Gemeente Rotterdam

Bestuurs- en concernondersteuning

Datum: 17 mei 2018

Privacybeleid Gemeente Rotterdam

Inleiding

Op 25 mei 2018 treedt de Algemene verordening gegevensbescherming (hierna AVG) in werking. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie (EU). Lidstaten hebben slechts zeer beperkte vrijheid om aanvullende regelgeving vast te stellen. De Nederlandse wetgever bereidt daartoe de Uitvoeringswet AVG (UAVG) voor. Feitelijk gaat het om modernisering van de wetgeving, die een kans biedt om maatschappelijk vertrouwen in technologie te versterken. Tevens stelt het organisaties in de gelegenheid om de beveiliging van waardevolle gegevens te verbeteren en zo te komen tot een privacyproof werkomgeving. Deze verordening vervangt de Wet bescherming persoonsgegevens (Wbp) en brengt een aantal verplichtingen met zich mee. De AVG is dus een verplichting en wel één die ons in positieve zin uitdaagt om een stevige ambitie uit te spreken ten aanzien van het privacybeschermingsniveau van zowel burgers, ondernemers als medewerkers. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij ons in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met privacygevoelige informatie wordt omgegaan. Deze ambitie heeft een vertaalslag gekregen in de gemeentelijke privacyverordening en is nader uitgewerkt in onze beleidsuitgangspunten, beleid en een governancestructuur. Omdat privacybewustzijn in ons DNA moet zitten om als gemeente Rotterdam werkelijk privacyproof te zijn, hebben wij tevens een vertaalslag gemaakt naar de betekenis hiervan voor onze kernwaarden. Datalekken ontstaan immers vaak door menselijke fouten (een tas met stukken in de metro, verloren usb-sticks, bezorgen van verkeerde post, etc.). AVG-compliance vraagt dan ook een behoorlijke inzet van alle medewerkers maar brengt dan ook het nodige, namelijk de zekerheid voor de burger dat zijn of haar persoonsgegevens bij ons in veilige handen zijn.

1 Privacy

Aanleiding

Binnen de gemeente Rotterdam werken we veel met persoonsgegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed uitvoeren van de gemeentelijke wettelijke taken. Men moet er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Rotterdam is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Directe aanleiding voor dit privacybeleid is de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG[1]), die de huidige privacywetgeving – de Wet bescherming persoonsgegevens (Wbp) – per 25 mei 2018 vervangt. Met de AVG is sprake van een versterking en uitbreiding van privacyrechten en ontstaan er meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens, worden uitgebreid. Een voorbeeld is de bevoegdheid om boetes tot 20 miljoen euro op te leggen. Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy.

De gemeente Rotterdam geeft met dit beleid duidelijk richting aan hoe de organisatie om moet gaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin persoonsgegevens worden verwerkt. Het ontwikkelde beleid is dan ook vooraf concernbreed afgestemd voordat het ter besluitvorming werd aangeboden. Het privacybeleid van de gemeente Rotterdam is in lijn met het algemeen beleid van de gemeenten en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. De AVG is niet van toepassing op verwerkingen die onder de Richtlijn gegevensbescherming opsporing en vervolging[2] vallen. Deze richtlijn moet nog worden geïmplementeerd. Het privacybeleid van de gemeente zal daarom worden geactualiseerd zodra het Rijk de wettekst bekend maakt.

[1] Het wetsvoorstel Uitvoeringswet AVG (UAVG) moet nog worden aangenomen. Na bekendmaking en inwerkingtreding van de Uitvoeringswet kan voor AVG, AVG en UAVG gelezen worden.
[2] Ook wel richtlijn politionele en justitiële samenwerking genoemd.

