DE BEDRIJFSVOERINGS PARTNER

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 3109

12 december 2025

Officiële uitgave van de gemeenschappelijke regeling De Bedrijfsvoeringspartner

Strategisch privacybeleid 2025 – 2028 DBP

Samenvatting Privacybeleid DBP 2025-2028

Het waarborgen van privacy is essentieel voor het vertrouwen van inwoners, medewerkers en partners in onze dienstverlening. Persoonsgegevens vormen een integraal onderdeel van veel werkprocessen. Zorgvuldige omgang met deze gegevens is nodig om zowel wetgeving na te leven als ethisch verantwoord te handelen. Transparantie, veiligheid en respect voor betrokkenen staan daarom centraal in het beleid van De BedrijfsvoeringsPartner (DBP).

Kern van het beleid

Het privacybeleid 2025–2028 van DBP geeft richting aan een zorgvuldige, rechtmatige en transparante omgang met persoonsgegevens. De nadruk ligt op het voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en het implementeren van passende beheersmaatregelen binnen alle lagen van de organisatie.

Ambitieniveau

DBP streeft volwassenheidsniveau 3 na (volgens CIP-model): voldoen aan wet- en regelgeving én actief risicobeheer op bestuurlijk niveau.

Acties om dit te realiseren:

- Inventarisatie huidige situatie en risico's;
- Integratie van privacy in processen, beleid en systemen;
- PDCA-cyclus: plannen, uitvoeren, controleren en verbeteren van privacymaatregelen.

Beheersmaatregelen & borging

- Register van verwerkingen en DPIA's;
- Verwerkersovereenkomsten;
- Melden en evalueren van datalekken;
- Bewustwordings- en trainingsprogramma's voor medewerkers;
- Drie verdedigingslinies en interne/externe audits.

Tot slot

DBP borgt privacy in nauwe samenhang met informatiebeveiliging. Het beleid draagt bij aan vertrouwen, verantwoording en continu verbeteren binnen een complexe publieke context. Dit beleid markeert een gezamenlijke stap in het versterken van de privacy-cultuur binnen en namens de deelnemende gemeenten.

Het Bestuur en de voorzitter van De BedrijfsvoeringsPartner, ieder voor zover het zijn / haar bevoegdheid betreft,

Overwegende dat:

De BedrijfsvoeringsPartner kaders heeft vastgesteld voor de privacyborging van persoonsgegevens die door of namens de gemeente worden verwerkt bij de uitvoering van haar (wettelijke) taken;

Gelet op artikel 24, lid 2 Algemene verordening gegevensbescherming

BESLUIT:

Vast te stellen het "Privacybeleid 2025-2028 DBP"

Dit privacybeleid geeft richting aan de wijze waarop binnen De BedrijfsvoeringsPartner (hierna DBP) wordt gezorgd voor een adequate, zorgvuldige en rechtmatige omgang met persoonsgegevens en de borging daarvan. Dit beleid beschrijft op hoofdlijnen (de 'wat') waar wij de aankomende tijd nadruk op leggen, mede richting gegeven door maatschappelijke en technologische ontwikkelingen. De daadwerkelijke uitvoering (de 'hoe') valt buiten de scope van dit privacybeleid en zal in procedures en werkinstructies beschreven worden.

Doelgroep
In dit beleid wordt onder "medewerker" verstaan eenieder die namens DBP op grond van een mandaat, machtiging of een geattribueerde bevoegdheid gegevens verwerkt.
Hieronder wordt in ieder geval begrepen:

- Eenieder die op grond van een arbeids-, inhuur-, uitzendkracht-, detacheringsovereenkomst onder gezag staat van het Bestuur van DBP; – zelfstandigen zonder personeel (ZZP'ers).

Toepasselijke regelgeving
Dit privacybeleid is opgesteld conform:

- 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 volgende maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO); Control: 18.1.1; 18.1.3; 18.1.4; Overheidsmaatregel: 18.1.3.1; 18.1.4.1; 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 DBP.

Bereik
Dit privacybeleid is vastgesteld en van toepassing op alle medewerkers binnen DBP en alle betrokkenen met wie DBP werkt en draagt bij aan transparantie over de manier waarop DBP omgaat met persoonsgegevens.

Dit privacybeleid is van toepassing op DBP en alle uit te voeren werkprocessen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verwerkingen).

