STEDELIJK PRIVACYKADER WET POLITIEGEGEVENS GEMEENTE AMSTERDAM

STEDELIJK PRIVACY KADER WET POLITIEGEGEVENS GEMEENTE AMSTERDAM 1
Inleiding en context 2
Governance 2
Verantwoordelijkheden 3
Kaders en sjablonen 3
Toezicht 3
Informatiebeveiliging 3
Informatiebeheer en bewaartermijnen 4
Inhoudelijke uitgangspunten 5
Verstrekken en ter beschikking stellen van politiegegevens 5
Technische inrichting applicaties 6
Organisatorische inrichting 7
Bevoegdheden borgen 7
Aanstellen bevoegd functionaris 7
Toepassen transparantie-vereisten 8
Uitoefenen rechten van betrokkenen 8
Quality Assurance: privacy by design and default borgen 9
Register van verwerkingen politiegegevens bijhouden 9
Register van verstrekkingen van politiegegevens bijhouden 9
Data Protection Impact Assessment (DPIA) uitvoeren 9
Auditcyclus uitvoeren 10

Inleiding en context

De visie van de gemeente Amsterdam op de steeds verder gaande digitalisering van de samenleving is neergelegd in de Agenda Digitale Stad 2023-2026. Hierin is ook weergegeven hoe belangrijk het is bij datagebruik en verzameling van data voortdurend aandacht te blijven geven aan ethische aspecten, de bescherming van de persoonlijke levenssfeer, de gegevensbescherming en de naleving van geldende wet- en regelgeving. Het voorliggende stuk is primair bedoeld als een intern gemeentelijk beleid, waarin de gemeentelijke organisatie de uitgangspunten en kaders die gelden bij de verwerking van politiegegevens vaststelt. Het biedt daarmee een handelingskader voor de ambtelijke organisatie en vervult hiermee een verplichting vanuit de Wet politiegegevens (Wpg)

Veel handhavers binnen de gemeente Amsterdam zijn aangesteld als buitengewoon opsporingsambtenaar (boa) en toezichthouder. Wanneer de handhaver daadwerkelijk optreedt als boa, valt de verwerking van persoonsgegevens onder de Wpg. De bevoegdheden van boa's zijn onderverdeeld in verschillende domeinen. Persoonsgegevens die binnen de reikwijdte van de Wpg vallen heten politiegegevens. Wat politiegegevens zijn is gedefinieerd in artikel 1 van de Wpg en de reikwijdte voor boa's is vastgelegd in het Besluit boa politiegegevens.

Het voorliggende stuk is bedoeld als intern gemeentelijk kader waarin de specifieke uitgangspunten en algemeen te volgen procedures bij de verwerking van politiegegevens op grond van de Wpg zijn vastgesteld. De onderdelen van het onderstaande beleid vloeien dan ook voort vanuit de verplichtingen de Wpg. De normen die uit de Wpg voortvloeien zijn grotendeels gelijk aan die uit de Algemene Verordening Gegevensbescherming (AVG). Dit Wpg kader is hiermee dan ook aanvullend op het "Stedelijk kader verwerken persoonsgegevens", waar het bijvoorbeeld de vastgestelde taken en verantwoordelijkheden betreft.

De wet- en regelgeving die de gegevensbescherming met betrekking tot politiegegevens reguleert, is verdeeld over;

- de Wet Politiegegevens (Wpg),
- het Besluit politiegegevens (Bpg),
- het Besluit boa politiegegevens (Bboapg),
- de Beleidsregels boa,
- het normenkader voor de privacy audit Wpg van NOREA. NOREA is de Beroepsorganisatie van IT-auditors in Nederland. Het NOREA normenkader is landelijk leidend bij de audits op de Wpg.