Leeswijzer
In dit document beschrijven we het concernbrede privacybeleid en verbinden we de strategische beleidsuitgangspunten aan de concrete inbedding binnen de uitvoeringsorganisatie.
In Hoofdstuk 2 gaan we in op de leidende principes, welke afgeleid zijn van de Rotterdamse kernwaarden. Daarmee wordt het kader duidelijk waarin het privacybeleid ingebed is. In Hoofdstuk 3 zetten we het governancemodel, inclusief de bijbehorende overlegstructuur, de instrumenten en het eigenaarschap van instrumenten uiteen. Tot slot gaan we in op de mogelijkheid voor clusters om het beleid indien nodig, clusterspecifiek nader uit te werken.

Het stuk is globaal dan ook op te delen in drie niveaus:
1) Leidende, van de kernwaarden afgeleide principes
2) Beleidskaders en governance
3) Clusterspecifieke uitwerking van het beleid

Om het mogelijk te maken de hoofdstukken ook los van elkaar te lezen komt het incidenteel voor dat begrippen meer dan eens geduid worden.

2 Kernwaarden

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. We handelen hierbij in lijn met onze kernwaarden:

- Samenwerken;
- Verantwoordelijkheid;
- Vertrouwen;
- Resultaatgericht; en
- Openheid.

Samenwerken
Als je ziet dat hulp nodig is, dan bied je die natuurlijk gewoon aan. En als je zelf hulp nodig hebt, vraag er dan om. Dat werkt prettig. Kijk over de grenzen van je eigen organisatie heen. Niet alleen als het nodig is, maar ook als het kan. Werk samen vanuit het besef dat goede resultaten de optelsom zijn van mensen die goed samenwerken. Dat gaat altijd verder dan je eigen belang of dat van je afdeling.

Samenwerken binnen onze gemeente en met organisaties buiten onze gemeente is van essentieel belang voor een optimale dienstverlening. Vanuit die samenwerking oog hebben voor privacy en de bescherming van persoonsgegevens, betekent dat we burgers direct en in begrijpelijke taal melden voor welke rechtmatige, gerechtvaardigde doelen wij hun persoonsgegevens registreren en met elkaar uitwisselen (als dit het geval is).

Verantwoordelijkheid
Afspraak is afspraak. Dus je neemt verantwoordelijkheid voor wat je doet. Je staat voor wat je onderneemt. Daar mogen je collega's je op aanspreken en burgers natuurlijk ook. En omdat je je ook verantwoordelijk voelt, vind je het ook geen probleem om toe te geven als er eens iets misgaat. Omdat je je realiseert dat je werk daar alleen maar beter van wordt.

Verantwoordelijkheid nemen om de privacy te waarborgen van burgers en andere partijen die met de gemeente Rotterdam te maken hebben, betekent dat je hen serieus neemt en dat ook laat zien. Dit kan door zorgvuldig om te gaan met de persoonsgegevens van de betrokkenen en zo nodig anderen erop aan te spreken als zij de vereiste zorgvuldigheid niet voldoende in acht nemen. Door als gemeente voor deze betrokkenen altijd goed bereikbaar en aanspreekbaar te zijn als deze een beroep doen op hun privacy rechten. Maar ook door het direct melden van datalekken, mocht er onverhoopt toch iets zijn misgegaan.

Vertrouwen
Vertrouwen moet je verdienen; van de burgers, je collega's en het management. Het is je taak om door je werk en je manier van omgaan met Rotterdammers en collega's het vertrouwen in de gemeente steeds verder te versterken. De diensten die je levert, komen voort uit wat Rotterdam en haar burgers nodig hebben en de Rotterdammers kunnen er ook op rekenen dat je zorgt voor correcte en consequente handhaving.

Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens in veilige handen zijn. Vertrouwelijkheid en integriteit zijn hierbij de sleutelwoorden. Daarnaast betekent dit dat de gemeente passende organisatorische en technische maatregelen neemt om de privacy te waarborgen.

