BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1173

2 november 2022

Officiële uitgave van de gemeenschappelijke regeling BAR-organisatie

Privacybeleid BAR-organisatie (Gemeenten Barendrecht, Albrandswaard en Ridderkerk)

Colofon

Naam document
Privacybeleid BAR-organisatie (Gemeenten Barendrecht, Albrandswaard en Ridderkerk)

Nummer zaaksysteem
536423

Doel
Dit Privacybeleid geeft richting aan de manier waarop binnen de BAR-organisatie en in opdracht van de gemeenten Barendrecht, Albrandswaard en Ridderkerk wordt gezorgd voor een adequate, zorgvuldige en rechtmatige omgang met persoonsgegevens en de borging daarvan. Dit beleid bevat daarom uitgangspunten, de organisatie en verantwoordelijkheden ten aanzien van privacy.

Bereik
Dit Privacybeleid is van toepassing op de BAR-organisatie en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking door de BAR-organisatie, zowel voor de interne organisatie als voor de gemeenten Barendrecht, Albrandswaard en Ridderkerk. Het is ook van toepassing op de gegevensverwerking die bij leveranciers c.q. in de Cloud zijn of worden ondergebracht.

Dit beleid richt zich op privacy voor zover het de verwerking van persoonsgegevens betreft, in de wetgeving 'gegevensbescherming' genoemd, en dus niet op andere aspecten van privacy zoals ruimtelijke privacy, het briefgeheim etc.

Dit beleid richt zich op de kaders voor Privacy. Voor de nadere invulling daarvan worden aanvullende beleidsstukken opgesteld (zie ook relatie met andere producten).

Dit beleid zal in een per gemeente aangepaste versie ter besluitvorming worden voorgelegd aan de gemeenten Barendrecht, Albrandswaard en Ridderkerk.

Doelgroep
Dit beleid is gericht op degenen die direct betrokken zijn bij het vaststellen en uitvoeren van het privacybeleid, zoals: Bestuur en management van de BAR-organisatie en de gemeenten en functionarissen rond privacy en informatiebeveiliging.

Daarnaast draagt dit privacybeleid bij aan transparantie richting inwoners over de manier waarop de BAR-organisatie omgaat met persoonsgegevens.

Dit Privacybeleid is openbaar en is beschikbaar voor proceseigenaren (lijnmanagement), applicatiebeheerders, externe partijen, ketenpartners, medewerkers en andere belanghebbende(n).

Versie
v0.7, 10 juni 2022

Versiebeheer
Het beheer van dit document berust bij de Coördinerend Privacy Officer (CPO).

Relatie met andere producten
Dit Privacybeleid heeft een relatie met:

- de Algemene verordening gegevensbescherming (Avg), die aantoonbaarheid, evaluatie en aanpassing van de maatregelen (Art 24 lid 1) vereist en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);
- de Wet Politiegegevens, die nader is uitgewerkt in:
  - o het Besluit Politiegegevens;
  - o het Besluit Politiegegevens Boa's.
- de volgende maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO);

- Control: 18.1.1;
- Control: 18.1.3;
- Control: 18.1.4;
- Overheidsmaatregel: 18.1.3.1;
- Overheidsmaatregel: 18.1.4.1;
- Overheidsmaatregel: 18.1.4.2.

– de Archiefwet;
– sectorspecifieke wet- en regelgeving over de verwerking van persoonsgegevens;
– mandaatregelingen voor verlening van mandaat en volmacht aan functionarissen van de BAR-organisatie;
– het informatiebeveiligingsbeleid.

Dit Privacybeleid heeft verder een relatie met beleidsdocumenten en procedures, waarin dit beleid nader is uitgewerkt. De Coördinerend Privacy Officer (CPO) houdt een overzicht bij van deze beleidsdocumenten, zoals bijvoorbeeld:
1. Gedragsregels/Handreiking "Veilig omgaan met informatie".
2. Sjablonen voor bijvoorbeeld verwerkersovereenkomsten.
3. Procesbeschrijvingen, zoals die voor datalekken, verzoeken van betrokken, DPIA's etc.

Vaststelling en inwerkingtreding
Dit Privacybeleid wordt vastgesteld door het Algemeen Bestuur van de BAR-Organisatie en wordt na vaststelling uitgevoerd. Het Privacybeleid is vastgesteld door:

Het Algemeen Bestuur van de BAR-organisatie op 19 oktober 2022

1: INLEIDING

De BAR-organisatie werkt met persoonsgegevens van inwoners en medewerkers, deels ook met gevoelige persoonsgegevens. Te denken valt aan het Burgerservicenummer (BSN), gegevens in de Basisregistratie personen (BRP) en gezondheidsgegevens bij de uitvoering van de Wet maatschappelijke ondersteuning 2015 (Wmo) en de Jeugdwet. Het waarborgen van de privacy van betrokkenen is daarbij belangrijk voor de rechtmatige uitvoering van gemeentelijke taken.

Persoonsgegevens zijn alle gegevens die –direct of indirect- herleidbaar zijn tot natuurlijke personen. Het gaat dus niet alleen om gegevens waar betrokkenen met naam en toenaam worden genoemd, maar ook om postcodes, autokentekens en cookies op de website.

Kaders voor het verwerken van persoonsgegevens en daarmee voor het waarborgen van de privacy van inwoners, medewerkers en andere betrokkenen zijn voor de BAR-organisatie de Algemene Verordening Persoonsgegevens (Avg), de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en de Wet Politiegegevens (Wpg). Deze staan in de context van de bredere bescherming van de persoonlijke levenssfeer als grondrecht, zoals dat geborgd is in het Europees Verdrag voor de Rechten van de Mens (EVRM).

Onder het verwerken van persoonsgegevens wordt onder meer het verzamelen, bewaren, raadplegen, gebruiken, verstrekken en vernietigen van informatie verstaan.

Het waarborgen van privacy is nodig om een goede werking van werkprocessen van de BAR-organisatie en samenwerking met andere organisaties mogelijk te maken in de maatschappelijke context waarin BAR-organisatie zich beweegt.

1.1: KERNWAARDEN, VISIE EN AMBITIE

Kernwaarden en visie [1]

Als BAR-organisatie zijn we een nabije overheid die met een warm hart betrokken is bij de gemeenschappen van de drie gemeenten en alle inwoners en partijen die daarin een plek hebben. We ondersteunen de drie besturen en werken met excellente dienstverlening aan de woon- en leefomgeving en complexe maatschappelijke vraagstukken die daarbij horen. De BAR-organisatie staan hiervoor vier kernwaarden centraal:

1) Missie, visie, kernwaarden en documenten BAR - BAR-plaza (bar-organisatie.nl)

- Persoonlijk
- Betrokken
- Betrouwbaar
- Modern

Bij de bescherming van persoonsgegevens volgt de BAR-organisatie deze kernwaarden. De betrokkene staat centraal. De BAR-organisatie is transparant richting de burger over de wijze waarop met hun persoonsgegevens wordt omgegaan en is dienstverlenend bij vragen en klachten hierover. De betrokkene moet kunnen vertrouwen op de manier waarop wij omgaan met persoonsgegevens. Nieuwe technologische ontwikkelingen die de BAR-organisatie in staat stellen om persoonsgegevens beter te beschermen en beveiligen, worden waar noodzakelijk toegepast.

