalve dat burgers gebaat zijn bij die transparantie, helpt het ook gemeenteraden en Rekenkamers in hun controlerende taken. Bovendien helpt het verantwoordelijken zelf als ze open kaart spelen en daarbij eerlijk zijn over de stand van zaken. Zo laten ze immers zien dat ze op de hoogte zijn van de situatie en kunnen ze verbeterprocessen presenteren. Het blijft voor verantwoordelijken van belang om te beseffen dat vertrouwen te voet komt, maar te paard gaat.

AANBEVELINGEN

- Leg verantwoording af aan de gemeenteraad door de AVG-rapportages en de reacties daarop actief te delen, en maak deze openbaar.
- Volg als gemeenteraad een AVG-cursus, gericht op de controlerende functie van de gemeenteraad, zodat gemeenteraadsleden beter weten waar ze op moeten letten.
- Vraag als gemeenteraadslid informatie op over de naleving van de AVG. Maak afspraken met het College van B&W (of de portefeuille houdende wethouder) over het periodiek op de hoogte gebracht worden over de stand van zaken.
- Doe als Rekenkamer onderzoek naar de opvolging van de AVG en de bescherming van persoonsgegevens.

5. WAT MOET ER BETER?

Gemeenten hebben hun basis gegevenshuishouding nog niet op orde. Zolang gemeenten niet weten welke persoonsgegevens ze in huis hebben, wat ze met die gegevens doen, of dat rechtmatig is, en of gegevens tijdig gearchiveerd worden, levert dat risico's op voor overheden en voor inwoners. Verwerkingsregisters zijn niet volledig of actueel, gemeenten hebben niet altijd goed in beeld met wie er samengewerkt wordt en welke contracten daaronder liggen. En hoe zit het met de beveiliging van al die gegevens in allerlei verschillende systemen? Ook worden AVG-verzoeken nog niet overal behandeld zoals zou moeten. Verzoeken blijven te lang liggen, zonder legitieme reden. En op het gebied van verantwoording afleggen aan de gemeenteraad valt ook nog winst te behalen. Zonder voldoende middelen en capaciteit kunnen gemeenten weinig doen om de situatie te verbeteren.

Naar aanleiding van dit onderzoek doen we de volgende aanbevelingen:

- Prioriteer het vullen en actueel houden van het verwerkingsregister. Zie dit niet als een eenmalige klus, maar als een doorlopend proces waarbij kritisch gekeken wordt naar welke verwerkingen nog noodzakelijk en rechtmatig zijn, en welke verwerkingen gestopt kunnen worden.
- Publiceer het verwerkingsregister op de website. Dit is welliswaar geen verplichting vanuit de AVG, maar het biedt wel transparantie.

- Verwerk geen gegevens op een manier die niet te verantwoorden is, bijvoorbeeld door algoritmen geautomatiseerde beslissingen te laten maken die niet transparant en motiveerbaar zijn. Houdt ten alle tijden de algemene beginselen van behoorlijk bestuur voor ogen.
- Zorg ervoor dat in beeld wordt gebracht met welke partijen samenwerkingen zijn aangegaan en vanuit welke hoedanigheid en bevoegdheid. Is er sprake van (gedeelde) verwerkingsverantwoordelijkheid of van een verwerker? Documenteer de daarbij behorende overeenkomsten centraal.
- Begin niet aan 'datagedreven werken' met behulp van nieuwe technologieën en datagedreven toepassingen zoals big data en algoritmen als de basis niet op orde is.
- Zorg voor een effectief proces voor AVG-verzoeken van burgers, waarbij de verantwoordelijkheden goed belegd zijn.
- Evalueer het proces voor AVG-verzoeken periodiek om te controleren of het proces effectief is en verzoeken tijdig en naar behoren worden afgehandeld.
- Maak voldoende middelen vrij voor één van de belangrijkste kerntaken die een gemeente heeft: de verwerking en bescherming van persoonsgegevens. Zonder voldoende capaciteit op het gebied van gegevensbescherming en -beveiliging kan de rest van de gemeentelijke organisatie niet gefaciliteerd worden, met alle gevolgen van dien. Het gaat hier niet om een 'nice to have' maar om een 'need to have'.
- Zie gegevensbescherming en -beveiliging niet als een taak van een klein groepje medewerkers, maar als een gezamenlijke verantwoordelijkheid voor alle afdelingen binnen de organisatie.
- Zorg ervoor dat de Functionaris Gegevensbescherming goed gepositioneerd is in de organisatie, zodat diens taken op onafhankelijke wijze uitgevoerd kunnen worden. Hiervoor is nodig dat er geen managementlagen zitten boven de toezichthouder en dat de toezichthouder rechtstreeks kan rapporteren aan de directie en wethouder.
- Reageer op de rapportages van de Functionaris Gegevensbescherming door aan te geven welke adviezen op welke wijze worden opgevolgd. Geef daarbij ook aan van welke adviezen er worden afgeweken en met welke reden.
- Leg verantwoording af aan de gemeenteraad, deel de AVG-rapportages en de reacties daarop, en maak deze openbaar.
- Volg als gemeenteraad een AVG-cursus, gericht op de controlerende functie van de gemeenteraad, zodat gemeenteraadsleden beter weten waar ze op moeten letten.