Resultaatgericht
Gemeente Rotterdam wil op kwaliteit en resultaten kunnen sturen. Niet alleen om de burger goed te kunnen bedienen, maar ook omdat de gemeente een moderne en aantrekkelijke werkgever wil zijn. En die legt de verantwoordelijkheid voor het werk bij haar medewerkers neer. Het is het resultaat dat telt. De gemeente Rotterdam stimuleert de eigen verantwoordelijkheid en het ondernemerschap van jou als medewerker. Er wordt een beroep gedaan op jouw vakmanschap, vanuit het vertrouwen dat jij het beste uit jouw werk wil halen. Andersom biedt het concern je rechtszekerheid en de faciliteiten om jouw eigen ontwikkeling gestalte te geven.

Resultaatgerichtheid als het gaat om privacybescherming, betekent vooral het creëren van meer bewustzijn bij de individuele medewerker. Het bewustzijn dat het borgen van de privacy van de betrokkenen hand in hand gaat met het sturen op kwaliteit en resultaten. Bijvoorbeeld door tijdig te reageren op verzoeken van betrokkenen, maar ook door pro-actief te handelen als de situatie daarom vraagt. Daarnaast betekent het verantwoordelijkheid nemen als regelgeving tekort schiet en dan actie te ondernemen om –waar nodig- zaken alsnog geregeld te krijgen.

Openheid
Je staat open voor de mening van anderen en voor kritiek. Je bent zelf ook open, je deelt je opvattingen en luistert naar die van je collega's van het concern en die van vertegenwoordigers van partners in de stad.

Openheid staat in het kader van privacybescherming voor transparantie. We informeren de burgers op passende wijze, via alle relevante kanalen die daarvoor beschikbaar zijn, over de verwerking van hun gegevens en de mogelijkheid om hun rechten uit te oefenen op het gebied van privacyregelgeving.

Deze principes vormen het raamwerk waarbinnen de in de Privacyverordening Rotterdam 2018 geformuleerde opdracht is uitgewerkt. Deze door de gemeenteraad geformuleerde opdracht behelst een uitwerking te geven aan ten minste de navolgende onderwerpen:

a. De beginselen inzake verwerking van persoonsgegevens;
b. De rechten van betrokkenen;
c. De informatiebeveiliging en voorkomen van datalekken;
d. Het register van verwerkingsactiviteiten;
e. De taken en bevoegdheden van de functionaris voor gegevensbescherming.

Deze opdracht heeft een beslag gekregen in het privacybeleid. In dit beleid laat de gemeente Rotterdam zien op welke manier zij op dagelijkse basis omgaat met privacy, en wat wel en niet verantwoord is. Het beleid is van toepassing op alle verwerkingen binnen de gemeente Rotterdam die onder de AVG vallen.

3 Privacybeleidskader

In relatie tot de clusters en andere beleidsdomeinen
Dit privacybeleid wordt centraal vastgesteld en is van toepassing op alle bestuursorganen van de gemeente; dit voor zover de AVG op de betreffende verwerkingen van toepassing is. Binnen de clusters kan het management op basis van dit beleid, indien zij dit nodig achten, aanvullend beleid formuleren als specifieke processen en procedures bij een cluster dit vereisen. Hierbij kan alleen met toestemming vooraf van de algemeen directeur BCO[3] worden afgeweken van het centraal vastgestelde beleid. De toepassing van het beleid wordt periodiek getoetst. Het privacybeleid werkt tevens door in alle voorkomende beleidsdomeinen.

Organisatie
De verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt (logischerwijze) bij de clusters. Dat betekent ook dat de lijn binnen de clusters zelf wordt aangesproken op het nakomen van de uit het privacybeleid voortvloeiende eisen. Privacy is immers niet een op zichzelf staand iets, maar is onlosmakelijk verbonden met de gemeentelijke diensteverlening. De clusters zorgen ervoor dat zij bij de uitvoering van het beleid worden bijgestaan door professionals op het gebied van privacy.

Verwerkingsverantwoordelijke
In de AVG wordt, sterker dan onder de Wbp het geval was, de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als ‘verwerkingsverantwoordelijken’) om te kunnen aantonen dat zij zich aan de wet houden (accountability). De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het doel van en de middelen voor de verwerking vaststelt.