Niet alle directies van de gemeente verwerken politiegegevens. De lijndirecties waar boa's zijn aangesteld doen dat per definitie wel. Ook zijn er verschillende lijndirecties die gegevens ontvangen hebben die eerst ooit door boa's (of door de politie) zijn verzameld. Die verwerken dan (ex)politiegegevens. Hier zijn ook regels aan verbonden.

Hieronder wordt eerst de governance van de Wpg binnen de gemeente beschreven, waarna we de inhoudelijke uitgangspunten benoemen die volgen uit de wet. Vervolgens wordt ingegaan op de technische vereisten op de applicaties die politiegegevens verwerken om af te sluiten met de manier waarop we organisatorisch invulling geven aan de vereisten.

Governance

De uitgangspunten voor het verwerken van politiegegevens vloeien rechtstreeks voort uit de wetgeving en moeten in de lijndirectie(s) geborgd. Daarbij is ondersteuning en advies van de

stedelijke coördinator en Privacy Officer Wet Politiegegevens aanwezig, hierna te noemen “Privacy Officer Wpg”. De Privacy Officer Wpg coördineert de werkzaamheden waar gewenst door de lijndirecties en informeert de medewerkers van de lijndirectie over de vereisten van de Wpg en denkt mee over oplossingen en maatregelen.

De Privacy Officer Wpg toetst tevens of de maatregelen in de lijndirectie voldoen aan het beleids- en wettelijk kader, de procedures en de stedelijke hulpmiddelen en sjablonen.

Verantwoordelijkheden

- Net als bij de AVG governance, blijft de lijndirectie waar politiegegevens worden verwerkt zelf verantwoordelijk voor het juist volgen van het beleids- en wettelijk kader. De directeur van de lijndirectie is gemandateerd verwerkingsverantwoordelijke, net als onder de AVG. De lijndirectie stelt ten minste één functionaris aan die belast is met naleving van de Wpg. Deze functionaris treedt op als contactpersoon voor de Privacy Officer Wpg.
- Wanneer in een lijndirectie verwerkingen plaatsvinden met als grondslag artikel 9 Wpg (‘gerichte opsporing’), wordt een Bevoegd Functionaris aangesteld door de lijndirectie. De Bevoegd Functionaris is de ‘hoeder’ van de gegevens die op grond van artikel 9 Wpg worden verwerkt. Deze rol wordt hieronder nader toegelicht.
- Waar de Privacy Officer Wpg kansen ziet voor verbetering door lijndirectieoverstijgende samenwerking, legt deze dit de lijndirecties voor. De lijndirecties blijven zelf verantwoordelijk of zij eventuele adviezen hierover overnemen.
- Wanneer een verwerking van politiegegevens voor hetzelfde doel lijndirectieoverstijgend plaats vindt, zijn de lijndirecties gedeeld verantwoordelijk. Wanneer een lijndirectie politiegegevens die door een andere lijndirectie zijn verzameld, hergebruikt voor een ander doel, is elke lijndirectie verantwoordelijk voor de juiste inrichting van de gegevensverwerking voor het eigen doel.

Kaders en sjablonen

De kaders voor de gegevensverwerking, die zijn vastgesteld in de Quality Assurance Acceptatiecriteria (QAA), en bestaan uit de sjablonen en instrumenten die gebruikt worden voor privacy producten, worden vastgesteld en voor gebruik geleverd door de vakgroep Digitale Rechten, Ethiek en Privacy als onderdeel van de directie Digitale Strategie & Informatie (DS&I). Waar van toepassing, zijn deze aangepast aan de specifieke verplichtingen vanuit de Wpg. De Privacy Officer Wpg ondersteunt de directies bij het gebruik van deze sjablonen en bewaakt het kader.

Toezicht

Intern toezicht en advies is belegd bij de Functionaris Gegevensbescherming (FG). De FG is specifiek voor de Wpg aangesteld, naast een aanstelling voor de AVG. Taken en bevoegdheden van de FG zijn omschreven in artikel 36 Wpg.