Dit beleid is opgesteld rekening houdende met privacy in het kader van de Algemene Verordening Gegevensbescherming (AVG) en andere relevante privacy wet- en regelgeving.

Verantwoordelijkheid en naleving
Het Bestuur en de voorzitter van DBP, de (coördinerend) Privacy Officer(s) en de proceseigenaren (clustermanagers) bevorderen de naleving van dit privacybeleid, de algehele communicatie en bewustwording (awareness) rondom privacy.

Beheer & herziening
Het inhoudelijke beheer van dit document berust bij de Coördinerend Privacy Officer (CPO) van DBP. Het privacybeleid wordt ten minste elke drie jaar herzien, of eerder indien omstandigheden en wet- en regelgeving daartoe vragen.

1: INLEIDING

Bij DBP streven we naar een slagvaardige en effectieve organisatie die hoogwaardige dienstverlening biedt aan onze partners. Onze medewerkers zetten zich in om nauw betrokken te zijn bij wat er leeft binnen onze eigen organisatie en die van onze gemeentelijke partners. Bij het uitvoeren van onze taken hechten we grote waarde aan de privacy van de personen van wie wij persoonsgegevens verwerken en gaan we zorgvuldig om met persoonlijke gegevens. Dit privacybeleid beschrijft hoe we dit waarborgen.

DBP voert haar werkzaamheden grotendeels uit onder mandaat en in lijnverantwoordelijkheid van de colleges van burgemeester en wethouders van de gemeenten Albrandswaard, Barendrecht en Ridderkerk. Dit betekent dat persoonsgegevens die worden verwerkt in het kader van gemeentelijke taken, in opdracht en onder de juridische verantwoordelijkheid van de betreffende gemeente vallen. DBP ondersteunt en faciliteert deze verwerkingen voor de diensten die zijn overeengekomen en waarvoor we zijn gemandateerd. We zijn geen verwerkingsverantwoordelijke voor deze gegevens. Voor de interne bedrijfsvoering, zoals personeelszaken en bedrijfsvoering van DBP zelf, is DBP wel verwerkingsverantwoordelijke.

De hoofdlijnen van dit privacybeleid zijn:

- Naleving van privacywetgeving (AVG, UAVG);
- Rollen en verantwoordelijkheden;
- De aanpak en beheersmaatregelen;
- Risicomanagement;
- Privacy by design en default standaard toepassen in processen;

Privacy en gegevensbescherming

DBP werkt met persoonsgegevens van betrokkenen. Betrokkenen zijn alle personen van wie de DBP persoonsgegevens verwerkt, zoals inwoners van de gemeentelijke partners, medewerkers, ondernemers en bezoekers. In sommige gevallen werken we ook met gevoelige en bijzondere persoonsgegevens.

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, kentekens en cookies op de website.

Binnen DBP vormen de AVG en de UAVG de wettelijke kaders voor het verwerken van persoonsgegevens. Deze wetgeving staat in het bredere kader van het grondrecht op privacy, zoals vastgelegd in het EVRM en het EU-Handvest. Binnen onze organisatie verwerken ook teams zoals de zorgadministratie, die gemeentelijke partners ondersteunen, gevoelige gegevens van burgers. Het is daarom essentieel dat dit met zorg en respect voor de privacy van deze betrokkenen gebeurt.

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

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

Bij de bescherming van persoonsgegevens staat de betrokkene centraal. DBP is transparant richting alle betrokkenen over de wijze waarop met persoonsgegevens wordt omgegaan en is dienstverlenend bij vragen en klachten hierover. Betrokken moeten kunnen vertrouwen op de wijze waarop wordt omgegaan met persoonsgegevens. Nieuwe technologische ontwikkelingen die DBP in staat stellen om persoonsgegevens beter te beschermen en beveiligen, worden waar noodzakelijk toegepast.

Rechtmatigheid, behoorlijkheid, transparantie

Het grootste deel van de verwerkingen van DBP, worden uitgevoerd op basis van mandaat. DBP gaat uit van de geldende wet- en regelgeving voor privacy en hanteert de AVG als basis. Voor verwerking van persoonsgegevens binnen DBP moet er dus altijd een rechtmatige grondslag bestaan.

DBP onderschrijft de rechten van betrokkenen zoals deze zijn gegeven op grond van de AVG en in voorkomende gevallen, zoals die zijn gegeven in bijzondere wetten zoals de Wet basisregistraties personen.

