



**Gemeente
Rotterdam**

Bezoekadres: Stadhuis Coolsingel 40
3011 AD Rotterdam
Postadres: Postbus 70012
3000 KP Rotterdam

Website: www.rotterdam.nl
E-mail: concernprivacyofficebco@rotterdam.nl
Inlichtingen: A.D. Mijland
Telefoon: 06-30421175

Portefeuillehouder: mr. A.H.P. van Gils
Cluster: Cluster BCO - Concernstaf en Strategie
Ons kenmerk: 21bb014575 – 22bo3866
Uw kenmerk: 21bb8175, 21bb007665

Datum: B&W 7 juni 2022

Betreft: Afdoening motie 'Gemeente Rotterdam voldoet aan privacywetgeving'

Aan de Gemeenteraad

Geachte raadsleden,

In vervolg op het verantwoordingsdebat ter vaststelling van de Jaarstukken 2020 is op 17 juni 2021 door uw raad de motie 'Gemeente Rotterdam voldoet aan privacywetgeving' aangenomen (21bb8175), ingediend door het raadslid van der Velden (Partij voor de Dieren).

De raad verzoekt hierin het college er zorg voor te dragen dat de organisatie duurzaam en aantoonbaar 'AVG-proof' wordt, daartoe een plan van aanpak op te stellen, daaraan een termijn te koppelen en het plan te delen met de raad.

In november 2021 informeerden wij u over de tussenstand en een toezegging (21bb8175 en 21bb007665). Via deze brief informeren wij u graag over de aanpak van het college om de AVG duurzaam in te bedden in de organisatie. Tevens is dit het voorstel tot afdoening van de motie.

Om u een beeld te geven van de huidige stand van zaken, nemen wij u in vogelvlucht mee vanaf de invoering van de Algemene Verordening Gegevensbescherming (AVG) in 2018 tot heden. Met daaruit volgend de resterende stappen. Met als doel een organisatie te zijn waarbij op een veilige manier met de persoonsgegevens van Rotterdammers wordt omgegaan.

Gezien de breedte van het onderwerp wordt in deze brief ook verwezen naar enkele hieraan gerelateerde raadsvoorstellen.

Eerste fase: de fundamente (2018-2019)

Met de invoering van de AVG in 2018 werden de privacyrechten van burgers versterkt en uitgebreid. De wet gaf organisaties meer verantwoordelijkheden en de externe toezichthouder (Autoriteit Persoonsgegevens) kreeg steviger bevoegdheden, waaronder de mogelijkheid om hoge boetes op te leggen.

In die eerste fase (2018- medio 2019) lag de focus binnen de gemeentelijke organisatie op het invoeren van de volgende wettelijk verplichte instrumenten:

- Privacybeleid en inrichting van de privacyfuncties, rollen en verantwoordelijkheden.
- Aanstelling van een Functionaris gegevensbescherming (FG) als interne toezichthouder.
- Register van verwerkingen.
- Protocol datalekmeldingen en datalekregister.
- Proces voor de Data Protection Impact Assessment (DPIA's).
- Model verwerkersovereenkomst.
- De inrichting van het proces voor AVG-verzoeken van burgers (Rechten van betrokkenen).
- Principles Privacy by design en privacy by default.
- Bewustwording (Blijf alert!)

Daarmee is een stevig fundament gelegd. De organisatie beschikt daarmee over de wettelijke instrumenten die de basis vormen om privacygevoelige gegevens van burgers en medewerkers te kunnen beschermen. De uitrol van het beleid en het 'tussen de oren krijgen' van wat de AVG beoogt, was de volgende stap.

Tweede fase: opbouw en inrichting (2019-2021)

Op deze fundamenteën werd in deze fase verder gebouwd.

In juli 2019 was het *register van verwerkingen* grotendeels compleet met daarin de processen waarbij persoonsgegevens verwerkt worden. Het register is de basis, zowel voor de verdere implementatie van de AVG als voor de sturing daarop.