Het college van burgemeester en wethouders (hierna college van B&W) respectievelijk de burgemeester zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke. Formeel is het college van B&W respectievelijk de burgemeester dan ook verantwoordelijk voor de verwerkingen die onder de reikwijdte van de AVG vallen. De verwerkingen op grond van de richtlijn gegevensbescherming opsporing en vervolging[4] vallen hier niet onder.

De verwerkingsverantwoordelijken zijn verantwoordelijk voor:

- De naleving van de beginselen voor de verwerking van persoonsgegevens.
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd.

[3] Als portefeuillehouder in de concerndirectie is directeur BCO namens de algemeen directeur verantwoordelijk voor de inhoudelijke voorbereiding van besluitvorming op het gebied van privacy.
4 Ook bekend als de richtlijn gegevensbescherming politionele en justitiële samenwerking

Gemeentesecretaris/Verantwoordelijkheid op ambtelijk niveau

De gemeentesecretaris is de algemeen directeur, de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur van het college. Hij of zij vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is dit kader ambtelijk verantwoordelijk.

Concerndirecteur/Verantwoordelijkheid op operationeel niveau

De verantwoordelijkheid voor het voldoen aan de privacywetgeving en beleid voor privacy binnen de clusters ligt bij de clusterdirecteuren. Een clusterdirecteur kan de verantwoordelijkheid voor taken die hierop betrekking hebben op operationeel niveau bij één van zijn MT-leden beleggen. Uitvoeringsgerichte bevoegdheden in dit kader - zoals de beslissing op verzoeken betreffende de uitoefening van rechten en ondertekening van de verwerkersovereenkomsten – worden de clusterdirecteur in mandaat verleend, met de bevoegdheid deze verder in de lijn onder te mandateren tot het niveau van afdelingsmanager.

Proceseigenaar (lijnmanagement)

Binnen de afdelingen zijn de proceseigenaren verantwoordelijk voor de naleving van de privacy wetgeving en het Rotterdamse privacybeleid. De proceseigenaar legt verantwoording af aan de clusterdirectie. De Privacy Officer biedt ondersteuning op het gebied van advisering bij het handelen conform het privacybeleid.

Functionaris voor de gegevensbescherming (FG)

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De FG ziet er op toe dat de gemeente Rotterdam voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy, het privacybeleid en informatiebeveiligingsbeleid. De functie kent een beperkte overlap met de CISO (zie hieronder), die zorg moet dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente te waarborgen. Zie voor de concrete invulling van de functie hoofdstuk governance.

Concern Privacy Officer (CPO) & Privacy Officer (PO)

De rol van de PO is die van adviseur van de concerndirecteur, portefeuillehouder en management van elk cluster/directie. Daarnaast ondersteunt de PO bij het verrichten van privacy impact analyses en overlegt waar nodig met de CPO over nieuwe ontwikkelingen. Per cluster is een PO benoemd. Deze PO is verantwoordelijk voor specifiek aan de cluster/directie gerelateerde kennis en implementatie van privacyvraagstukken.

De CPO is de linking-pin naar directies en clusters en verantwoordelijk voor de behandeling van organisatiebrede privacyvraagstukken en is verantwoordelijk voor het privacy-proces. Verder heeft de CPO een rol in de algemene kennisoverdracht met betrekking tot privacy en het signaleren en implementeren van organisatiebrede privacyvraagstukken. Zie ook hoofdstuk 4 Governancestructuur.

Concern Informatie Security Officer (CISO) en Decentrale Informatie Security Officer (DISO)
De CISO is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern. De CISO stelt kaders op voor informatiebeveiliging en adviseert het bestuur hierover op strategisch niveau. De DISO is gepositioneerd binnen een cluster en legt verantwoording af aan de CISO en de clusterdirectie. Samen houden de CISO en DISO toezicht op de informatiebeveiligingsmaatregelen die een cluster neemt om gegevens, waaronder persoonsgegevens, te beveiligen. De CISO en DISO werken hierbij nauw samen met de FG, CPO en PO's.