Ambitie

De organisatie wil aantoonbaar voldoen aan wet- en regelgeving met betrekking tot persoonsgegevens en "in control" zijn. Dat wil zeggen dat de organisatie overzicht heeft en risico's bewust neemt vanuit bestuurlijk niveau. Dit betekent dat eventuele (rest) risico's die niet afgedekt (kunnen) worden door beheersmaatregelen, bijvoorbeeld omdat zij niet proportioneel worden geacht, ter acceptatie worden voorgelegd aan de directieraad en/of bestuur van de organisatie. De AVG vereist in dit kader passende organisatorische en technische beheersmaatregelen en aantoonbaarheid, evaluatie en aanpassing van de maatregelen (onder andere Art 24 lid 1 WPG).

1.2: OPBOUW PRIVACYBELEID

Dit privacybeleid is opgedeeld in zeven hoofdstukken en sluit af met een bijlage 'rollen en namen'. In dit hoofdstuk worden de kernwaarden, ambitie en de relatie met informatiebeveiliging omschreven. Hoofdstuk 2 van het privacybeleid gaat in op de uitgangspunten van de BAR-organisatie voor de zorgvuldige omgang met persoonsgegevens en de kaders waaruit deze uitgangspunten voortvloeien. Hoofdstuk 3 beschrijft de rollen en verantwoordelijkheden die betrokken zijn bij de bescherming van persoonsgegevens binnen de BAR-organisatie. In hoofdstuk 4 wordt de aanpak van privacy omschreven, waarna het beleid zich richt op inhoudelijke beleidskeuzes (hoofdstuk 5). Hoofdstuk 6 ziet op de specifieke verwerking van politiegegevens. Ten slotte gaat hoofdstuk 7 over de publicatie en wijziging van het beleid.

2: UITGANGSPUNTEN EN KADERS

2.1: WETTELIJK KADER

De wettelijke kaders voor het verwerken van persoonsgegevens zijn voor de BAR-organisatie gegeven in:

- de Algemene verordening gegevensbescherming (Avg), die
  - het kunnen aantonen van het voldoen aan de AVG (art. 5 lid 2 AVG) vereist;
  - aantoonbaarheid, evaluatie en aanpassing van de maatregelen (Art 24 lid 1) vereist.

- de Uitvoeringswet Avg (UAVG);
- de Wet Politiegegevens, die nader is uitgewerkt in:
  - het Besluit Politiegegevens;
  - het Besluit Politiegegevens Boa's.

- en wetten ten aanzien van de taakuitvoering van gemeenten, zoals bijvoorbeeld:
  - de wet Basisregistratie Personen (BRP);
  - de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI);
  - de Wet Maatschappelijke Ondersteuning (Wmo);
  - de Jeugdwet (Jw);
  - de Participatiewet (Pw);
  - de Archiefwet.

Daarnaast committeert de organisatie zich voor het aspect van de beveiliging van persoonsgegevens (Art 5 lid 1 sub f en Art 32 AVG) aan de Baseline Informatiebeveiliging Overheid (BIO) die is vastgesteld voor alle overheidslagen. De BIO is gebaseerd op de beheersmaatregelen van de internationale norm ISO27001, die deels nader zijn uitgewerkt in overheidsmaatregelen. Voor het privacybeleid zijn met name de volgende maatregelen uit de BIO van belang:

- Control: 18.1.1;
- Control: 18.1.3;

- Control: 18.1.4;
- Overheidsmaatregel: 18.1.3.1;
- Overheidsmaatregel: 18.1.4.1;
- Overheidsmaatregel: 18.1.4.2.

2.2: RELATIE TUSSEN PRIVACY EN INFORMATIEBEVEILIGING

Burgens en medewerkers hebben recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. Dit vraagt een adequate beveiliging van deze persoonsgegevens en het respecteren van de geldende privacywetgeving. Het beschermen van persoonsgegevens is het gemeenschappelijke domein waar privacy en informatiebeveiliging samenkomen.

Dit privacybeleid beschrijft hoe persoonsgegevens die worden verwerkt door of namens de organisatie worden beschermd. Het borgen van de beveiliging van informatie die niet ziet op individuele personen is gevat in een afzonderlijk informatieveiligheidsbeleid.

In de praktijk is er een nauwe samenwerking tussen informatiebeveiliging en privacy, bijvoorbeeld bij bewustwording en training van medewerkers en bij het adviseren over en beoordelen van nieuwe applicaties. Het privacybeleid heeft door de nauwe samenhang tussen privacy en informatiebeveiliging een relatie met het Informatiebeveiligingsbeleid.

2.3: ORGANISATIEKADERS

Beleidsdocumenten en procedures

Dit Privacybeleid heeft intern een relatie met beleidsdocumenten en procedures, waarin dit beleid nader is uitgewerkt. De Coördinerend Privacy Officer (CPO) houdt een overzicht bij van deze beleidsdocumenten, zoals bijvoorbeeld:

1. Gedragsregels/Handreiking "Veilig omgaan met informatie".
2. Sjablonen voor bijvoorbeeld verwerkersovereenkomsten.
3. Procesbeschrijvingen, zoals die voor incidentbeheer, datalekken, verzoeken van betrokken, DPIA's etc.

Uitgangspunten

Voor gegevensbescherming - de zorgvuldige omgang met persoonsgegevens - en de borging daarvan gaat de BAR-organisatie uit van de hiernavolgende uitgangspunten.

Naleving privacybeleid

Het dagelijks bestuur van de BAR-organisatie, de directieraad, de (Coördinerend) Privacy Officer(s) en de proceseigenaren (lijnmanagers) bevorderen de naleving van dit privacy-beleid, de algehele communicatie en bewustwording (awareness) rondom privacy.

Drie verdedigingslinies / Three lines of defense

Bij de toepassing van gegevensbescherming staat het faciliteren van de werkprocessen van de organisatie voorop. Privacy dient hieraan een bijdrage te leveren door het veilig werken met informatie te faciliteren.

De organisatie wil aantoonbaar voldoen aan wet- en regelgeving. De Avg vereist in dit kader passende organisatorische en technische beheersmaatregelen en aantoonbaarheid, evaluatie en aanpassing van de maatregelen en verplichtingen in de AVG (Art 5 lid 2 AVG; art 24 lid 1 AVG).

De organisatie wil "in control" zijn, dat wil zeggen overzicht hebben en risico's bewust nemen vanuit bestuurlijk niveau. Dit betekent dat eventuele (rest) risico's die niet afgedekt (kunnen) worden door beheersmaatregelen, bijvoorbeeld omdat zij niet proportioneel worden geacht, ter acceptatie worden voorgelegd aan directieraad van de BAR-organisatie.