- Vraag als gemeenteraadslid informatie op over de naleving van de AVG. Maak afspraken met het College van B&W (of de portefeuille houdende wethouder) over het periodiek op de hoogte gebracht worden over de stand van zaken.
- Doe als Rekenkamer onderzoek naar de opvolging van de AVG en de bescherming van persoonsgegevens.

NAWOORD

OVER BITS OF FREEDOM EN DIT ONDERZOEK

Bits of Freedom is een burgerrechtenorganisatie die gelooft in een open en rechtvaardige informatiesamenleving. Een waarin mensen de macht ter verantwoording kunnen roepen en de status quo effectief kunnen bevragen. Sinds 1999 zet Bits of Freedom zich in om wetgeving en beleid te beïnvloeden ter ondersteuning van deze visie. Dat doen we door middel van belangenbehartiging, onderzoek, campagne en juridische actie, in Nederland en Brussel.

Bits of Freedom zet zich in voor de bescherming van het recht op privacy. De AVG is een belangrijke wet waarin het recht op de bescherming van persoonsgegevens geborgd wordt. In een maatschappij waarin de mogelijkheden met data steeds groter worden en persoonsgegevens steeds kostbaarder, groeit ook het belang om rechten van mensen te beschermen. Burgers staan in een afhankelijke en onevenwichtige relatie tot de overheid. Hen wordt niet de keuze voorgelegd of ze het goed vinden dat hun persoonsgegevens door overheden verwerkt worden, want vaak berust de verwerking op een wettelijke grondslag. Dat brengt voor overheden ook de verantwoordelijkheid met zich mee om op een betrouwbare en veilige manier met persoonsgegevens om te gaan.

Als burgerrechtenorganisatie focussen we ons op situaties die grote impact hebben op burgers en de maatschappij. In dit onderzoek hebben we ons gericht op gemeenten, omdat deze overheidsinstellingen het dichtst bij de burger staan. Van de wieg tot het graf worden er door gemeenten persoonsgegevens verwerkt die soms heel gevoelig van aard zijn. De afgelopen jaren zijn er verschillende signalen geweest dat de overheid niet altijd even verantwoordelijk omgaat met haar verplichting om de persoonsgegevens van mensen te beschermen. Denk bijvoorbeeld aan het recente datalek bij de GGD in Rotterdam en het incident bij Bureau Jeugdzorg Utrecht in 2019, waarbij duizenden dossiers van kwetsbare kinderen op straat kwamen te liggen als gevolg van slechte AVG-naleving. Evenals het toeslagenschandaal waarbij de AVG-schendingen, maar ook de mensenrechtenschendingen in het algemeen een bodemloze put lijkt te zijn. Dit soort onrechtmatige praktijken en datalekken hebben ernstige gevolgen voor het leven van slachtoffers en kunnen iemands leven ingrijpend veranderen.

Onze beleidsadviseur betrokken bij dit onderzoek is in het verleden als Functionaris Gegevensbescherming bij één van de onderzochte gemeenten werkzaam geweest. Deze ervaring hielp bij de interpretatie van de ontvangen stukken en om de informatie in perspectief te plaatsen. Dit on-

derzoek is uiteraard enkel op basis van de stukken die we van gemeenten hebben ontvangen tot stand gekomen.