Verantwoordingsplicht
De verantwoordingsplicht van de gemeente, ook wel accountability genoemd, brengt met zich mee dat de gemeente niet alleen de regels moet naleven, maar dit ook moet kunnen aantonen. In dit kader neemt de desbetreffende verantwoordelijke de volgende maatregelen:

1. Een actueel en volledig registerverwerkingen en het publiceren van een abstract van het register.
2. Opname in het verwerkingenregister van alle relevante documenten die betrekking hebben op de naleving van de verplichtingen uit de AVG, zoals informatieplicht en de afspraken met verwerkers.
3. Openbaarmaking van het onderhavige privacybeleid.
4. Zorgen voor de aantoonbaarheid van de juiste behandeling van informatie.

Tevens houdt de verantwoordingsplicht in dat de gemeente een register van datalekken die zijn opgetreden bijhoudt en, waar passend, een gegevensbeschermingseffect beoordeling uitvoert.

NB Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.

Rechten van betrokkenen
Binnen het beleid worden de volgende rechten van betrokkenen geborgd:

Recht op informatie
De gemeente verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreffen, heeft de gemeente de plicht om betrokkenen, voor zover deze daar niet reeds van op de hoogte zijn, te informeren over verwerkingen van hun persoonsgegevens. De gemeente verstrekt dan aan betrokkenen informatie over de verwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt.[5] Dit met inachtneming van de beperkingen zoals die neergelegd zijn in wet- en regelgeving. Als gemeente hechten we er belang aan om dit op een eenduidige wijze te doen. Hiertoe ontwikkelen we uitvoeringsbeleid. We actualiseren daarom ook het privacybeleid zodra we besluiten hoe we de taken en verantwoordelijkheden in deze binnen het concern beleggen.

[5] Zie de artikelen 13 en 14 AVG

Een deel van deze te verstrekken informatie is steeds terugkerende informatie zoals de verwerkingsverantwoordelijke, de contactgegevens van de FG en de rechten van betrokkenen. Om volledige informatieverstrekking te bewerkstelligen, maar ook om redenen van eenduidigheid en efficiëntie, is een format vastgesteld voor de informatieplicht waarin de terugkerende informatie al is ingevuld. De clusters vullen dit format in en het wordt gebruikt ter voldoening aan de informatieplicht. Een exemplaar wordt bewaard in het registerverwerkingen.

Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht op correctie
Als de gemeente persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de gemeente om dit te verbeteren. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht om vergeten te worden
Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de gemeente niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

Recht op bezwaar tegen verwerking
Betrokkenen hebben het recht aan de gemeente te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. De gemeente moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Recht op beperking van de verwerking
Het recht op beperking houdt in dat de gemeente de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)
De gemeente is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, de uitoefening van een openbaar gezag, wanneer deze zijn openbare taken uitoefent of aan een wettelijke verplichting voldoet. Desondanks zal de gemeente in voorkomende gevallen voorzieningen treffen in het kader van dataportabiliteit.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling
Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

Uitoefening van rechten
Om gebruik te maken van de bovenstaande rechten kunnen de betrokkenen een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de website van de gemeente ingediend worden. Binnen vier weken beoordeelt de gemeente of het verzoek gerechtvaardigd is. De gemeente laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de gemeente de behandeling van het verzoek met twee maanden verlengt.
De gemeente behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure.

Als het verzoek niet op tijd wordt opgevolgd, deelt de gemeente uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij de gemeente of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

Klachten
Elke betrokkene heeft het recht bij de gemeente een klacht in te dienen of bezwaar te maken tegen de wijze waarop zijn of haar persoonsgegevens worden verwerkt. Voor eenduidige en efficiënte klachtafhandeling verwijst de gemeente naar de centrale klachtenregeling waarin de FG een centrale rol vervult.