De organisatie past daarvoor de drie verdedigingslijnen toe vanuit Interne Controle:

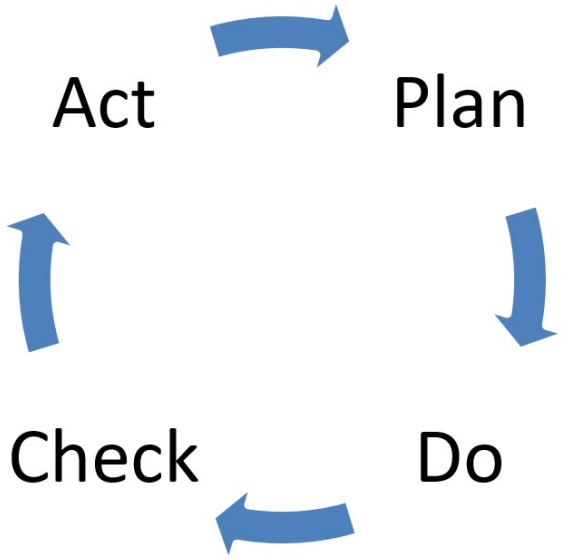
1) De beheersing van werkprocessen binnen de afdeling onder verantwoordelijkheid van de lijnmanager. Dat wil zeggen: werkprocessen op orde, passende werkinstructies en werken volgens afspraken.
2) Borging/controle van beheersmaatregelen in de lijn, bijvoorbeeld door kwaliteitsfunctionarissen of teamleiders. Deze borgingsmaatregelen/controles hebben als doel vast te stellen en aan te tonen dat werkprocessen conform de afspraken verlopen en deze te evalueren en waar nodig aan te passen. Deze borging wordt voor privacy gecoördineerd door de CPO en uitgevoerd in de lijn op basis van controleplan. Dit omvat ook de diverse audits vanuit ENSIA (Eenduidige Normatiek Single Information Audit).
3) Interne en externe audits vanuit de stafafdeling Concerncontrol, onder andere de Verbijzonderde Interne Controles (VIC) en controles/audits op basis van Art 213a van de Gemeentewet en Art. 33 van de Wet Politiegegevens. Daaronder valt ook de evaluatie van de opzet, bestaan en werking van de 1e en de 2e verdedigingslinie.

Managementsysteem voor informationele privacy (PIMS)

De BAR-organisatie doorloopt een plan-do-check-act cyclus voor de verbetering en beheersing van de verwerking van persoonsgegevens. Het doorlopen van deze cyclus vormt het managementsysteem voor informationele privacy (PIMS). De plan-do-check-act cyclus wordt op het niveau van de BAR-organisatie en op het niveau van de beheersmaatregelen toegepast:

- *Plan:* inrichten en documenteren van de beheersmaatregelen en de organisatiebrede aanpak van privacy op basis van geldende normen, wettelijke eisen en risico's voor de organisatie. (in termen van interne controle: de opzet, 1e verdedigingslinie)
- *Do:* aantonen van de uitvoering van beheersmaatregelen en de organisatie-brede aanpak van privacy. (in termen van interne controle: het bestaan, 1e verdedigingslinie)
- *Check:* de borging/controle en evaluatie van de beheersmaatregelen en de organisatiebrede aanpak van privacy met als criteria de volledige uitvoering van de maatregelen en de effectiviteit hiervan. Daarbij wordt ook rekening gehouden met de voortschrijdende ontwikkeling van de techniek en bedreigingen. Hieronder vallen ook interne en externe audits. (de werking, 2e en 3e verdedigingslinie)
- *Act:* het aanpassen en/of verbeteren van beheersmaatregelen en de organisatiebrede aanpak van privacy op basis van bovengenoemde evaluatie.

Het doorlopen van deze cyclus zorgt voor een adequate beheersing waarbij de organisatie aantoonbaar voldoet aan de Avg en de Wpg.



Beheersmaatregelen / Control Framework
Om te komen tot passende beheersmaatregelen wordt gebruik gemaakt van raamwerken met beheersmaatregelen (Control Framework) om te waarborgen dat de wetgeving adequaat wordt afgedekt. Voorbeelden van beheersmaatregelen zijn het voeren van een verwerkingenregister, het informeren van betrokkenen, het overeen komen van verwerkersovereenkomsten en het uitvoeren van Data Protection Impact Assessments (DPIA's).

Keuzes bij implementatie en aanpassing van de beheersmaatregelen uit de genoemde raamwerken, zijn gebaseerd op een risicoafweging en worden proportioneel getroffen. Daarbij wordt onder andere rekening gehouden met de financiële mogelijkheden van de organisatie respectievelijk de deelnemende gemeenten. Voor de proportionele toepassing van maatregelen wordt gebruik gemaakt van een dataclassificatie. Daarmee kunnen beheersmaatregelen worden afgestemd op het risicoprofiel van de persoonsgegevens ten aanzien van de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens.

De organisatie houdt een overzicht bij van de implementatie van de beheersmaatregelen uit de gekozen raamwerken.

Externe partijen
De BAR-organisatie verlangt van externe partijen die gegevens in opdracht van de organisatie verwerken en ketenpartners waarmee gegevens van inwoners worden uitgewisseld aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging en borging van privacy als de BAR-organisatie zelf. Het gaat daarbij bijvoorbeeld om IT-leveranciers, maar ook ketenpartners in bijvoorbeeld Wmo en Jeugdzorg, zoals zorginstellingen. Dit wordt gewaarborgd in juridische overeenkomsten, zoals verwerkersovereenkomsten.

Medewerkers
Wanneer dit beleid en/of beheersmaatregelen eisen stellen aan taken en verantwoordelijkheden van medewerkers dan worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de leidinggevende en de medewerker. Immers in de HR21 normfuncties zijn de werkzaamheden met betrekking tot privacy niet expliciet opgenomen. Deze specifieke werkzaamheden passen niet bij het karakter van een generieke functiebeschrijving waarin de werkzaamheden op hoofdlijnen zijn beschreven. Conflicterende taken en verantwoordelijkheden behoren hierbij te worden gescheiden.

Iedere medewerker, zowel vast als tijdelijk, intern of extern, (keten)partner of betrokkene, is verplicht waar nodig gegevens en applicaties te beschermen tegen ongeautoriseerde toegang (naleven privacybeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit te melden.

Iedere medewerker wordt geacht de gedragsregels van de organisatie te kennen en uit te dragen bij het uitoefenen van zijn of haar functie. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern en overige betrokkene(n) voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders.

3: ROLLEN EN VERANTWOORDELIJKHEDEN

3.1: BAR-ORGANISATIE

Het dagelijks bestuur is bestuurlijk eindverantwoordelijke voor de Informatieveiligheid & Privacy (I&P) die door de BAR-organisatie wordt uitgevoerd voor de gemeenten.[2] Met andere woorden zij bewaakt of gemeentelijke informatiebeveiligingsdoelstellingen worden/zijn gerealiseerd door de BAR-organisatie. In die hoedanigheid stelt zij beleid vast, waarin wordt aangegeven hoe zij met die verantwoordelijkheid wil omgegaan.