DE SCOPE VAN DIT ONDERZOEK

Met onze verzoeken openbaarheid van bestuur wilden we erachter komen hoe de tien grootste gemeenten de privacywet naleven. De AVG bevat allerlei verplichtingen voor verwerkingsverantwoordelijken die er gezamenlijk voor moeten zorgen dat de rechten van betrokkenen goed geborgd zijn. Voor ons, als kleine organisatie, was het niet mogelijk de naleving van de gehele wet te toetsen. We hebben ons daarom beperkt tot onderdelen die de meeste impact hebben op burgers en de maatschappij. Namelijk of gemeenten voldoende overzicht hebben van de persoonsgegevens die ze verwerken en hoe er met deze gegevens wordt omgegaan; de wijze waarop AVG-verzoeken in behandeling worden genomen; of er voldoende prioriteit wordt gegeven aan de naleving van de AVG door voldoende middelen en capaciteit ter beschikking te stellen; en of er voldoende verantwoording wordt afgelegd aan controlerende organen binnen de gemeenten.

Deze onderwerpen hebben een indruk gegeven van hoe het gemeenten is vergaan sinds de inwerkingtreding van de AVG. Met de beperkte informatie die ons ter beschikking is gesteld en de nauwe scope van ons onderzoek kunnen we echter niet vaststellen hoe de AVG in z'n geheel wordt nageleefd door gemeenten. Ook laten sommige gemeenten gelukkig een groei zien, waardoor het mogelijk is dat er sinds de laatste rapportages die wij ontvangen hebben, ontwikkelingen zijn geweest waardoor gemeenten inmiddels beter voldoen aan de AVG. Daar hopen we op.

Alle documenten waar dit rapport op gebasseerd is, zijn te vinden op onze website www.bitsoffreedom.nl.

WOORD VAN DANK

We danken de gemeenten die we onderzocht hebben voor hun openheid, de medewerking en de gesprekken. We hopen dat de gemeenten die we onderzocht hebben, maar ook andere gemeenten, zich uitgedaagd voelen de rechten van burgers nog beter te beschermen en dat dit rapport als duwtje in de rug wordt beschouwd. Uiteraard lichten we onze conclusies en aanbevelingen graag nader toe aan de betreffende gemeenten. We danken ook de Functionarissen Gegevensbescherming en andere professionals binnen en buiten gemeenten die met ons in gesprek gingen over hun ervaringen en hun inzichten deelden over wat er beter moet en kan.

KOM JE OOK IN ACTIE?

Ben je een burger en wil je weten hoe het in jouw gemeenten gesteld is met de bescherming van jouw persoonsgegevens? Dan kun je op grond van de Wet openbaarheid van bestuur een verzoek indienen bij je gemeente. Je kunt bijvoorbeeld, zoals wij voor dit onderzoek hebben gedaan, alle rapportages opvragen van de Functionaris Gegevensbescherming. Ook kun je informatie (bijvoorbeeld een Data Protection Impact Assessments) opvragen over bepaalde gegevensverwerkingen, zoals de inzet van wifi-sensoren, camera's of het gebruik van algoritmen. Ook kun je beroep doen op je AVG-rechten, zoals het recht op inzage. Bits of Freedom heeft daar een handige tool voor. Kijk daarvoor op mydatadoneright.eu. We hopen dat dit onderzoek anderen inspireert verder op onderzoek uit te gaan naar de wijze waarop het recht op privacy geborgd wordt. Onze grondrechten vormen immers een belangrijk fundament van onze rechtsstaat, die we niet als vanzelfsprekend mogen beschouwen.