Indien naar de mening van de betrokkene de beslissing op een klacht niet tot het gewenste resultaat heeft geleid kan de betrokkene zijn of haar klacht voorleggen aan de gemeentelijke Ombudsman, Meent 106, 3011 JR Rotterdam.[6]

De betrokkene kan zijn of haar klacht of een verzoek tot bemiddeling ook indienen bij de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ 's Gravenhage.

[6] https://www.ombudsmanrotterdam.nl/klacht-indienen

Bewustwording

De clusters zorgen voor voldoende bewustwording bij hun medewerkers op het gebied van privacy. Hierbij dienen zij minimaal op de hoogte te zijn van de privacyregels en de voor hun werkzaamheden relevante bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen. De verantwoordelijkheid voor bewustwording ligt bij de clusters. Er wordt per cluster een awareness plan privacy opgesteld, als onderdeel van het clusterjaarplan, met daarin de jaarlijks terugkerende en eenmalige activiteiten. De clusters worden hierbij ondersteunt door periodiek centraal te organiseren awareness campagnes.

Informatiebeveiliging en Datalekken

Informatiebeveiligingsbeleid

Informatiebeveiliging is de verzamelnaam voor de processen, die de gemeente inricht om de betrouwbaarheid van informatie te beschermen, ook als die zich in gemeentelijke processen of in informatiesystemen bevinden. Het begrip 'informatiebeveiliging' heeft betrekking op:

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Het Informatiebeveiligingsbeleid 2018, dat door het college is vastgesteld, heeft betrekking op alle gemeentelijke processen, waaronder de processen waarin (persoons)gegevens worden verwerkt. De CISO ziet toe op de naleving van dit beleid.

Meldplicht datalekken

Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de gemeente in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken[7] en de getroffen perso(o)n(en) te beschermen.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

[7] Protocol melding en afhandeling datalekken

De plicht tot het melden van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit gemeentelijke bestanden en/of gegevens waarvoor de gemeente verantwoordelijkheid draagt. Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de Autoriteit Persoonsgegevens. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval wordt dit ook aan de betrokkenen gemeld, in eenvoudige en duidelijke taal.

Beveiligingsmaatregelen
Deze (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen. Waar passend omvatten de maatregelen op grond van artikel 32 AVG onder meer het volgende:

a) De pseudonimisering en versleuteling van persoonsgegevens;
b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Wanneer de gemeente persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de gemeente ervoor dat passende beveiligingsmaatregelen (conform het concern informatiebeveiligingsbeleid) worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

Het register van verwerkingsactiviteiten
De functionaris voor gegevensbescherming (FG) houdt namens de verantwoordelijke een register bij, bestemd voor de inschrijving van verwerkingen van persoonsgegevens.
De clusterdirectie draagt, daarin bijgestaan door de PO, zorg voor de inschrijving van de verwerkingen van persoonsgegevens, die binnen het cluster plaatsvinden.

Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:

a. de naam van de verwerking;
b. wie de verantwoordelijke is voor de verwerking;
c. het doel van de verwerking;
d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i. de verwijderingstermijnen die in acht genomen worden;

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten (eventuele verwerkersovereenkomst, model Gegevensbeschermingseffectbeoordeling, privacyprotocol, informatieverplichting). Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de clusterdirectie zorg voor wijziging hiervan in het register en informeert de FG hierover.

Naleving van het beleid

Risico-beheersing (en controle mechanismen)
Vanuit de gedachte van risicobeheersing, neemt de gemeente verschillende maatregelen om de risico's bij de verwerking van persoonsgegevens in kaart te brengen en te verminderen. Hiervoor gelden vier cycli van risicobeheersing:

1. In kaart brengen verwerkingen met persoonsgegevens;
2. Uitvoeren Gegevensbeschermingseffectbeoordelingen, evaluatie van getroffen maatregelen, of formuleren van aanvullende maatregelen;
3. Afleggen verantwoording aan toezichthoudende FG;
4. Periodiek evalueren van privacy incidenten.

