RIDDERKERK

GEMEENTEBLAD

Officiële uitgave van de gemeente Ridderkerk

Nr. 300193

9 juli

2025

Privacybeleid gemeente Ridderkerk 2025 - 2027

het college van burgemeester en wethouders van de gemeente Ridderkerk

Overwegende dat;

Ons college kaders heeft vastgesteld voor de privacy-borging 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 en artikel 160, lid 1 sub a en c Gemeentewet;

B E S L U I T vast te stellen

Privacybeleid gemeente Ridderkerk 2025 – 2027

Doel
Dit Privacybeleid geeft richting aan de manier waarop binnen gemeente Ridderkerk wordt gezorgd voor een adequate, zorgvuldige en rechtmatige omgang met persoonsgegevens van zowel burgers, inwoners en medewerkers (hierna: betrokkenen) en de borging daarvan. Dit privacybeleid beschrijft op hoofdlijnen (de 'wat') waar de gemeente Ridderkerk de aankomende tijd nadruk op legt, mede richting gegeven door maatschappelijke ontwikkelingen en wet- en regelgeving. De daadwerkelijke uitvoering (de 'hoe') valt buiten de scope van dit beleid en zal in procedures en werkinstructies beschreven worden.

Doelgroep
In dit beleid wordt onder "medewerker" verstaan een ieder die namens een bestuursorgaan van de gemeente Ridderkerk op grond van een mandaat, machtiging of een geattribueerde bevoegdheid gegevens verwerkt ter uitvoering van de (wettelijke) taken van de gemeente.
Hieronder wordt in ieder geval begrepen:
- een ieder die op grond van een arbeids-, inhuur-, uitzendkracht-, detacheringsovereenkomst onder gezag staat van het college of het Bestuur van DBP (DBP);
- Zelfstandige zonder personeel (ZZP'ers);
- Buitengewoon opsporingsambtenaren (boa's), ambtenaren burgerlijke stand, leerplichtambtenaren, toezichthouders, heffings- en invorderingsambtenaren.

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

Dit privacybeleid is van toepassing op de Gemeente Ridderkerk en alle uit te voeren werkprocessen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verwerkingen), inclusief gegevensverwerkingen door Gemeente Ridderkerk in opdracht van derden.

Dit beleid is opgesteld rekening houdende met privacy in het kader van de Algemene verordening privacy (AVG) en andere relevante privacy wet- en regelgeving. De Wet Politiegegevens (Wpg) wordt eveneens behandelt, omdat de Gemeente Ridderkerk ook persoonsgegevens verwerkt die onder de Wpg vallen.

Versie
maart 2025

Verantwoordelijkheid en naleving
Het college van burgemeester en wethouders (B&W) is verantwoordelijk voor de vaststelling van dit privacybeleid en de te stellen kaders.

Voor het bevorderen van de naleving van dit privacybeleid, de algehele communicatie en bewustwording (awareness) rondom privacy dragen zorg:
1. ons college,
2. het management van de gemeente,

3. het management van DBP (DBP),
4. de proceseigenaren van de gemeente en DBP,
5. de (Coördinerend) Privacy Officer(s) van DBP.

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

De visie van de gemeente Ridderkerk is gericht op het bevorderen van een leefbare, veilige en toekomstbestendige gemeente. Dit doen we op duidelijke, realistische en zakelijke wijze. Ons handelen wordt bepaald door de behoeften en de opgaven van onze inwoners, ondernemers en maatschappelijke instellingen. De kernwaarden van Ridderkerk zijn betrouwbaar, betrokken, persoonlijk en modern.

De gemeente Ridderkerk werkt met persoonsgegevens van betrokkenen. Betrokkenen zijn alle personen van wie de gemeente persoonsgegevens verwerkt, zoals inwoners, medewerkers, ondernemers en bezoekers. In sommige gevallen werken we ook met gevoelige en bijzondere persoonsgegevens. Te denken valt aan het Burgerservicenummer (BSN), gegevens in de Basisregistratie personen (BRP), gezondheidsgegevens bij de uitvoering van de Wet maatschappelijke ondersteuning 2015 (Wmo) en de Jeugdwet en politiegegevens verwerkt door Boa's. 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, kentekens en cookies op de website.