EINDNOTEN

1 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-biedt-10-stappen-plan-voorbereiding-nieuwe-privacywet
2 Artikel 30 AVG
3 Jaarverslag van de Functionaris Gegevensbescherming Gemeente Utrecht, 2018, p.3
4 https://www.utrecht.nl/bestuur-en-organisatie/privacy/register-verwerkingen/
5 DR rapportage concerncontrol Gemeente Eindhoven, mei 2021
6 Algemene Verordening Gegevensbescherming toezichtsrapportage en advies van de FG Gemeente Almere, tweede kwartaal 2021, p.5
7 Algemene Verordening Gegevensbescherming, Stand van zaken en aanbevelingen, naar aanleiding van de resultaten van de nulmeting van 25 oktober 2018, Gemeente Breda, p.7
8 Agendapunt Rapportagelijn Functionaris Gegevensbescherming, Gemeente Rotterdam, 24 oktober 2018, p.2
9 Agendapunt 2.A. Tweede rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 20 februari 2019, p.3
10 Agendapunt 4. Derde Rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 26 juni 2019, p.1
11 Agendapunt Jaarverslag 2019 Functionaris Gegevensbescherming, Gemeente Rotterdam, 18 maart 2020, p.1
12 Voordracht voor de College vergadering van 06 juli 2021, ICT en Digitale Stad (42), B40, Gemeente Amsterdam, p.3
13 Voordracht voor de College vergadering van 06 juli 2021, ICT en Digitale Stad (42), B40, Gemeente Amsterdam, p.2
14 Jaarplan privacy 2020 gemeente Den Haag, functionaris gegevensbescherming, 10 juni 2020, p.3
15 Jaarverslag 2018 Functionaris Gegevensbescherming Gemeente Groningen, 16 april 2019, p.2
16 https://autoriteitpersoonsgegevens.nl/nl/nieuws/werkwijze-belasting-dienst-strijd-met-de-wet-en-discriminerend
17 https://www.amnesty.nl/actueel/xenophobic-machines-discrimination-through-un-regulated-use-of-algorithms-in-the-dutch-childcare-benefits-scandal
18 Jaarplan privacy 2020, Gemeente Den Haag, 10 juni 2020, p.2
19 https://nos.nl/artikel/2366864-fraude-opsporen-of-gevaar-van-discriminatie-gemeenten-gebruiken-slimme-algoritmes
20 Artikel 12 e.v. AVG
21 Artikel 12 lid 3 AVG
22 Artikel 12 lid 3 AVG
23 Evaluatie Privacybeleid 2018, Gemeente Nijmegen, 1 september 2019, p.1
24 Jaarrapportage Privacy 2020, Gemeente Nijmegen, 23 november 2020, p.1
25 Kennisneming van de Rapportage 2020 informatiebeveiliging en de Rapportage 2020 Functionaris gegevensbescherming, Gemeente Amsterdam, 6 juni 2021, p.4
26 Jaarverslag 2018 Functionaris Gegevensbescherming, Gemeente Groningen, 16 april 2019, p.2
27 Verslag Functionaris voor gegevensbescherming 2019/2020, 5 juli 2021, p.7
28 Algemene verordening gegevensbescherming, Rechten van betrokkenen uitgelicht: het inzagerecht, Gemeente Breda, 30 augustus 2019
29 AVG Jaarrapportage 2019, College van B&W, Gemeente Breda, p.15
30 AVG jaarrapportage 2020, Gemeente Breda, 5 maart 2021, p.2
31 Voortgangsrapportage AVG/BIO, Gemeente Breda, 14 juni 2021, p.5
32 Agendapunt 2.B Rapportage CPO n.a.v. tweede rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 20 februari 2019, p.2
33 Agendapunt 4. Derde rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 26 juni 2019, p.2 e.v.
34 Agendapunt vierde Rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 6 november 2019, p.4
35 Jaarverslag 2020 Functionaris Gegevensbescherming, Gemeente Rotterdam, p.7
36 Artikel 37 lid 1 aanhef en onder a AVG
37 Artikel 39 AVG
38 Artikel 38 AVG
39 Agendapunt 2.A. Tweede Rapportage Functionaris gegevensbescherming, Gemeente Rotterdam, 20 februari 2019, p.2