De cycli van risicobeheersing worden in de praktijk aan de hand van de hieronder toegelichte controlemechanismen ten uitvoer gebracht.

Gegevensbeschermingseffectbeoordeling [8]
Een Gegevensbeschermingseffectbeoordeling[9] is een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
Een Gegevensbeschermingseffectbeoordeling wordt doorgaans uitgevoerd door de PO, voorafgaand aan de verwerking en bij bestaande verwerkingen, waar sprake is van een gegevensverwerking die een hoog privacyrisico oplevert voor de betrokkenen. Tevens stelt de AP nog een lijst samen voor verwerkingen waarbij een Gegevensbeschermingseffectbeoordeling altijd verplicht is. Of er sprake is van een hoog privacyrisico, toetst de gemeente aan de hand van een Risk Impact Assessment (RIA). De RIA wordt uitgevoerd op het moment dat een van de BIV-classificaties 2 of hoger scoort. Dus naast de Vertrouwelijkheid, waar privacy geraakt wordt, ook op Beschikbaarheid en Integriteit.

[8] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
[9] Ook wel een Data Protection Impact Assessment (DPIA)

Op grond van de AVG is verder in ieder geval sprake van een hoog privacyrisico indien de gemeente:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied;
    - Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;
- Indien wordt voldaan aan twee of meer criteria van de in bijlage 1 opgenomen criteria van de werkgroep van Europese privacy-toezichthouders (WP29).

Voor de Gegegevensbeschermingseffectbeoordeling gelden de volgende kaders:

1. Een Gegevensbeschermingseffectbeoordeling vindt plaats voordat met de betreffende verwerking wordt gestart.
2. Een Gegevensbeschermingseffectbeoordeling wordt na maximaal 3 jaar herhaald ter evaluatie, alsmede bij wijzigingen waardoor de risico's van de verwerking toenemen.
3. Bij het uitvoeren van een Gegevensbeschermingseffectbeoordeling wordt de FG altijd geïnformeerd.
4. De clusterdirectie ziet toe op het nemen van maatregelen die blijkens de Gegevensbeschermingseffectbeoordeling nodig zijn om de risico's te verkleinen.
5. Het resultaat van de Gegevensbeschermingseffectbeoordeling en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het registerverwerkingen.
6. Indien de clusterdirectie niet in staat is om voldoende maatregelen te treffen om de risico's te beperken, wordt de AP om een voorafgaande raadpleging gevraagd.
7. Gegevensbeschermingseffectbeoordelingen die binnen de gemeente worden uitgevoerd vinden plaats volgens de gemeentelijke standaard bepaalt door de FG.

Overgangsregeling

Voor verwerkingen met een hoog privacyrisico die voor 25 mei 2018 al bestonden is een Gegevensbeschermingseffectbeoordeling na deze datum verplicht indien:

1. De verwerking verandert, bijvoorbeeld door nieuwe technologie of wijziging van doel;
2. Het risico verandert;
3. De omgeving verandert, bijvoorbeeld door maatschappelijke veranderingen.

Deze overgangstermijn eindigt op 25 mei 2021.

Privacyprotocol
De clusterdirectie stelt indien nodig aanvullend een specifiek privacyprotocol vast voor een bepaald proces waarbij persoonsgegevens worden verwerkt, indien:

1. De verwerking blijkens de Gegevensbeschermingseffectbeoordeling extra privacywaarborgen behoeft; of
2. De PO daartoe adviseert.

Het college van B&W stelt een model vast, waaraan het privacyprotocol dient te voldoen.

De FG toetst het privacyprotocol op rechtmatigheid en volledigheid en neemt dit op in de registerverwerkingen.