Voor processen die waarschijnlijk een hoog risico opleveren voor betrokkenen, bijvoorbeeld wanneer grootschalig of gevoelige persoonsgegevens worden verwerkt, is een DPIA (Data Protection Impact Assessment) nodig. Hieruit volgen maatregelen die de risico's kunnen verkleinen. Van de aanvraag voor een bijstandsuitkering tot een parkeerboete, van cameratoezicht tot handhaving op straat, de gemeente kent vele processen met een hoog privacyrisico. Daar lag dus nog een grote opgave. Inmiddels zijn de meeste DPIA's op bestaande processen uitgevoerd.

Ook het afsluiten van *verwerkersovereenkomsten* was een flinke opgave. Wanneer de gemeente een (externe) partij inschakelt om namens haar persoonsgegevens te verwerken, kan zij daarvoor alleen gebruikmaken van verwerkers die afdoende garanties bieden dat die verwerking aan de vereisten van de AVG voldoet. Die vereisten worden vastgelegd in een overeenkomst met de verwerkende partij. Voor de meeste verwerkingen waarbij een (externe) verwerker is betrokken is een overeenkomst afgesloten waarin die garanties zijn vastgelegd.

In deze fase is *advisering over privacy en AVG* verder geprofessionaliseerd. De privacy experts worden steeds vaker gevraagd te adviseren bij vaak complexe maatschappelijke vraagstukken waarbij privacy een rol speelt. Dit vraagt kennis op zowel het gebied van AVG als van domeinwetgeving.

De *transparantie* is in deze periode vergroot, met een openbare versie van het register van verwerkingen op de website van de gemeente Rotterdam.

Tevens richtten wij ons in deze periode actief op het *vergroten van het bewustzijn* door campagnes (Blijf Alert!) en kennisdeling, zoals e-learnings voor alle medewerkers.

Daarnaast is er een plan van aanpak voor de borging van *Privacy by design*; dat wil zeggen dat al bij het ontwerpen van een systeem of proces rekening wordt gehouden met privacy. Het wordt dan een integraal onderdeel van een werkproces.

Derde fase: de afronding (eind 2022)

De tweede fase bleek een stevige opgave. De focus ligt in de derde fase (tot eind 2022) op efficiënte(re) werkprocessen, door de evaluatie van werkafspraken en protocollen en de verbetering daarvan. Het gaat daarbij om de herijking van alle eerdergenoemde AVG-instrumenten, zoals het DPIA proces, de datalekmeldingen, het verbeteren van het inzageproces voor burgers, etc. Daarnaast wordt de inrichting van de privacyfunctie in de organisatie (governance) onderzocht en waar nodig aangepast.

Het streven is om deze fase voor het eind van dit jaar af te ronden. De onderwerpen zijn in lijn met de verbeterpunten die de Functionaris Gegevensbescherming (FG) benoemt in zijn jaarverslag om als organisatie *in control* te komen.

AVG thema	Acties 2022	Gereed
Datalekken	Evalueren en herziening van het datalekproces /datalekprotocol	Jul 2022
Verwerkersovereenkomst	- Procesbeschrijving, Factsheet en Beslisboom - Afsluiten verwerkersovereenkomsten voor geregistreerde verwerkingen met een verwerker	Aug 2022 Dec 2022
Transparantie	Actualiseren Privacyverklaring en actualiseren communicatie op Rotterdam.nl en Intern (RIO)	Aug 2022
Verwerkingsregister	Inrichting en beheer verwerkingsregister	Aug 2022
Governance	Herziening Privacy Governance structuur en -beleid	Okt 2022
AVG verzoeken	Evalueren en doorontwikkeling proces AVG-verzoeken (Rechten van Betrokkenen)	Nov 2022
DPIA	- Evalueren en Herijking DPIA Proces/ instrumenten - Uitvoeren DPIA's (Data Protection Impact Assessment) voor alle geregistreerde risicovolle verwerkingen	Dec 2022 Dec 2022
Privacy by Design	Uitrol Privacy by Design	Dec 2022