40 Agendapunt 2.B Rapportage CPO n.a.v. Tweede Rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam 20 februari 2019, p.4
41 Agendapunt 4. Derde Rapportage Functionaris Gegevensbescherming, Gemeente Rotterdam, 26 juni 2019, p.1
42 Privacy Monitor Eerste Kwartaal 2021, FG rapport, Gemeente Rotterdam, p.2
43 Verslag Functionaris voor Gegevensbescherming 2019/2020,Gemeente Utrecht, 5 juli 2021, p.7
44 Bestuurlijke reactie Jaarverslag Fucntionaris Gegevensbescherming, Gemeente Utrecht, 13 juli 2021, p.2
45 Algemene verordening gegevensbescherming, Stand van Zaken en Aanbevelingen, Naar aanleiding van de resultaten van de nulmeting van 25 oktober 2018, Gemeente Breda, 29 november 2018, p.9
46 AVG Jaarrapportage 2019, College van B&W, Gemeente Breda, p.11
47 AVG Jaarrapportage 2020, Gemeente Breda, 5 maart 2021, p.2
48 Voortgangsrapportage AVG/BIO, Gemeente Breda, 14 juni 2021
49 Jaarverslag Functionaris Gegevensbescherming 2019, Gemeente Den Haag, juni 2020, p.5
50 Viermaandelijkse Wethoudersrapportage IV-Beleid en ICT, periode januari-april 2020, Gemeente Den Haag, mei 2020, p.7
51 Viermaandelijkse Rapportage IV-Beleid en ICT, periode januari-april 2021, Gemeente Den Haag, mei 2021, p.3
52 Blijkt uit een gesprek met de gemeente Tilburg
53 Status Implementatie Baseline Informatiebeveiliging Gemeenten (BIG), Gemeente Eindhoven, maart 2017, p.4
54 Rapportage van BIG naar BIO, Concerncontrol, Gemeente Eindhoven, juli 2019, p.8
55 IT Audit Management Letter 2019, Gemeente Eindhoven, Deloitte, 2 oktober 2019, p.7
56 Jaarverslag 2018 Functionaris Gegevensbescherming, Gemeente Groningen, 16 april 2019, p.2 en 12
57 Managementreactie opde toezichtsrapportage Q2 2021, Gemeente Almere, 10 september 2021, p.3
58 Rapportage Informatiebeveiliging en Privacy, periode 2017, Gemeente Nijmegen, p.11
59 Rapportage Informatiebeveiliging en Privacy, periode 2019, Gemeente Nijmegen, p.10
60 AVG Jaarrapportage 2019, College van B&W, Gemeente Breda, p.11
61 Zie bijvoorbeeld de Nederlandse Digitaliseringsstrategie 2021
62 Wij schreven hier eerder over in deze blog: https://www.bitsoffreedom.nl/2020/12/18/digitaal-wakker-terwijl-de-toezichthouder-in-slaap-wordt-gehouden/
63 Artikel 155 lid 1 Gemeentewet
64 Artikel 169 Gemeentewet
65 Artikel 182 Gemeentewet
66 o.a. Voordracht voor de College vergadering van 15 december 2020, Instemmen met het Stedelijk kader informatiebeveiliging gemeente Amsterdam, VN2020-029441
67 o.a. Raadsbrief Jaarverslag gegevensbescherming, Gemeente Utrecht, 9 juli 2021, 9009809
68 o.a. B&W-dossier Beslissingsblad, Jaarrapportage 2020, bescherming van persoonsgegevens (AVG), Gemeente Eindhoven, 7 april 2021, 20bst00883
69 o.a. https://gemeenteraad.groningen.nl/Documenten/Bijlage-Jaarverslag-2018-Functionaris-Gegevensbescherming.pdf
70 12 juni 2021, 21bb007665 (https://gemeenteraad.rotterdam.nl/Agenda/Document/5617ea1b-b9c2-4f25-9c95-686610c9cb90?documentId=054d34f8-1679-4925-b8af-018f42dff73a&agendaItemId=f4e45d90-d241-403f-a82a-3f14cd21cb30)
71 https://denhaag.raadsinformatie.nl/document/9887853/1#search=%22avg%22
72 https://c.connectedviews.com/05/SitePlayer/gemeente_breda?session=114621
73 Rapportage informatiebeveiliging en Privacy periode 2017, Gemeente Nijmegen, pagina 3 (en de daarop volgende rapportages).
74 https://rekenkamer.rotterdam.nl/onderzoeken/in-onveilige-handen/
75 https://www.utrecht.nl/fileadmin/uploads/documenten/7.extern/Rekenkamer/20210407_Bestuurlijk_rapport_informatieveiligheid.pdf
76 https://www.nvrr.nl/rekenkamerrapport/9857/informatieveiligheid-smart-en-safe/
77 https://112.wpcdnnode.com/rekenkamerbreda.nl/wp-content/uploads/Informatiebeveiliging-bij-de-gemeente-Breda.pdf
78 https://www.nijmegen.nl/over-de-gemeente/rekenkamer/onderzoeksrapporten/informatiebeveiliging-en-privacybescherming/

Bits of Freedom komt op voor jouw vrijheid en privacy op internet.

Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd.

Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Bits of Freedom
www.bitsoffreedom.nl
@bitsoffreedom
Prinseneiland 97HS
1013 LN Amsterdam

Contactpersoon:
Evelyn Austin
+31 6 2689 5124
evelyn@bitsoffreedom.nl

B5EC 8503 1F6C BEC6 47E6
C0BA E7D0 CB5B 8803 65C9
(bitsoffreedom.nl/openpgp)

BITS OF FREEDOM

Voor jouw internetvrijheid