Informatiebeveiliging

Informatiebeveiliging wordt binnen dit beleidskader niet apart behandeld, omdat ten aanzien van de Wpg hetzelfde beleid geldig is als wat gevolgd wordt voor de AVG-verwerkingen. Hierbij wordt verwezen naar het Stedelijk kader Informatiebeveiliging Gemeente Amsterdam 2020.

Wel zijn er Wpg specifieke eisen die worden gesteld aan de applicaties waarin politiegegevens worden verwerkt die voortkomen uit de Wpg zelf (artikel 32a, logging) en het normenkader dat de NOREA hanteert bij de audits. De gemeente toetst in elke Data Protection Impact Assessment (DPIA) waarbij politiegegevens worden verwerkt of de systemen en processen voldoen aan de op dat

moment geldende specifieke informatiebeveiligingseisen op het gebied van de Wpg. Over deze inrichting volgt hieronder meer.

Informatiebeheer en bewaartermijnen

Hoe lang politiegegevens bewaard mogen worden is onder de Wpg afhankelijk van in welk kader ze verzameld zijn. Hierin is een verschil in gegevens die verzameld zijn in het kader van artikel 8, 9 of 13 Wpg. Onder deze artikelen verzameld de gemeente politiegegevens voor verschillende doeleinden.

In het register van verwerkingen voor politiegegevens (hieronder beschreven) is de grondslag en het artikel te vinden te vinden waaronder de politiegegevens vallen, waarmee ook de bewaartermijn is gedefinieerd.

De Wpg kent een aantal fases van informatiegebruik die in de verschillende applicaties moeten zijn geborgd.

Dit is voor artikel 8-verwerkingen van politiegegevens:

- Ruime toegang: een jaar lang de mogelijkheid om te bladeren en vervolgens;
- Gerichte toegang: vier jaar (alleen) de mogelijkheid tot gericht zoeken; .
- Bewaartermijn: de gegevens mogen na vijf jaar niet meer raadpleegbaar zijn behalve voor audits, onderzoeken van toezichthouders en het afhandelen van klachten. De Wpg noemt dit in artikel 14 “verwijderen”.
- Vernietigen: tien jaar vanaf het begin van de verwerking dienen de gegevens definitief vernietigd te zijn, tenzij er op basis van de archiefwet een uitzondering is gemaakt.[1] Voor artikel 9-verwerkingen:
- Aanmelden: een artikel 9-verwerking dient binnen één week te worden goedgekeurd door een Bevoegd Functionaris.
- Actief: tot uitspraak of verjaring. Het gaat bij artikel 9 om “gerichte opsporing”: het dossier dient dan ook actief te blijven tot er een afdoening is van het doel. Dat betekent in de praktijk het moment dat er een uitspraak is in de zaak (schuldig of onschuldig) dan wel de zaak geseponeerd is. Vanaf dat moment wordt het dossier gesloten.
- Hergebruik: beschikbaar voor zes maanden. In het geval daar noodzaak toe is, in verband met een opsporing van strafbare feiten, kan het dossier nog in het eerste half jaar na sluiting worden heropend, maar alleen na toestemming van de Bevoegd Functionaris.
- Bewaren gesloten dossier: een hierna gesloten dossier wordt vijf jaar bewaard ten behoeve van audits, onderzoeken van toezichthouders en klachten, en daarna vernietigd. Daarbij geldt dezelfde uitzondering voor cultureel erfgoed en historisch onderzoek.

Voor artikel 13-verwerkingen:

- Artikel 13-verwerkingen zijn verdere verwerkingen van onder artikel 8 en artikel 9 verzamelde politiegegevens ten behoeve van een ondersteunende taak, in de regel in een

---

- [1] Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats. Daarbij worden met toepassing van artikel 15 van de Archiefwet 1995 beperkingen aan de openbaarheid gesteld.

groter (landelijk) samenwerkingsverband. De bewaartermijnen die gelden onder artikel 8 en artikel 9 blijven voor deze gegevens leidend. Artikel 13 kent geen eigen bewaartermijn.