DBP is open en transparant over hoe zij met persoonsgegevens omgaat. Persoonsgegevens zullen nooit voor commercieel gewin worden gebruikt.

Doelbinding

DBP verwerkt slechts persoonsgegevens wanneer dit noodzakelijk is voor het doel van de verwerking.

Opslagbeperking

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, sectorale wetgeving, de Archiefwet en bijbehorende Selectielijst, waarbij de wetgeving voor gaat op de selectielijst. De proceseigenaar is verantwoordelijk voor tijdige archivering, dan wel vernietiging van persoonsgegevens.

Integriteit en vertrouwelijkheid

Persoonsgegevens worden goed beveiligd opgeslagen, zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van ‘privacy by design’ besteedt DBP al tijdens de ontwikkeling, voor zowel eigen bedrijfsvoering als in opdracht van de gemeenten, van producten en diensten (zoals informatiesystemen) aandacht aan privacyverhogende maatregelen.

Medewerkers verwerken alleen persoonsgegevens die noodzakelijk zijn voor hun taakuitvoering. Daarbij wordt gezorgd voor passende organisatorische en technische beveiliging ter bescherming van de persoonsgegevens, zoals zorg dragen voor het ‘loggen’ (het vastleggen van met data uitgevoerde handelingen) daar waar dat noodzakelijk is. Er wordt gewerkt met geheimhoudingsverklaringen voor

externen en leveranciers en met externe partners worden convenanten en/of verwerkersovereenkomsten afgesloten.

Dataminimalisatie

DBP streeft naar minimale gegevensverwerking.

Alleen die persoonsgegevens worden verwerkt die in redelijke verhouding staan tot het doel van de verwerking. Als het doel kan worden bereikt met een minder ingrijpende verwerking, dan streven wij ernaar om voor die verwerking te kiezen. Op deze manier houden wij de inbreuk op de persoonlijke levenssfeer van de burger zo beperkt mogelijk.

Het uitgangspunt geldt dat DBP geen bijzondere persoonsgegevens registreert die aanleiding kunnen geven tot discriminatie. DBP registreert geen bijzondere persoonsgegevens waaruit bijvoorbeeld gezondheid, religieuze of levensbeschouwelijke overtuiging, politieke opvattingen, ras of etnische afkomst, of seksuele voorkeur blijkt. Uitzonderingen hierop zijn enkel mogelijk als de wet dit vereist of toestaat.

Ambitie

DBP streeft ernaar te voldoen aan de basisvereisten van de AVG en heeft hiervoor haar ambitieniveau bepaald aan de hand van de vijf volwassenheidsniveaus die het Centrum Informatiebeveiliging en Privacybescherming (CIP) hanteert.

Het CIP is een publiek-private netwerkorganisatie die zich richt op het verbeteren van informatiebeveiliging en privacybescherming binnen de overheid. Het model van het CIP is voor DBP een waardevol instrument, omdat het een gestructureerde en stapsgewijze aanpak biedt om volwassenheid op het gebied van privacybeheer te verbeteren.

Het gewenste ambitieniveau voor DBP is niveau 3, wat inhoudt dat wordt voldaan aan de geldende wet- en regelgeving. Dit betekent dat de gemeente niet alleen de wettelijke eisen naleeft, maar ook actief inzicht heeft in de risico's die gepaard gaan met gegevensverwerking en deze bewust beheert op bestuurlijk niveau.

Om dit ambitieniveau te bereiken zijn en worden de volgende stappen gezet:

- Huidige situatie in kaart brengen: Het vaststellen van het huidige niveau van privacybeheer binnen de organisatie om te bepalen welke verbeteringen nodig zijn.
- Risicobeheer: Het verkrijgen van inzicht in de risico's die gepaard gaan met gegevensverwerking en het bewust beheren van deze risico's op bestuurlijk niveau.
- Integratie van privacy: Het structureel integreren van privacy in processen, systemen en beleid binnen DBP.

In overeenstemming met de AVG implementeren we passende organisatorische en technische maatregelen die aantoonbaar zijn. Dit omvat het vastleggen en communiceren van procedures en werkinstructies, zodat rollen en verantwoordelijkheden duidelijk zijn en er adequaat kan worden gehandeld.