De directieraad van de BAR-organisatie is ambtelijk eindverantwoordelijk voor de uitvoering van het privacybeleid. De directie geeft invulling aan die verantwoordelijkheid door het omzetten van het beleid in doelstellingen en plannen, de integratie daarvan in de processen van de organisatie, toewijzing van rollen en verantwoordelijkheden, het ter beschikking stellen van middelen, het bekendmaken van het beleid en het belang daarvan, het aansturen en ondersteunen van medewerkers bij en het toezien op uitvoering van het beleid, evaluatie en bijstelling van de aanpak van privacy en beheersingsmaatregelen.

Daarbij wordt de directie ondersteund door de organisatie, namelijk door:

- alle **medewerkers** die elk verantwoordelijk zijn voor het uitvoeren van het privacybeleid als onderdeel van hun professionele verantwoordelijkheid. Om hen daarbij te ondersteunen is er een beleidsdocument "Veilig omgaan met informatie en bedrijfsmiddelen", waarin gedragsregels staan voor medewerkers, en worden medewerkers bewust gemaakt van hun rol/bijdrage en geïnformeerd over hoe zij deze kunnen uitvoeren/leveren, zowel bij indiensttreding als op basis van regelmatige bewustwordings- en leerinterventies. Daarvoor wordt jaarlijks een programma opgesteld door de Coördinerend Privacy Officer en de CISO.
- **leidinggevenden**/proceseigenaren die
    - verantwoordelijk zijn voor de uitvoering van het privacybeleid en beheersmaatregelen binnen hun afdeling. Informatiesystemen en processen die door meerdere organisatieonderdelen worden gebruikt vallen onder de verantwoordelijkheid van de door de directie aangewezen systeemeigenaar;
    - zorgen voor adequate inrichting van werkprocessen en aansturing van medewerkers (1e verdedigingslinie);
    - toezien op de naleving van het beleid en bevorderen van privacybewustzijn;
    - onderdelen van beheersmaatregelen uitvoeren, zoals het vullen van het verwerkingenregister, de uitvoering van DPIA's en risicoanalyses, het beoordelen van toegangsrechten, etc.;
    - relevante wettelijke, statutaire, regelgevende en contractuele eisen voor hun informatiesystemen vaststellen, documenteren en actueel houden;
    - processpecifieke borgings-/controleactiviteiten uitvoeren, vaak samenhangend met processpecifieke applicaties;
    - processpecifieke beheersmaatregelen uitvoeren, bijvoorbeeld voortvloeiend uit wetgeving, zoals over basisregistraties, waardedocumenten (zoals reisdocumenten/rijbewijzen), DigID en SUWI;
    - verantwoordelijk zijn voor het nemen van maatregelen om datalekken binnen hun afdeling te voorkomen;
    - voor zover zij leidinggevenden zijn van teams met Bijzonder Opsporingsambtenaren (Boa's), verantwoordelijk zijn voor de implementatie, uitvoering en borging van de Wpg binnen hun team.
- **Decentrale Aanspreekpunten voor Privacy en Informatiebeveiliging** (DAPI) benoemen, die de leidinggevende ondersteunen bij het uitvoeren van de bovengenoemde taken (op welk niveau van de organisatie de benoeming van een DAPI wenselijk is hangt af van de omvang van de afde-

2) NB t.a.v. de rol van College van burgemeesters en wethouders bij vertaling van het beleid naar de gemeenten: Het college van burgemeester en wethouders van elk van de deelnemende gemeenten is eindverantwoordelijk voor privacy binnen de gemeentelijke organisatie en legt daarover extern verantwoording af. Het college geeft richting aan het privacybeleid, bepaalt op hoofdlijnen welke privacyrisico's acceptabel zijn en welke privacyrisico's ze wil afdekken. De uitvoering van het privacybeleid is belegd bij het bestuur van de BAR-organisatie, conform de convenanten die de deelnemende gemeenten met de BAR-organisatie hebben afgesloten (zie bijlage 2). Daartoe is een mandaatbesluit van toepassing (zie bijlage 3). Het college houdt toezicht op de uitvoering. Daarnaast legt het college van burgemeester en wethouders verantwoording af over de status van de gegevensbescherming binnen de gemeente aan de landelijke toezichthouders en de gemeenteraad. Deze verantwoording bestaat in ieder geval uit periodieke externe Wpg audit, een verklaring van het college van burgemeester en wethouders (collegeverklaring) en een passage over privacy in het jaarverslag.

ling en de hoeveelheid gevoelige gegevens die daarin wordt verwerkt). Onder deze taken vallen het signaleren van beveiligings-/privacyissues binnen de afdeling, aanleveren van rapportageinformatie aan CISO en CPO, informatieverzameling voor DPIA's, het aanleveren van informatie voor het register van verwerkingen en verzoeken van betrokkenen, bevorderen van het bewustzijn binnen de afdeling. De DAPI zijn aanspreekpunt bij audits, zoals de Wpg audit. De leidinggevende behoudt de eindverantwoordelijkheid.

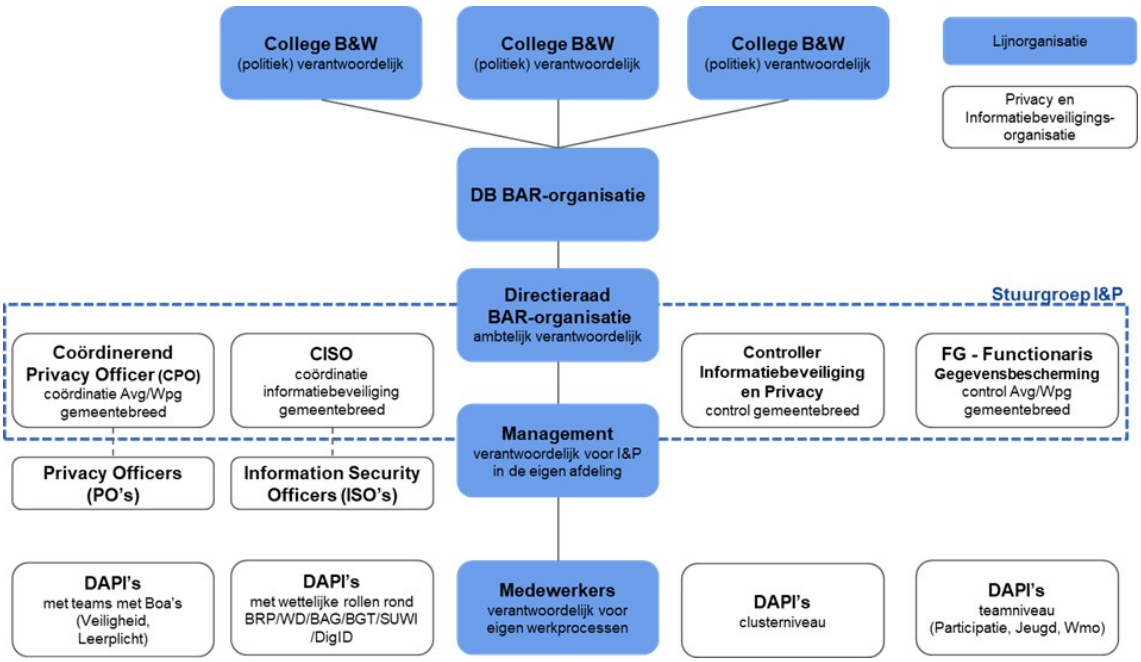
- de **Coördinerend Privacy Officer** (CPO), die
    - o het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli coördineert;
    - o de implementatie, uitvoering en borging van beheersmaatregelen coördineert;
    - o rapporteert daarover en over datalekken aan de Stuurgroep;
    - o de stuurgroep en management gevraagd en ongevraagd adviseert over privacy/gegevensbescherming in brede zin;
    - o de afhandeling en evaluatie van datalekken, verzoeken van betrokkenen en van de Autoriteit Persoonsgegevens coördineert;
    - o privacybewustzijn bevordert in de gehele organisatie;
    - o coördineert de activiteiten van PO's en DAPI's, ook inhoudelijk.