Inhoudelijke uitgangspunten

Verstrekken en ter beschikking stellen van politiegegevens

De Wpg maakt een onderscheid tussen het *ter beschikking stellen* van politiegegevens en het *verstrekken* ervan. Binnen het domein van de reikwijdte van de Wpg wordt gesproken over ter beschikking stellen van politiegegevens. Wanneer gegevens de reikwijdte van de Wpg verlaten doordat de partner waaraan gegevens worden doorgegeven onder een andere wetgeving voor gegevensbescherming valt, is er sprake van verstrekken.

Er wordt een "stedelijk kader uitwisseling van politiegegevens" opgesteld, inclusief een sjabloon voor een register van verstrekkingen. De procedure biedt het kader en geeft inzicht in hoe de rechtmatigheid kan worden bewaakt. Het kader wordt, in overleg met de lijndirecties die boa's hebben aangesteld, vastgesteld door de vakgroepmanager Digitale Rechten, Ethiek en Privacy.

In zijn algemeenheid geldt bij het ter beschikking stellen van politiegegevens:

- Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met de partijen die een opsporingsbevoegdheid hebben ('ja, tenzij').
- Informatie over of een persoon en/of registratie in het bestandsysteem voorkomt, kan geautomatiseerd worden gedeeld, artikel 9 gegevens uitgezonderd.
- Artikel 9 gegevens worden alleen ter beschikking gesteld na toestemming van de Bevoegd Functionaris.
- Wanneer de samenwerkende partner in het politiedomein ook de inhoudelijke gegevens van een dossier wenst, wordt altijd een afweging gemaakt van proportionaliteit, subsidiariteit en noodzakelijkheid alvorens deze gegevens ter beschikking worden gesteld. Bij artikel 8 gegevens wordt de afweging door de lijndirectie gemaakt en vastgesteld. Bij artikel 9 gegevens wordt de afweging door een Bevoegd Functionaris gemaakt. De Privacy Officer Wpg kan adviseren en ondersteunen.

Bij het verstrekken van politiegegevens:

- Gaat het om het delen van gegevens met organisaties en personen zónder opsporingsbevoegdheid. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt voor zover dit *noodzakelijk* is voor de doelen die in de wet- en regelgeving van de Wpg zijn genoemd, en er een Wpg-grondslag is voor verstrekking waarbij aan de daarbij behorende randvoorwaarden is voldaan ('nee, tenzij');
- Moet er worden voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt met goedkeuring door het 'bevoegd gezag'[2], en

[2] Het 'bevoegd gezag' is feitelijk het orgaan dat bevoegd is tot de bepaalde politietaak. Bij handhaving van de rechtsorde, waar de bevoegdheid van de boa ligt, is dat het Openbaar Ministerie. Bij handhaving van Openbare Orde en Veiligheid is dat de burgemeester, wanneer deze de politie voor die taak gebruikt (openbare orde handhaven is géén boa taak!).

- Moet de ontvanger gewezen worden op de geheimhoudingsplicht en de verplichting eventuele onjuistheden terug te melden. Daarbij moet de gemeente vervolgens weer ketenpartners informeren.

Het zorgvuldig omgaan met persoonsgegevens is mensenwerk. Het bewustzijn van boa's over hun verantwoordelijkheid hierin wordt voortdurend aangescherpt, en zij worden in staat gesteld de juiste kennis op te doen. Zo worden risico's verkleind en veilig en verantwoord gedrag aangemoedigd.