In lijn met de AVG vereist dit de implementatie van passende organisatorische en technische maatregelen, die bovendien aantoonbaar zijn. Dit omvat het vastleggen en communiceren van onderliggende procedures en werkinstructies, zodat rollen en verantwoordelijkheden helder zijn en er adequaat kan worden gehandeld.

2. UITGANGSPUNTEN EN KADERS

Wettelijk kader

De wettelijke kaders voor het verwerken van persoonsgegevens zijn voor de DBP 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).
- wetten ten aanzien van de taakuitvoering van gemeenten, wanneer handelend onder mandaat, 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.

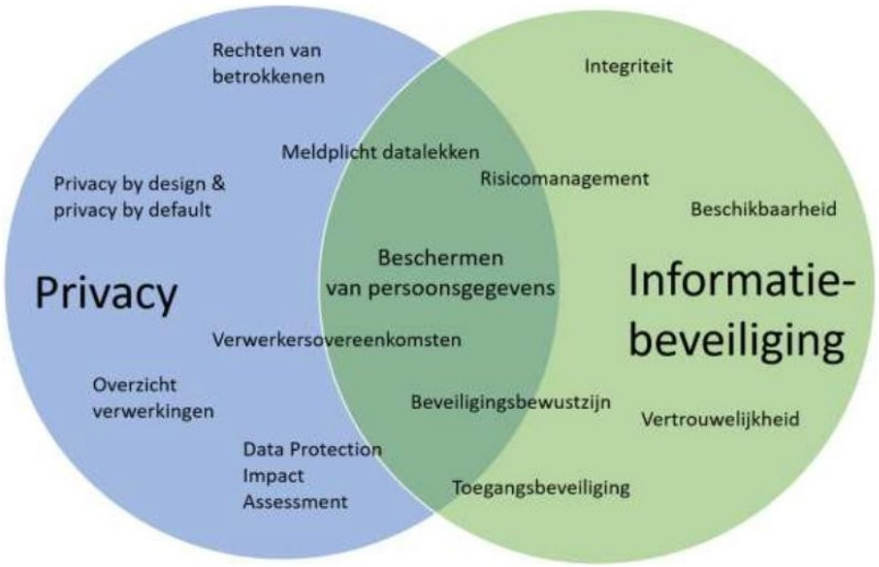
In situaties waarin DBP werkzaamheden uitvoert onder mandaat van de gemeenten, zijn de colleges van B&W van de betreffende gemeenten verwerkingsverantwoordelijke. DBP verwerkt in die gevallen persoonsgegevens vanuit het mandaat van de gemeenten, als vastgelegd in de mandaatbesluitregelingen. Voor de eigen bedrijfsvoeringsactiviteiten (zoals HR, interne bedrijfsvoering en contractbeheer) is DBP zelf verwerkingsverantwoordelijke.

Daarnaast committeert DBP 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. Ook is het uitgangspunt het gebruik maken van de verwerkersovereenkomst van de VNG. 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; 18.1.3; 18.1.4;
- Overheidsmaatregel: 18.1.3.1; 18.1.4.1; 18.1.4.2.

Relatie tussen Privacy en Informatiebeveiliging

Betrokkenen hebben het recht op privacy en bescherming van hun persoonlijke gegevens. Dit betekent dat er zorgvuldig moet worden omgegaan met deze gegevens en dat ze goed beveiligd moeten worden. Ook moeten alle regels rondom privacy worden gerespecteerd. Het beschermen van persoonsgegevens is een belangrijk gebied waarin privacy en informatiebeveiliging samenkomen, omdat beide nodig zijn om ervoor te zorgen dat gegevens veilig blijven en niet zomaar toegankelijk zijn voor anderen.



Dit privacybeleid beschrijft hoe persoonsgegevens die worden verwerkt door of namens de drie gemeenten worden beschermd. Het borgen van de beveiliging van deze informatie is beschreven in een afzonderlijk informatieveiligheidsbeleid.

In de praktijk is er een nauwe samenwerking tussen informatiebeveiliging en privacy, bijvoorbeeld bij bewustwording en training van medewerkers, bij het adviseren over en beoordelen van nieuwe applicaties en de uitvoering van een risicoanalyse op een proces.

Risicomanagement

DBP 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).