Privacy door ontwerp (privacy by design)
Privacy door ontwerp omvat vier uitgangspunten:

- Minimaal gebruik van persoonsgegevens
- Passende bescherming van de persoonsgegevens
- Gerechtvaardigd gebruik van persoonsgegevens
- Borg de rechten van betrokkenen

Dit betekent dat bij het ontwerpen van producten en/of diensten, het inkopen van systemen en bij de uitvoering van haar werkzaamheden de gemeente de volgende uitganspunten hanteert:

Minimaal gebruik van persoonsgegevens:

- De gemeente verzamelt (of vraagt om) niet meer gegevens dan noodzakelijk of juridisch mogelijk;
- De gemeente verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel;
- Bij configuratie van systemen kiest de gemeente altijd voor de privacy-vriendelijke variant (privacy by default);
- De informatie die de gemeente verwerkt is correct en actueel;
- De gemeente maakt geen onnodige kopieën;
- De gemeente verwijdert wat niet meer nodig is.

Passende bescherming:

- De gemeente slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag;
- De gemeente beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben;
- De gemeente beschermt persoonsgegevens door o.a. het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid verminderd.

Als uitgangspunt kiest de gemeente voor technische maatregelen om de privacy door ontwerp te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de gemeente naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met informatiebeveiliging uitgewerkt

Privacy bij ontwerp dient organisatorisch geborgd te zijn om de gemeente te beschermen tegen het in strijd werken met wet en regelgeving. Binnen de gemeente worden vier relevante processen onderscheiden die zich bezighouden met het ontwerp proces van producten en diensten:

1. Demand-supply proces;
2. Architectuurproces;
3. Inkoopproces;
4. Contractproces.

Privacy dient bij alle vier de processen een cruciaal onderdeel te zijn, dat toe ziet op het betrekken van de PO en CISO/DISO.

Inschakeling verwerkers, verwerkersovereenkomst

Verwerkers
Wanneer de gemeente een partij inschakelt om ten behoeve van de gemeente persoonsgegevens te verwerken en het verwerken van de persoonsgegevens de *primaire* taak is van deze partij, kan deze partij worden beschouwd als verwerker. De gemeente schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst en worden voordat de dienstverlening aanvangt en daarna periodiek of steekproefsgewijs getoetst.

De concerndirectie stelt het model vast, waar de standaardverwerkersovereenkomst minimaal aan moet voldoen. Hierbij geldt geen overgangsregeling; de standaardverwerkersovereenkomst zal zo vroeg mogelijk in gebruik worden genomen om te anticiperen op de inwerkingtreding van de AVG per 25 mei 2018.

Andere afspraken
In voorkomende gevallen treedt de gemeente Rotterdam op als verwerker voor derden. Hierbij zijn deze derden de Verwerkingsverantwoordelijke. De gemeente streeft er in deze gevallen naar voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen voor gelijksoortige verwerkingen. De gemeente biedt daarbij aan de Verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen. De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de gemeente Rotterdam aanvangt.

Verder kan het voorkomen dat de gemeente een andere partij inschakelt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld. Ook dan maakt de gemeente passende afspraken. In dat geval zal de gemeente een overeenkomst sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectieve verantwoordelijkheden worden vastgelegd.

Camerabeelden

Camerabeelden binnen de gemeentelijke organisatie
De gemeente past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera's,

burgerloketten en wachtkamers. Voor elke registratie van camerabeelden bepaalt de gemeente of en hoe lang deze worden bewaard.

Afwijken van beleid
Afwijken van het beleid is in beginsel niet toegestaan.

Dit privacybeleid treedt in werking na vaststelling door de verantwoordelijke, de burgemeester en het college van burgemeesters en wethouders. Het beleid wordt elk jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via [medium]. De meest actuele versie van het beleid is te vinden op [link]

Aldus vastgesteld door burgemeester, college van burgemeester en wethouders van gemeente Rotterdam op [datum],
[Naam. Functie] [Naam. Functie]
[Handtekening] [Handtekening]