- Er wordt een stedelijk kader uitwisseling van politiegegevens opgesteld, inclusief een sjabloon voor een register van verstrekkingen. Dit kader biedt het handelingsperspectief en geeft inzicht in hoe de rechtmatigheid kan worden bewaakt vanuit de werkpraktijk. Uitgangspunt is dat verstrekkingen per organisatie worden bijgehouden in een stedelijk door de Privacy Officer Wpg te onderhouden register, waarvoor deze van informatie wordt voorzien door de lijndirecties. Individuele verstrekkingen aan structurele partners worden voorzien van een audittrail door de verplichte logging in de applicaties.
- De gemeente geeft invulling aan de verplichting dat opsporingsambtenaren voldoende kennis moeten hebben op het gebied van veilige en verantwoorde gegevensverwerking. Hiervoor is een terugkerende trainingsmethode ingericht waarmee ook getoetst kan worden dat/of de boa's deze training hebben gevolgd. Afhankelijk van de omvang en complexiteit van de gegevensverwerking vult elke lijndirectie waar boa's werken deze verantwoordelijkheid binnen de kaders van wet- en regelgeving in.Ontvangen van politiegegevens

Bij het ontvangen van politiegegevens gelden de volgende voorwaarden:

- Er is onderscheid tussen het ontvangen van gegevens door de Boa's in het kader van hun opsporingsbevoegheid (Wpg-regime) of het ontvangen van politiegegevens in het bestuursrechtelijk domein.
- Bepaal onder welk verwerkingsregime de ontvangen gegevens vallen in de verwerking bij de gemeente Amsterdam.
- Waarborg de geheimhouding wanneer de ontvangen Wpg gegevens verder worden verwerkt in het AVG-domein. Daarbij geldt dat ex-politiegegevens herkenbaar moeten zijn in de systemen.
- Maak een afweging bij ontvangst van inzageverzoeken of afstemming noodzakelijk is met de oorspronkelijke verstrekker van de politiegegevens. Dit is nodig om de geheimhouding te waarborgen.

Technische inrichting applicaties

- De hierna genoemde verplichtingen uit de Wpg zijn geborgd binnen de applicaties van de gemeente waarin politiegegevens worden verwerkt, aanvullend op de bestaande eisen voor het ontwerp:Er is een afscheiding in de applicaties en het gegevensbeheer van politiegegevens. Deze zijn als zodanig herkenbaar. Bovendien is vermeld of gegevens worden verwerkt onder de grondslag van artikel 8, 9 of 13 Wpg;
- Er is in de dossiers een scheiding aangebracht tussen waarneming, feit en oordeel;
- Er wordt in de dossiers onderscheid gemaakt tussen categorieën betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Het doel van het boa/politieonderzoek is opgenomen in de applicatie of moet worden ingevoerd, waaronder het strafbare feit waarvan betrokkene verdacht wordt. Dit kan indien van toepassing door middel van de feitcodes uit de database van het OM;

- Documentatie van de verstrekkingen (het delen van gegevens buiten het politiedomein) is op orde met daarbij de datum en tijd, ontvanger, redenen en de doorgegeven gegevens;
- Er wordt geen gebruik gemaakt van (sub)verwerkers buiten de EER.;
- Bij doorgifte van gegevens aan verwerkingsverantwoordelijken in derde landen buiten de EER wordt onderscheid gemaakt tussen ter beschikking stellingen aan andere opsporingsdiensten en verstrekkingen aan partijen buiten het politiedomein;
- Bij doorgifte aan verwerkingsverantwoordelijken in derde landen buiten de EER wordt deze doorgifte op juistheid en rechtmatigheid getoetst door een privacy- of compliance officer en de doorgifte wordt vastgelegd;
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens;
- Er vinden in de lijndirectie kwaliteitscontroles plaats op doelbinding, noodzakelijkheid, juistheid, volledigheid en beschikbaarheid van politiegegevens;
- Er wordt voldaan aan de specifieke eisen die worden gesteld aan de informatiebeveiliging voor politiegegevens zoals omschreven in het NOREA-normenkader voor de Wpg audits. Dit normenkader is hierin leidend.
- Bewaartermijnen worden Wpg conform geautomatiseerd gehandhaafd binnen de Wpg hoofdapplicatie.
- De verschillende fases van gebruik in de bestaanscyclus van politiegegevens zoals omschreven in artikel 14 Wpg (zie: “bewaartermijnen”) vereisen dat in de autorisatie van applicaties gegevens afgeschermd moeten kunnen worden.