DBP wil “in control” zijn, dat wil zeggen overzicht hebben van waar de risico's op het gebied van privacy liggen en deze risico’s bewust beheren op bestuurlijk niveau.

Om het risicomanagement te versterken hanteert DBP drie verdedigingslinies, te weten:

1. Het in kaart hebben van mogelijke risico’s tijdens de uitvoering van werkprocessen binnen de afdeling onder verantwoordelijkheid van de lijnmanager. Dat wil zeggen: hoog risico verwerkingen in beeld, 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.
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. Daaronder valt ook de evaluatie van de opzet, bestaan en werking van de 1e en de 2e verdedigingslinie.

Borging

De borging van het beheersen en verbeteren van privacy wordt meegenomen in de plan do-check-act cyclus en bestaat uit:

Plan: inrichten en documenteren van de beheersmaatregelen en DBP-brede aanpak van privacy op basis van geldende normen, wettelijke eisen en risico’s voor DBP (in termen van interne controle: de opzet, 1e verdedigingslinie).

Do: aantonen van de uitvoering van beheersmaatregelen en DBP-brede aanpak van privacy (in termen van interne controle: het bestaan, 1e verdedigingslinie).

Check: de borging/controle en evaluatie van de beheersmaatregelen en DBP-brede 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 DBP-brede aanpak van privacy op basis van bovengenoemde evaluatie (in termen van interne controle: de opzet, 1e verdedigingslinie).

Beheersmaatregelen

Om te komen tot passende beheersmaatregelen wordt gebruik gemaakt van raamwerken met beheersmaatregelen om te waarborgen dat de wetgeving adequaat wordt afgedekt. Voorbeelden van beheersmaatregelen zijn het hebben van een up-to-date en volledig register van verwerkingen en algoritmeregister, het informeren van betrokkenen, het overeenkomen en beoordelen van verwerkersovereenkomsten en het uitvoeren van Data Protection Impact Assessments (DPIA’s).

Externe partijen

DBP verlangt van externe partijen die gegevens in opdracht van de organisatie verwerken en ketenpartners waarmee gegevens van betrokkenen worden uitgewisseld dat zij aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging en borging van privacy.

Medewerkers

Wanneer dit beleid en/of beheersmaatregelen eisen stelt aan taken en verantwoordelijkheden van medewerkers dan worden deze opgenomen in aanvullende individuele afspraken, welke in specifieke procedures en werkinstructies staan, of zullen worden, opgenomen.

3. ROLLEN EN VERANTWOORDELIJKHEDEN

Gezien de bijzondere positie van DBP als bedrijfsvoeringsorgansiatie voor drie gemeenten en het feit dat elke gemeente een eigen privacybeleid en formeel aangestelde Functionaris Gegevensbescherming (FG) heeft, wordt samenwerking met de gemeentelijke FG geborgd door regelmatige afstemmingsoverleggen.

Daarbij wordt de uitvoering van privacy ondersteund door:

- alle **medewerkers** die verantwoordelijk zijn voor het uitvoeren van het privacybeleid als onderdeel van hun professionele verantwoordelijkheid.
- **leidinggevenden**/proceseigenaren die
  - Verantwoordelijk zijn voor de uitvoering van het privacybeleid en de beheersmaatregelen binnen hun cluster of team. Informatiesystemen en processen die door meerdere organisatieonderdelen worden gebruikt, vallen onder de verantwoordelijkheid van de systeemeigenaar;
  - Zorgen voor een adequate inrichting van werkprocessen en de aansturing van medewerkers (1e verdedigingslinie);
  - Toezien op de naleving van het beleid en het bevorderen van privacybewustzijn;
  - Onderdelen van beheersmaatregelen uitvoeren, zoals het bijhouden van het verwerkingenregister, het uitvoeren van DPIA's en risicoanalyses, en het beoordelen van toegangsrechten;
  - Relevante wettelijke, statutaire, regelgevende en contractuele eisen voor hun informatiesystemen vaststellen, documenteren en actueel houden;
  - Processpecifieke borgings-/controleactiviteiten uitvoeren, vaak samenhangend met processpecifieke applicaties;
  - Verantwoordelijk zijn voor het nemen van maatregelen om datalekken binnen hun afdeling te voorkomen.