- **de Privacy Officer(s) (PO's),** die: op operationeel niveau gevraagd en ongevraagd adviseert en ondersteunt bij de uitvoering van het privacybeleid en jaarplan en de implementatie en uitvoering van beheersmaatregelen, zoals DPIA's, verzoeken van betrokkenen, de afhandeling en evaluatie van datalekken, het bevorderen van privacybewustzijn, het register van verwerkingen.
- de **Functionaris Gegevensbescherming** (FG), die toezicht houdt, kaders aangeeft, informeert en adviseert vanuit zijn/haar wettelijke taak conform de Avg en de Wpg en daarover rapporteert aan de Stuurgroep I&P en is bevoegd rechtstreeks te verslag te doen aan de gemeentesecretaris en het dagelijks bestuur van de BAR-organisatie.
- de **Chief Information Security Officer (CISO)**, die
    - o het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli coördineert;
    - o De implementatie, uitvoering en borging van beheersmaatregelen coördineert;
    - o rapporteert daarover en over beveiligingsincidenten aan de Stuurgroep I&P en is bevoegd rechtstreeks te verslag te doen aan de gemeentesecretaris en het dagelijks bestuur van de BAR-Organisatie;
    - o De stuurgroep en management gevraagd en ongevraagd adviseert over informatiebeveiliging in brede zin;
    - o Beveiligingsincidenten registreert in een incidentenregister en de afhandeling en evaluatie hiervan coördineert;
    - o beveiligingsbewustzijn bevordert in de gehele organisatie;
    - o coördineert de activiteiten van ISO's en DAPI's, ook inhoudelijk.

- de stafafdeling **Concern control**, die:
    - o interne audits coördineert, bijvoorbeeld: de Verbijzonderde Interne Controles (VIC) en het onderzoeksplan doelmatigheid en doeltreffendheid op basis van Art 213a van de Gemeentewet en interne audits op basis van Art. 33 van de Wet Politiegegevens;
    - o externe audits coördineert, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening en de externe audit op basis van Art. 33 van de Wet Politiegegevens.

- **andere medewerkers** die verantwoordelijk zijn voor specifieke onderdelen van het beleid, zoals het uitvoeren van specifieke beheersmaatregelen en de bewaking daarvan. Deze specifieke taken en verantwoordelijkheden worden benoemd in de beschrijving van de beheersmaatregelen.

Een en ander is hieronder schematisch weergegeven:



Besturing door de Stuurgroep Informatiebeveiliging en privacy (I&P)
De Stuurgroep Informatiebeveiliging en privacy (I&P) geeft namens de directie sturing aan de uitvoering van het privacybeleid. De stuurgroep bestaat uit:

- Algemeen Directeur BAR-Organisatie
- Manager Concerncontrol (CCC)
- Directeur met portefeuille Juridische Zaken en Inkoop (JZI) / Informatie en Automatisering (IFA) / Dienstverlening (DVL)
- Manager Juridische Zaken en Inkoop (JZI)
- Manager Cluster Maatschappij
- Manager Informatie en automatisering (IFA)
- Functionaris Gegevensbescherming (FG)
- Coördinerend Privacy Officer (CPO)
- Chief Information Security Officer (CISO)

De Voorzitter van de stuurgroep I&P, tevens lid van de directieraad, gehoord de leden van de Stuurgroep[3]:

- wijst ook de verantwoordelijkheden voor beheersmaatregelen toe aan functies binnen de organisatie;
- adviseert de directieraad over besluiten met betrekking tot de implementatie van beheersmaatregelen en acceptatie van (rest-)risico's.

De CPO rapporteert functioneel in de Stuurgroep I&P aan de directieraad.

De CPO wordt ondersteund door:

- Privacy Officer(s) (PO's);
- verantwoordelijken voor beheersmaatregelen die door de Stuurgroep aan hen zijn toegewezen;
- leidinggevenden en hun Decentrale aanspreekpunten Privacy en Informatiebeveiliging (DAPI) voor de implementatie en borging binnen de afdelingen.

Taken en verantwoordelijkheden zijn hier op hoofdlijnen beschreven en worden nader uitgewerkt in de documentatie van beheersmaatregelen, procedures etc.

3) Conform mandaatbesluit

4: DE AANPAK VAN PRIVACY

4.1: JAARCYCLUS

Om de borging van het privacybeleid en de daarvan afgeleide plannen te realiseren, doorloopt de BAR-organisatie de onderstaande Plan, Do, Check, Act (PDCA) cyclus, zowel organisatiebreed als per beheersmaatregel, resulterend in een Information Privacy Management System (PIMS).

Het PIMS wordt toegepast door in aansluiting bij (bestaande) bestuurs- en P&C-cycli jaarlijks:

– **Plan**: Een jaarplan met verbeterpunten op te stellen, rekening houdend met de organisatiestrategie en -doelstellingen, risico's, regelgeving, de stand van de techniek en beschikbare middelen.

  Het jaarplan voor privacy wordt opgesteld op basis van:

  - evaluatie van de uitvoering en resultaten van het vorige verbeterplan;
  - risicoanalyse t.a.v. privacy op basis van de separaat beschreven aanpak voor risicoanalyse die het identificeren, analyseren/beoordelen, evalueren en het nemen van maatregelen omvat;
  - evaluatie van de implementatie van beheersmaatregelen ten opzichte van de gekozen control frameworks (GAP-analyse);
  - datalekken;
  - trends ten aanzien van bedreigingen, kwetsbaarheden en technologische mogelijkheden en maatschappelijke ontwikkelingen;
  - prioriteiten van toezichthouders, in het bijzonder de Autoriteit Persoonsgegevens;
  - het privacybeleid en evaluatie van de naleving daarvan;
  - de strategie en doelstellingen van de organisatie.