De instellingen van applicaties dwingen zoveel mogelijk een juist gebruik af, doordat de standaard instellingen die gelden voor een gebruiker (boa) zijn afgestemd op diens bevoegdheden. Bij aanschaf of wijzigingen in systemen worden bovenstaande uitgangspunten toegepast (privacy door ontwerp en standaardinstellingen).

Wanneer het onvermijdelijk is dat personeel met een ondersteunende taak, maar zonder opsporingsbevoegdheid, toegang heeft tot politiegegevens worden zij hiervoor gemachtigd door de (gemandateerd) verwerkingsverantwoordelijke. Hun aantal dient tot een minimum beperkt te blijven. In de machtigingen wordt vastgelegd het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen. [3]

Organisatorische inrichting

Bevoegdheden borgen

Er zijn procedures in de lijndirecties waar boa’s werkzaam zijn om te borgen dat boa’s bevoegd zijn voor het handhavingsdomein waarvoor zij zijn aangesteld. Hierbij is aandacht voor monitoring van de getuigschriften, bij- en nascholing en de categoriale beschikkingen.

- Voor de monitoring van bevoegdheden stelt elke lijndirectie die politiegegevens verwerkt een eigen procedure op.

Aanstellen bevoegd functionaris

Het is noodzakelijk om vast te stellen of er sprake is van gerichte opsporing zoals bedoeld in artikel 9 Wpg. Wanneer in een lijndirectie verwerkingen plaatsvinden met als grondslag artikel 9 Wpg (‘gerichte

[3] Dit volgt uit Bpgboa art. 3.

opsporing'), wordt een Bevoegd Functionaris aangesteld. De Bevoegd Functionaris is de 'hoeder' van de gegevens die op grond van artikel 9 Wpg worden verwerkt. Dit is een persoon met aantoonbaar voldoende kennis en vaardigheden over dit type gegevens, zowel vanuit het oogpunt van de gegevensbescherming (kennis van de Wpg) als vanuit het vakinhoudelijke oogpunt (kennis van het type opsporing).

Het kan beleid zijn van een lijndirectie waar boa's zijn aangesteld om geen artikel 9 dossiers te behandelen, maar deze over te dragen aan een andere opsporingsinstantie, zoals de politie. Wanneer dit het geval is, wordt dit duidelijk in het handhavingsbeleid van de directie omschreven. De boa's werkzaam bij die lijndirectie worden geschoold om artikel 9 verwerkingen te herkennen, zodat voorkomen kan worden dat boa's 'onbewust' artikel 9 verwerkingen uitvoeren. De FG kan steekproefsgewijs controles uitvoeren om toezicht te houden op de uitvoering van dat beleid.

De Bevoegd Functionaris kan zich laten ondersteunen en van advies voorzien door de Privacy Officer Wpg.

- De lijndirectie bepaalt wie als Bevoegd Functionaris wordt aangesteld, en stelt een protocol vast waarin diens taken worden beschreven en de procedure hoe diens taken procesmatig worden ingebed in de dagelijkse werkzaamheden. Tevens zorgt de lijndirectie dat de Bevoegd Functionaris in de applicatie waarin politiegegevens worden verwerkt, zijn/haar rol kan vervullen.

Toepassen transparantie-vereisten

Mensen over wie wij politiegegevens verwerken hebben recht op informatie. Deze wordt langs dezelfde weg als bij de AVG ingevuld, dat wil zeggen, door middel van het publiceren van privacy verklaringen en het register van verwerkingen. De Vakgroepmanager Digitale Rechten, Ethiek en Privacy heeft hiervoor een kader vastgesteld in de vorm van een sjabloon. De Privacy Officer Wpg doet voorstellen aan de lijndirectie voor de invulling van de verklaring, het is echter de verwerkende lijndirectie die inhoudelijk verantwoordelijk blijft voor de privacyverklaring.