- de Coördinerend Privacy Officer (CPO), die
  - het opstellen, de uitvoering, evaluatie en bijstelling van het beleid en de jaarlijkse verbetercycli coördineert;
  - de implementatie, uitvoering en borging van beheersmaatregelen coördineert en daarover rapporteert;
  - de stuurgroep IV&P en management gevraagd en ongevraagd adviseert over privacy; o de afhandeling en evaluatie van datalekken en verzoeken van betrokkenen coördineert;
  - privacybewustzijn bevordert in de gehele organisatie.

- De Privacy Officer(s) (PO's) van DBP, die:
  - Op operationeel niveau gevraagd en ongevraagd adviseren;
  - Ondersteunen bij de uitvoering van het privacybeleid en het jaarplan;
  - Helpen bij de implementatie en uitvoering van beheersmaatregelen, zoals DPIA's, verzoeken van betrokkenen, de afhandeling en evaluatie van datalekken en het bevorderen van privacybewustzijn en het bijhouden van het register van verwerkingen.

- De Functionaris Gegevensbescherming (FG) van DBP, die:
  - De BedrijfsvoeringsPartner informeert en adviseert over de verplichtingen uit de AVG; Toeziet op de naleving van de AVG binnen DBP;
    - Op verzoek advies geeft over risicoanalyses;
    - Samenwerkt met de toezichthouder (Autoriteit Persoonsgegevens);
    - Optreedt als contactpunt voor de Autoriteit Persoonsgegevens;
    - Rechtstreeks verslag uitbrengt aan het bestuur van DBP;
    - Jaarlijks een verslag met aanbevelingen opstelt.

- De Chief Information Security Officer (CISO) van DBP, die:
  - Het opstellen, de uitvoering, evaluatie en bijstelling van het informatiebeveiligingsbeleid en de jaarlijkse verbetercycli coördineert;
  - De implementatie, uitvoering en borging van beveiligingsmaatregelen coördineert;
  - Rapporteert over beveiligingsincidenten aan de Stuurgroep IV&P en rechtstreeks verslag kan doen aan het CMT;
  - Het management gevraagd en ongevraagd adviseert over informatiebeveiliging;
  - Beveiligingsincidenten registreert in een incidentenregister en de afhandeling en evaluatie hiervan coördineert;
  - Beveiligingsbewustzijn bevordert in de gehele organisatie.

- Directeur van DBP: verantwoordelijk voor de integratie van informatieveiligheid en privacy in de gemeentelijke processen.
- Het team control, dat:
  - interne audits coördineert, bijvoorbeeld: de Verbijzonderde Interne Controles (VIC) en het onderzoeksplan doelmatigheid en doeltreffendheid op basis van Art 213a van de Gemeentewet;
  - externe audits coördineert, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening.

- De **Stuurgroep Informatieveiligheid en privacy (IV&P)** heeft de verantwoordelijkheid voor het toezicht op informatieveiligheid en privacy binnen DBP en vervult een kaderstellende en toezichthoudende rol richting de gemeenten.
  - o Directeur DBP
  - o Chief Information Security Officer (CISO)
  - o Chief Privacy Officer (CPO)
  - o Clustermanager I&A
  - o Teamleider Control

- **Het CMT** van De BedrijfsvoeringsPartner heeft de eindverantwoordelijkheid voor het toezicht op informatieveiligheid en privacy binnen DBP.

4. DE AANPAK VAN PRIVACY

Jaarcyclus

Bij uitvoering van gemeentelijke taken onder mandaat worden persoonsgegevens verwerkt in overeenstemming met het privacybeleid en de specifieke richtlijnen van de verantwoordelijke gemeente. DBP borgt dat medewerkers zich bewust zijn van deze kaders. De FG van de gemeente behoudt in deze situaties zijn/haar formele rol als toezichthouder. DBP ondersteunt de FG van de gemeente met benodigde informatie en rapportages.

Om de borging van het privacybeleid en de daarvan afgeleide plannen te realiseren, doorloopt DBP de onderstaande Plan, Do, Check, Act (PDCA)-cyclus, zowel organisatiebreed als per beheersmaatregel.

Plan: Team IV&P binnen DBP stelt een driejarenplan met verbeterpunten op, rekening houdend met de strategie en –doelstellingen van DBP, risico's, regelgeving (waaronder eventuele wijzigingen in de wetgeving), de stand van de techniek, beschikbare middelen en het advies van de FG. Het plan bevat meetbare doelen en een activiteitenplanning met rollen en verantwoordelijkheden, benodigde middelen, tijdslijnen en resultaten.