  Het plan bevat meetbare doelen en een activiteitenplanning met verantwoordelijken, benodigde middelen, tijdslijnen en resultaten.

– **Do**: het jaarplan en beheersmaatregelen uit te voeren, waarbij beheersmaatregelen worden ingevoerd en stapsgewijs worden verbeterd. Onder de beheersmaatregelen vallen onder andere:

  - onderhouden van een register van verwerkingen;
  - informeren van betrokkenen;
  - afhandelen van datalekken en verzoeken van betrokkenen;
  - afsluiten van verwerkersovereenkomsten met leveranciers en de controle van de naleving daarvan;
  - tijdig wissen van persoonsgegevens die niet meer nodig zijn;
  - uitvoeren van DPIA's.

  De uitvoering van het jaarplan en de beheersmaatregelen wordt bewaakt. De CPO rapporteert daarover elk kwartaal via de Stuurgroep aan de directie. Waar nodig worden er aanvullende maatregelen genomen.

– **Check**: borgings-/controleacties uit te voeren om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd en of zij effectief zijn. De borgings-/controle acties worden opgenomen in een controleplan, zodat alle geïmplementeerd maatregelen passend worden afgedekt. De CPO rapporteert elk kwartaal daarover en over datalekken en andere relevante gebeurtenissen via de Stuurgroep aan de directie, vergezeld van verbetervoorstellen, waar van toepassing.

  Voor geïmplementeerde onderdelen van het PIMS en geïmplementeerde beheersmaatregelen wordt bepaald of en zo ja hoe deze worden opgenomen in het audit-plan van de organisatie. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben.

  Op basis van de rapportages van de CPO en audits wordt privacy geëvalueerd door de stuurgroep I&P. De voorzitter van de stuurgroep I&P neemt op basis daarvan besluiten over de verbetering van het managementsysteem en beheersingsmaat-regelen. Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus gerapporteerd over het doorlopen van de beschreven PDCA-cyclus met betrekking tot privacy. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld.

– **Act**: bij te sturen, te herprioriteren en/of aanvullende maatregelen te nemen of aanbevelingen te doen voor het volgende verbeterplan naar aanleiding van afwijkingen van plannen en beheersmaatregelen en andere ontwikkelingen, bijvoorbeeld in de maatschappij, wet- en regelgeving of techniek. Dit gebeurt met name in de stuurgroep op basis van de adviezen van de CPO. Waar nodig vindt besluitvorming in de directie of op bestuurlijk niveau plaats. Daarmee zorgt de organisatie voor een continue verbetering van privacy.

4.2: IMPLEMENTATIE OF VERNIEUWING BEDRIJFSPROCESSEN

Naast deze jaarlijkse cyclus wordt privacy geborgd bij de implementatie of vernieuwing van bedrijfsprocessen. Het gaat daarbij bijvoorbeeld om de implementatie van nieuwe taken, werkprocessen of nieuwe (versies van) applicaties. De CISO en CPO stellen daarvoor een proces op dat waarborgt dat nieuwe of vernieuwde bedrijfsprocessen voldoen aan het privacybeleid en dat de vereiste beheersmaatregelen daarvoor zijn geïmplementeerd. Dit proces bevat ten minste de volgende onderdelen:

– een dataclassificatie, waarin de eisen aan vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens in het nieuwe of vernieuwde proces worden vastgesteld;
– een DPIA (Data Protection Impact Assessment, dan wel, Gegevensbeschermingsef-fectbeoordeling) wordt alleen uitgevoerd als deze verplicht is. De DPIA bestaat onder andere uit een analyse van risico's voor betrokkenen en een onderbouwing van de rechtmatigheid van de nieuwe verwerking van persoonsgegevens onderbouwd;
– bij een hoge dataclassificatie wordt een risicoanalyse uitgevoerd, tenzij deze al in het kader van een DPIA is of wordt uitgevoerd. In een risicoanalyse worden risico's geïdentificeerd en beoordeeld. Op basis daarvan beslist de proceseigenaar om een risico te accepteren, te beperken (te mitigeren), over te dragen (te verzekeren) of te vermijden (door de activiteit te staken);
– keuze van passende maatregelen om de privacyrisico's te beperken;
– acceptatie van eventuele restrisico's door de directieraad van de BAR-organisatie;
– bewaking van de uitvoering van de gekozen maatregelen ten aanzien van de risico's die in de DPIA of in de risicoanalyse zijn vastgesteld.

4.3: SAMENWERKING

Specifieke informatie op het gebied van privacy van relevante expertisegroepen en de VNG wordt gebruikt om de inrichting van privacy te verbeteren.

De organisatie heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie. Dit overzicht wordt door de CPO beheerd en minimaal jaarlijks bijgewerkt.

4.4: EVALUATIE EN HERZIENING

Het Privacybeleid wordt ten minste elke drie jaar herzien op basis van:

– een evaluatie van het beleid;
– maatschappelijke ontwikkelingen en ontwikkelingen in de organisatiestrategie, wet- en regelgeving, de stand van de techniek en risico's;
– organisatiestrategie en -doelstellingen;
– documentatie van de jaarlijkse verbetercycli (zie boven);
– terugkoppeling van belanghebbende partijen, bijvoorbeeld de gemeenteraad en de medezeggenschap;
– onafhankelijke beoordelingen (audits);
– aanbevelingen van relevante instanties, zoals toezichthouders (bijvoorbeeld de Autoriteit Persoonsgegevens), en de VNG.

5: INHOUDELIJKE KEUZES

De BAR-organisatie hanteert de volgende keuzes, tenzij door het DB, gemandateerd aan de directie gehoord de Stuurgroep I&P een afwijking daarvan wordt besloten:

5.1: BEWUSTWORDING EN TRAINING

De CPO stelt jaarlijks in samenwerking met de CISO een bewustwordings- en trainingsplan op en coördineert de uitvoering daarvan samen met de CISO. Bij het opstellen van het bewustwordings- en trainingsplan wordt rekening gehouden met trends in bedreigingen en maatschappelijke ontwikkelingen.

De DAPI's ondersteunen de uitvoering van het bewustwordings- en trainingsprogramma in hun eigen clusters en teams en adviseren de CPO en de CISO bij het opstellen van het bewustwordings- en trainingsprogramma.

5.2: REGISTER VAN VERWERKINGEN

In het register van verwerkingen wordt per verwerking de volgens de Avg verplichte informatie opgenomen, ten minste aangevuld met organisatorische verantwoordelijkheid en gebruikte applicaties. Het detailniveau wordt bepaald door het doel en de grondslag van de verwerking. Alle gebruik van persoonsgegevens voor hetzelfde doel met dezelfde grondslag valt binnen één verwerking, inclusief verstrekkingen van persoonsgegevens aan derden, ook al is er specifiek voor de verstrekking een additionele grondslag.