Er kunnen nog andere middelen worden ingezet in het kader van transparantie. Noodzaak daarvoor doet zich zeker voor in gevallen waarin er sprake is van een overgang van bestuursrecht (AVG) naar strafrecht (Wpg). De betrokkene dient immers te weten wat diens rechten en plichten zijn. Wanneer hier reden voor is, zoekt de lijndirectie in overleg met de Privacy Officer Wpg naar een laagdrempelige, transparante en werkbare oplossing.

Uitoefenen rechten van betrokkenen

Betrokkenen hebben onder de Wpg rechten, zoals inzage en rectificatie, maar deze rechten zijn anders gedefinieerd dan onder de AVG. De formaliteiten wanneer betrokkenen hun rechten uitoefenen, zijn grotendeels gelijk, met uitzondering van de behandeltermijnen en de uitzonderingsgronden die de verwerkingsverantwoordelijke heeft om niet aan een verzoek te voldoen.

Daarom is de afhandeling van Wpg verzoeken op een grotendeels hetzelfde, maar enigszins afwijkende manier ingericht als de afhandeling van verzoeken onder de AVG.

- De afhandeling van verzoeken van betrokkenen die hun rechten op basis van de Wpg willen uitoefenen, volgt in hoofdlijnen hetzelfde proces als onder de AVG. Afwijkingen zijn omschreven in een aanvullende "procedure afhandeling verzoeken van betrokkenen Wpg". Deze is opgesteld door de privacy officer Wpg in overleg met het Loket Persoonsgegevens, dat de aanvragen ontvangt en in behandeling neemt, en vastgesteld door de Vakgroepmanager Digitale Rechten, Ethiek & Privacy van de directie DS&I. Hierin is ondermeer opgenomen dat bij Wpg verzoeken het advies van de Privacy Officer Wpg wordt ingewonnen.

Quality Assurance: privacy by design and default borgen

Om de eisen uit de Wpg met betrekking tot privacy by design and default te borgen, zal een lijndirectie die een nieuwe verwerking van politiegegevens wil toepassen of een bestaande verwerking wijzigt, het 'Quality Assurance' traject doorlopen. Hierin zijn ook voor de Wpg specifiek verplichte stappen aanwezig, waarbij de Privacy Officer Wpg kan ondersteunen bij het uitvoeren van de diverse analyses.

Register van verwerkingen politiegegevens bijhouden

Er is een register van verwerkingen van politiegegevens, dat afzonderlijk van het AVG register is te raadplegen en dat de relaties met verwante verwerkingen in het bestuurlijk domein (AVG) toont. Hiervoor wordt dezelfde procedure gevolgd als in het AVG-beleid.

- Lijndirecties en de Privacy Officer Wpg werken samen bij het op orde houden van het register van verwerkingen. Hierin worden dezelfde structuren gebruikt als bij het AVG-register.
- De Vakgroepmanager Digitale Rechten, Ethiek en Privacy stelt een stedelijk sjabloon vast voor het register van verwerkingen dat aan de specifieke Wpg vereisten voldoet en stelt dit waar nodig bij.Dit op voordracht van de Privacy Officer Wpg.

Register van verstrekkingen van politiegegevens bijhouden

In het register van verstrekkingen van politiegegevens moet worden bijgehouden, om aan de documentatieplicht van de Wpg te voldoen, welke verstrekkingen plaats vinden vanuit het Wpg regime (opsporingsdomein) aan andere domeinen, waar de AVG of Wsjg (Wet Justitiële en Strafvorderlijke gegevens) van toepassing is.

De verstrekkingen worden op twee niveaus gedocumenteerd.