Do: Het jaarplan en de beheersmaatregelen worden uitgevoerd, waarbij beheersmaatregelen stapsgewijs worden ingevoerd en verbeterd. Onder de beheersmaatregelen vallen onder andere:

- Onderhouden van het register van verwerkingen;
- Actief informeren van betrokkenen;
- Afhandelen van datalekken en verzoeken van betrokkenen;
- Afsluiten van verwerkersovereenkomsten met leveranciers en controle van de naleving daarvan;
- Naleven van bewerkings- en verwerkingstermijnen;
- Uitvoeren van DPIA's.

De uitvoering van het jaarplan en de beheersmaatregelen wordt bewaakt door de CPO van DBP, waarbij systeem- en proceseigenaren zorgen voor de naleving in de operationele processen.

Check: Borgings-/controleacties worden uitgevoerd om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd en effectief zijn. De borgings-/controleacties worden opgenomen in een controleplan, zodat alle geïmplementeerde maatregelen passend worden afgedekt.

De FG geeft onafhankelijk advies over de naleving van de AVG tijdens de evaluaties in de Check-fase en rapporteert hierover aan het bestuur en de Voorzitter van DBP.

Act: Team IV&P zal bijsturen, herprioriteren en/of aanvullende maatregelen nemen of aanbevelingen doen voor het volgende verbeterplan op basis van de resultaten in de Check-fase, inclusief aanbevelingen uit interne en externe audits en incidentrapportages. Hiermee zorgt DBP voor een continue verbetering van privacy.

5. PRIVACY BEHEERSMAATREGELEN

Bewustwording en training

Het team IV&P stelt jaarlijks een bewustwordings- en trainingsplan op voor zowel DBP als de 3 deelnemende gemeenten en coördineert de uitvoering. Bij het opstellen van het bewustwordings- en trainingsplan wordt rekening gehouden met aanbevelingen van de FG en trends in bedreigingen en maatschappelijke ontwikkelingen.

REGISTER VAN VERWERKINGEN

DBP zorgt voor een up-to-date en volledig register van verwerkingen voor de interne werkprocessen van de DBP. DBP streeft ernaar om het Register van verwerkingen zo in te richten dat deze eenvoudig kan worden ingezien wanneer dat opgevraagd wordt.

Data Protection Impact Assessment

In het geval van nieuwe of gewijzigde hoog risico verwerkingen is het uitgangspunt dat er een Data Protection Impact Assessment (DPIA) wordt uitgevoerd. Daarbij hanteren wij een gestandaardiseerde werkwijze: een pre-scan bepaalt of een DPIA nodig is; zo ja, wordt deze uitgevoerd middels een vast format.

De proceseigenaar is verantwoordelijk voor uitvoering en opvolging; het Privacy Office biedt inhoudelijke ondersteuning. bevindingen en verbetermaatregelen uit DPIA's worden gemonitord.

Datalekken

Medewerkers zijn gehouden datalekken, beveiligingsincidenten en kwetsbaarheden te melden. Datalekken binnen DBP en de deelnemende gemeenten worden centraal en via Topdesk gemeld en indien nodig tijdig gemeld aan de AP en/of betrokkenen.

Alle meldingen worden opgenomen in een datalekregister. Daarin wordt per melding aangegeven of er sprake is van een datalek, of melding aan AP en/of betrokkene verplicht is en een schriftelijke onderbouwing en de mogelijke acceptatie van risico's door het management.

Datalekken worden maandelijks 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. Dit is een mooi voorbeeld van de PDCA-cyclus.

Transparantie en Rechten van betrokkenen

DBP informeert betrokkenen over de verwerking van persoonsgegevens en over zijn/haar rechten. DBP heeft als doel om dit zo efficiënt mogelijk te doen, door:

- Dit op te nemen op een zo begrijpelijk mogelijke wijze in de privacyverklaring op de website.

Inwerkingtreding

"Privacybeleid gemeente De BedrijfsvoeringsPartner 2025 – 2028" treedt in werking de dag na publicatie

Aldus besloten op 12 november 2025,

Bestuur van de Bedrijfsvoeringspartner

de directeur,
H.T. van Bochove

de bestuurders:

H. van Os

C. Pille,

M. Stolk,