Het register wordt beheerd door de CPO.

Het register wordt jaarlijks gecontroleerd en geactualiseerd door de proceseigenaren, ondersteund door de DAPI en gecoördineerd door de (C)PO.

5.3: DPIA

Een DPIA wordt alleen uitgevoerd wanneer deze verplicht is volgens de Avg Art 35, Wpg Art 4c of richtlijnen van de EDPB of de AP. De voorzitter van de Stuurgroep I&P, tevens lid van de directieraad, gehoord de leden van de Stuurgroep[4]kan besluiten dat een DPIA moet worden uitgevoerd op basis van een advies van CPO of CISO.

Voor de uitvoering van een DPIA voorafgaand aan de implementatie of wijziging van de verwerking is de proceseigenaar eindverantwoordelijk. Deze wordt daarbij ondersteunt door de DAPI, een eventuele projectleider en de PO.

Bij de uitvoering van een DPIA worden de door de CPO vastgestelde werkwijze en sjablonen gehanteerd. Onderdeel daarvan is Privacy by design en default.

De conceptrapportage voor de DPIA wordt ter toetsing voorgelegd aan de CPO en de CISO alvorens deze ter advisering aan de FG wordt voorgelegd conform Avg Art 35 lid 2. De BAR-organisatie hanteert deze werkwijze ook bij DPIA op basis van de Wpg.

De finale DPIA-rapportage wordt door de proceseigenaar vastgesteld en opgestuurd aan de CPO. Deze registreert de te treffen additionele maatregelen. De proceseigenaar informeert de CPO ten minste elke 3 maanden over de status van de implementatie van de additionele maatregelen. De CPO neemt de status van de additionele maatregelen mee in de rapportage aan de stuurgroep.

5.4: DATALEKKEN

Medewerkers zijn gehouden datalekken, beveiligingsincidenten en kwetsbaarheden te melden. Deze worden volgens een procedure afgehandeld en –indien in de Avg/Wpg voorgeschreven – tijdig gemeld aan de AP en/of betrokkenen. Gegevens van de melden zijn alleen voor een beperkt aantal functionarissen, zoals CPO en CISO in te zien.

Alle meldingen worden opgenomen in een register. Daarin wordt per melding aangegeven of er sprake is van een datalek en of melding aan AP en/of betrokkene verplicht is.

Elk datalek wordt geëvalueerd met het oog op het treffen van maatregelen om herhaling te voorkomen. Jaarlijks worden alle datalekken geëvalueerd om trends en patronen te herkennen en om maatregelen te treffen om herhaling te voorkomen.

5.5: TRANSPARANTIE EN RECHTEN VAN BETROKKENEN

De BAR-organisatie informeert betrokkenen over de verwerking van zijn/haar persoonsgegevens en over zijn/haar rechten:

- Bij eerste schriftelijke contact met specifiek voor de verwerking.
- In algemene termen met een privacyverklaring op de website.

Daarbij wordt ook aangegeven hoe men een verzoek op basis van de Avg of de Wpg kan indienen en er is een procedure om deze verzoeken tijdig af te handelen. Onderdeel daarvan is de identificatie van

4) Conform mandaatbesluit

de aanvrager middels een wettelijk erkend legitimatiebewijs. Bij schriftelijke verzoeken kan daarvan een kopie worden gebruikt.

5.6: GEAUTOMATISEERDE BESLUITVORMING, WAARONDER PROFILERING

De BAR-organisatie maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering zoals bedoeld in de Avg Art 22.

5.7: OVEREENKOMSTEN MET DERDEN

De proceseigenaren zijn verantwoordelijk voor het afsluiten van verwerkersovereenkomsten met partijen aan wie de verwerking van persoonsgegevens is uitbesteed (verwerkers). De uitvoering kan bijvoorbeeld door de DAPI of een projectleider worden gedaan. De PO adviseert de proceseigenaar over de informatie die in de verwerkersovereenkomst moet worden opgenomen. Elke verwerkersovereenkomst moet voor ondertekening worden getoetst door een PO.

Bij het opstellen van verwerkersovereenkomsten wordt gebruik gemaakt van het sjabloon van de VNG en zijn een aantal door de BAR-organisatie opgestelde basiseisen van toepassing. Afwijkingen van dit sjabloon en deze eisen is alleen mogelijk na goedkeuring door de voorzitter van de Stuurgroep I&P, tevens lid van de directieraad, gehoord de leden van de Stuurgroep[5] na advies van de CPO en de CISO. Dat kan nodig zijn als leveranciers niet aan bepaalde eisen willen of kunnen voldoen.

5.8: BEWAARTERMIJNEN

Persoonsgegevens worden niet langer bewaard dan nodig voor het doel waarvoor de persoonsgegevens zijn verzameld. Daartoe wordt per verwerking een bewaartermijn vastgesteld, in sommige gevallen worden meerdere bewaartermijnen voor verschillende categorieën van gegevens vastgesteld. Het vaststellen van bewaartermijnen gebeurt op basis van de Avg, de Wpg, sectorale wetgeving, de archiefwet en de Selectielijst, waarbij de wetgeving voor gaat op de selectielijst. De proceseigenaar is verantwoordelijk voor tijdige wissing van persoonsgegevens. Per verwerking wordt vastgesteld wie door de proceseigenaar is benoemd om deze wissing uit te voeren.

5.9: DOORGIFTE

De BAR-organisatie verwerkt geen gegevens buiten de Europese Economische Ruimte (EER) en staat haar leveranciers (verwerkers) niet toe om gegevens die in opdracht van de BAR-organisatie worden verwerkt, buiten de EER door te geven.

6: BELEID TEN AANZIEN VAN DE VERWERKING VAN POLITIEGEGEVENS

6.1: ALGEMENE UITGANGSPUNTEN

De BAR-organisatie hanteert het volgende beleid, tenzij door het DB, gemandateerd aan de directie gehoord de Stuurgroep I&P een (tijdelijke) afwijking daarvan wordt besloten:

Uitgangspunten en bereik

1) De BAR-organisatie hanteert als raamwerk voor beheersmaatregelen (Control Frame-work) het door Wpg-auditoren gehanteerde raamwerk, zoals dat is opgenomen in bij-lage 3 en 4 van de NOREA-handreiking privacy audit Wpg voor boa's.
2) Wanneer gebruik gemaakt wordt van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS), dan wordt met de leverancier een verwerkers-overeenkomst afgesloten en dient deze een Third Party Memorandum (TPM) conform de NOREA-handreiking privacy audit Wpg voor boa's.
3) De BAR-organisatie voert voor elke verwerking van politiegegevens een DPIA uit. (deze is verplicht het gaat om gevoelige gegevens en er sprake is van een ongelijk machtsverhouding tussen de Boa en de verdachte)
4) De BAR-organisatie verwerkt politiegegevens op basis van Artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (Art 15-21 en 23-24). De BAR-organisatie verwerkt politiegegevens verder in het kader van Art 13 Wpg (ondersteunende taken), voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt.
5) De BAR-organisatie verwerkte geen gegevens op basis van
   a) Art 9 Wpg (onderzoek in een bepaald geval). Wel verlenen Boa's medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten.