Vierde fase: datatechnologie en gegevensdeling, 2022 en verder

Met de afronding van de voorgaande fases constateren we dat we de risico's voor de privacy van burgers voor een groot deel in kaart hebben en daarmee kunnen verkleinen. De grip op privacy groeit daarmee. Maar risico's zullen er altijd zijn. Een organisatie die 100% 'AVG proof' is bestaat niet. Want ondertussen digitaliseert de samenleving in sneltreinvaart en brengt nieuwe uitdagingen met zich mee. Samengevat betekent dit dat de organisatie zich vanaf 2022 richt op *kaders en richtlijnen* voor:

- Algoritmes en kunstmatige intelligentie (22bb1555, collegebrief governance algoritmes)
- Smart cities (22bb3084, afwegingskader sensoren, datatoepassingen en AI)
- Datagedreven werken en (her)gebruik van gegevens
- Gegevensdeling in het sociale en veiligheidsdomein

- Gegevensdeling buiten de grenzen van de EU (Schremms II)¹
- Implementatie van Europese en landelijke kaders en wetgeving

In samenhang daarmee blijven we doorlopend werken aan:

- Continuïteit in het beheer en uitvoering van de AVG-instrumenten
- Advisering op privacyvraagstukken
- Driejaarlijkse uitvoering DPIA's
- Uitvoering van maatregelen voortkomend uit de DPIA's
- Toepassen van Privacy by design
- Blijvende aandacht voor privacy creëren door kennis (e-learning) en campagnes
- Inrichting privacy volgens de WPG (Wet Politiegegevens, die ook geldt voor handhavingsfuncties)
- Transparantie: informatie voor de burger, uitbreiden van het openbare register van verwerkingen met alle samenvattingen van DPIA's en uitbreiding van het algoritmeregister, ook in het kader van de WOO (Wet Open overheid).

De toekomst

De uitdagingen zijn ook voor de komende jaren groot. Rotterdam heeft veel ambities die pas mogelijk worden als rechten van onze burgers en medewerkers goed worden beschermd en het vertrouwen er is dat persoonsgegevens in goede handen zijn bij de overheid. Privacybeleid moet daarop aansluiten, én worden nageleefd. Want de privacy van burgers is een groot goed, vastgelegd in de Grondwet, dat beschermd dient te worden. Ook de ethische aspecten moeten daarin zwaar wegen.

Anderzijds neemt de maatschappelijke druk op de overheid toe als het gaat om thema's als armoedebestrijding of veiligheid. Daar ontstaat soms een spanningsveld met de privacywetgeving. De uitdaging ligt dan ook in het vinden van een goede balans tussen wetgeving enerzijds en wat nodig is om deze doelen te bereiken en de burger integraal van dienst te kunnen zijn, met oog voor de menselijke maat.

Dit vergt voor bestuur en organisatie alertheid op de relatie tussen bestuurlijke wensen enerzijds en het risico voor de privacy van de burger anderzijds, en we zien dit dan ook als een belangrijk aandachtspunt. Het college is zich hiervan bewust en onderschrijft haar rol om deze maatschappelijke waarde te beschermen en te verdedigen, en daarin de juiste afwegingen te maken.

Met bovenstaande stellen wij voor de motie 'Gemeente Rotterdam voldoet aan privacywetgeving' als afgedaan te beschouwen.

Burgemeester en Wethouders van Rotterdam,

De secretaris,

V.J.M. Poozen

De burgemeester,

A. Aboutaleb

¹ Op 16 juni heeft het Hof van Justitie van de Europese Unie een [uitspraak gedaan in de Schrems II-zaak](#), met als gevolg dat gegevens leveren of opslag daarvan in de VS niet is toegestaan tenzij aan een aantal eisen en waarborgen moet voldoen. Dit geldt ook voor veel andere landen buiten de EU. Dit heeft gevolgen voor veel organisaties.