- Op het niveau van organisaties waaraan verstrekt wordt. Elke directie informeert de Privacy Officer Wpg over bestaande, nieuwe of vervallen structurele verstrekkingen. Deze houdt een overzicht bij in het stedelijke register van verstrekkingen. Deze procedure is verder beschreven in het "stedelijk kader uitwisseling politiegegevens".
- Op het niveau van de feitelijke verstrekking van data, doordat applicaties zo zijn ingericht dat elke verstrekking in de logdata is terug te vinden.

Data Protection Impact Assessment (DPIA) uitvoeren

Of een DPIA moet worden uitgevoerd, kan worden vastgesteld aan de hand van een Privacy Quick Scan. Voor verwerkingen die plaatsvinden onder de Wpg is een apart sjabloon beschikbaar. Dit sjabloon wordt vastgesteld door de Vakgroepmanager Digitale Rechten, Ethiek en Privacy.

De lijndirectie voert de DPIA voor de Wpg uit, en betrekt de Privacy Officer Wpg bij de uitvoering. Wanneer er ook gegevens in een proces worden verwerkt die onder de AVG vallen, wordt van geval tot geval bekeken of één DPIA kan volstaan of dat twee verschillende templates moeten worden doorlopen.

De DPIA kan pas vastgesteld worden wanneer deze is voorgelegd ter advies aan de Functionaris Gegevensbescherming (FG). Diens advies wordt los toegevoegd als bijlage. In de regel wordt het advies verder verwerkt in de DPIA, en wanneer advies niet wordt opgevolgd, wordt dit gemotiveerd ('comply or explain'). De DPIA wordt dan ter vaststelling van de maatregelen dan wel acceptatie van restrisico's voorgelegd aan de lijndirectie, zijnde gemandateerd verwerkingsverantwoordelijke.

- De lijndirecties voeren zelf de DPIA uit, ondersteund door de Privacy Officer Wpg. Daarbij geldt hetzelfde proces en dezelfde werkwijze als bij de AVG.
- De DPIA's vloeien voort uit en maken integraal onderdeel uit van de Quality Assurance Acceptatiecriteria. Dit betekent ook dat zij elke drie jaar worden geactualiseerd, of eerder wanneer er een substantiële wijziging in het proces plaatsvindt.

Auditcyclus uitvoeren

Er geldt een verplichting tot het uitvoeren van privacy audits zoals vastgelegd in de “Regeling periodieke audit politiegegevens” vastgesteld door de minister van Justitie en Veiligheid. De rapportage die uit de vierjaarlijkse externe audit voortvloeit wordt verstrekt aan de Autoriteit Persoonsgegevens. Wanneer er een verplichting is tot een hercontrole, wordt deze ook ingezonden. De externe privacy/Wpg audit wordt altijd verricht door een geregistreerde (NOREA) auditor. Er vinden ook elk jaar interne audits plaats, waarbij op onderdelen een audit wordt uitgevoerd.

- Bij de Wpg auditcyclus is de opdrachtgever voor de externe audit de gemeentesecretaris.
- Bij de Wpg auditcyclus is de opdrachtgever voor interne audits de controller en wordt uitgevoerd door de afdeling Interne Audit & Onderzoek van de directie Middelen en Controls (DMC).
- De directeur van een directie waar Wpg verwerkingen plaats vinden en die als (gemandateerd) verwerkingsverantwoordelijke optreedt is auditee bij de audits en verantwoordelijk voor het aanleveren van bewijsmateriaal en het informeren van de auditor. De Privacy Officer Wpg treedt hierbij ondersteunend en coördinerend op.
- De Privacy Officer Wpg voorziet de CIO, gemeentesecretaris en de directie DMC van advies over de auditcyclus. De Privacy Officer Wpg verzamelt informatie over de planning van interne audits door directie DMC en de externe audits door de ACAM, en coördineert in overleg deze audits in een stedelijk auditplan dat in principe vier jaren vooruitkijkt.