5) Conform mandaatbesluit

b) Art 11 Wpg. (geautomatiseerd vergelijken en in combinatie zoeken voor een Art 9 onderzoek)
c) Art 17a Wpg. (Doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte)
d) en maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering als bedoeld in de Wpg Art 7a.

6) Toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerden toegang hebben tot politiegegevens.
7) Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

Rollen, taken en bevoegdheden

8) De Privacy Officer inventariseert jaarlijks of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden dit beleid en het verwerkingenregister indien nodig aangepast.
9) De Teamleider van het team met daarin Boa's is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:
   a) Het onder de aandacht brengen van de handreiking/gedragsregels voor Boa's bij de medewerkers en het toezien op deze gedragsregels.
   b) Het bijhouden van een overzicht met geautoriseerden.
   c) Actueel houden van het verwerkingenregister t.a.v. verwerkingen in het team.
   d) Bijhouden van een lijst met veel regelmatig voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking.
   e) Zorgen dat Art 8 gegevens
      i) Na 1 jaar alleen nog beschikbaar zijn voor gericht zoeken.
      ii) Na 5 jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures.
      iii) Na 10 jaar worden vernietigd.

10) De Teamleider van het team met daarin Boa's heeft de volgende bevoegdheden
   a) Het nemen van autorisatiebesluiten in de zin van Wpg Art 6 lid 3, 4, 5 met behulp van het formulier "Autorisatie verwerking politiegegevens".
   b) Het besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix voor het informatiesysteem waarin politiegegevens worden verwerkt.

11) De Functionaris Gegevensbescherming
   a) adviseert en informeert over de Wpg, onder andere over DPIA's;
   b) houdt toezicht op de uitvoering van de Wpg;
   c) werkt samen met de AP en is contactpunt voor de AP;
   d) stelt jaarlijks een verslag op met bevindingen.

12) De FG voert de volgende controles uit:
   i) Steekproefsgewijze beoordeling van Processen Verbaal, ten minste jaarlijks, op de volgende criteria:
      (1) Werken conform de gedragsregels.
      (2) Adequaat hanteren van doelbinding.
      (3) Noodzakelijkheid, rechtmatigheid, juiste en volledige verwerking van politiegegevens.
      (4) Alleen verwerken van bijzondere politiegegevens wanneer dit onvermijdelijk is.
      (5) Documentatie van de herkomst van politiegegevens.
      (6) Onderscheiding tussen feitelijke en subjectieve gegevens, c.q. feiten en persoonlijke oordelen.
      (7) Onderscheiden tussen verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers, getuigen en veroordeelden.
      (8) Vastlegging van ter beschikkingstellingen en verstrekkingen.

   ii) Correcte en tijdige uitvoering van verzoeken van betrokkenen, zoals vernietiging en rectificatie van politiegegevens.
   iii) Toewijzing van autorisaties.
   iv) Bewustmaking en opleiding van Boa's en andere geautoriseerden.
   v) De audits.
   vi) Toetsen van tijdige uitvoering en/of actualisering van DPIA incl. privacy by design and default.

vii) Toetsten van het testen en evalueren van de doeltreffendheid van de be-heersmaatregelen, bijvoorbeeld n.a.v. de DPIA.
viii) Controle van volledigheid en juistheid van het verwerkingenregister voor zover het Wpg verwerkingen betreft.

13) Interne en externe Wpg audits worden gecoördineerd door de stafafdeling Concern-control.
14) Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en – indien van toepassing- bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

6.2: SPECIFIEK BELEID TEN AANZIEN VAN HET CLUSTER VEILIGHEID

De BAR-organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

6.3: SPECIFIEK BELEID TEN AANZIEN POLITIEGEGEVENS BIJ DE UITVOERING VAN DE LEERPLICHTWET

De BAR-organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder Art 16 lid 5 en Art 26. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

6.4: SPECIFIEK BELEID TEN AANZIEN POLITIEGEGEVENS BIJ DE UITVOERING VAN DE PARTICIPATIEWET

De BAR-organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving in het kader van de Participatiewet door de Sociale Recherche. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

6.5: SPECIFIEK BELEID TEN AANZIEN POLITIEGEGEVENS BIJ DE UITVOERING VAN BOUW- EN WONINGTOEZICHT

De BAR-organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving met betrekking tot bouw- en woningtoezicht. Daarom zijn binnen dit taakveld geen Boa's aangesteld en is de Wpg niet van toepassing.

7: PUBLICATIE EN WIJZIGINGEN

Dit document staat voor alle medewerkers ter inzage op het intranet en wordt op aanvraag ter beschikking gesteld aan andere belanghebbenden. Dit document wordt periodiek geactualiseerd. De geactualiseerde versie wordt op het intranet gepubliceerd en de medewerkers worden daarop geattendeerd.

Het Algemeen Bestuur van de BAR-organisatie op 19 oktober 2022

De heer H.W.J. Klaucke
Secretaris

Mevrouw A. Attema
Voorzitter BAR-organisatie

BIJLAGE 1: ROLLEN EN NAMEN

Dit overzicht wordt ingevuld en bijgehouden door de CPO en de CISO, mede op basis van de benoemingen van DAPI door de Cluster-managers en teamleiders en gepubliceerd op intranet. Hier is afgezien van het invullen van namen in verband met wijzigingen en de publicatie van dit beleid.

Rol	Naam	Vervanger
Chief Information Security Officer (CISO)		
Operationeel/Technisch ISO (TISO)		
Operationeel ISO Maatschappij en Veiligheid, Ensia en projecten		
Coördinerend Privacy Officer (CPO)		
Operationeel Privacy Officer		
Operationeel PO Maatschappij en Veiligheid en Projecten		
Controller Informatiebeveiliging en Privacy		
Functionaris Gegevensbescherming		
DAPI Cluster Staf (Concerncontrol, Financiën en Strategie)		
DAPI Dienstverlening (incl. BRP, WD)		
DAPI Cluster I&A		
DAPI Juridische Zaken en Inkoop		
DAPI Cluster Uitvoering		
DAPI Cluster Voorbereiding en Beheer		
DAPI Cluster Facilitair		
DAPI Cluster Ontwikkeling leefomgeving en regio		
DAPI Cluster Ruimtelijke Ontwikkeling		
DAPI Cluster Vastgoed		
DAPI Cluster Ontwikkeling Mens en Organisatie		
DAPI Cluster Veiligheid – team BOA		
DAPI Cluster Veiligheid – APV en OOV		
DAPI Cluster Maatschappij – Team Participatie, schulddienstverlening & wijkteams incl. SUWI		
DAPI Cluster Maatschappij – Team Leerplicht & Jeugd		
DAPI Cluster Maatschappij – Team WMO		