Kaders voor het verwerken van persoonsgegevens en daarmee voor het waarborgen van de privacy van betrokkenen zijn voor gemeente Ridderkerk de Algemene verordening gegevensbescherming (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) en het Handvest van de Grondrechten van de EU (Handvest EU).

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 en rechtmatige werking van werkprocessen van de gemeente Ridderkerk en samenwerking met andere organisaties mogelijk te maken in de maatschappelijke context waarin Gemeente Ridderkerk zich beweegt.

Bij de bescherming van persoonsgegevens staat de betrokkene centraal. Gemeente Ridderkerk is transparant richting alle betrokkenen over de wijze waarop met persoonsgegevens wordt omgegaan en is dienstverlenend bij vragen en klachten hierover. Betrokkenen moeten kunnen vertrouwen op de manier waarop gemeente Ridderkerk omgaat met persoonsgegevens. Nieuwe technologische ontwikkelingen die gemeente Ridderkerk in staat stellen om persoonsgegevens beter te beschermen en beveiligen, worden waar noodzakelijk toegepast. De gemeente Ridderkerk streeft ernaar om bij het verwerken van persoonsgegevens uitsluitend te handelen conform de privacy beginselen.

Gemeente Ridderkerk wordt ondersteund op het gebied van privacy door DBP, om optimale bescherming van persoonsgegevens te kunnen waarborgen. DBP voert op grond van mandaten de bedrijfsvoeringstaken van de gemeente uit. Hier is onder andere het beheer van alle geautomatiseerde systemen, technische gegevensverwerking, privacy-advisering en gedeeltelijk uitvoering in onder gebracht.

Rechtmatigheid, behoorlijkheid, transparantie
De gemeente Ridderkerk houdt zich aan de geldende privacywet- en regelgeving, waarbij de AVG als uitgangspunt dient. De gemeente Ridderkerk erkent en respecteert de rechten van betrokkenen, zoals vastgelegd in de AVG en in specifieke wetten, zoals de Wet basisregistratie personen.

Daarnaast hanteert de gemeente het principe van 'éénmalige vastlegging, meervoudig gebruik', tenzij dit niet mag of praktisch niet uitvoerbaar is. Dit houdt in dat gegevens die al bekend zijn, niet onnodig opnieuw worden opgevraagd. Waar mogelijk wordt gebruikgemaakt van brongegevens uit het stelsel van basisregistraties.

Transparantie is een belangrijk uitgangspunt: de gemeente is duidelijk over hoe zij met persoonsgegevens omgaat en welke gegevens zij met derden deelt binnen een specifiek doel, tenzij wettelijke of andere gerechtvaardigde belangen zich daartegen verzetten.

Persoonsgegevens van inwoners worden niet gedeeld met derden, tenzij dit noodzakelijk is voor publieke doeleinden en/of de uitvoering van specifieke wetgeving, zoals bij openbare vergaderingen, of in het sociaal domein. In sommige gevallen kan de gemeente wettelijk verplicht zijn om gegevens te verstrekken, maar dit gebeurt alleen wanneer er geen alternatieve manier is om het doel te bereiken.

Onder geen beding zullen persoonsgegevens voor commerciële doeleinden worden gebruikt.

Doelbinding
Gemeente Ridderkerk hanteert het uitgangspunt alleen persoonsgegevens te verwerken wanneer dit noodzakelijk is voor het doel van de verwerking. Dat wil zeggen dat we (verenigbaar) doel hebben met de persoonsgegevens die we verwerken.

Opslagbeperking
Persoonsgegevens worden niet langer bewaard dan nodig voor het doel waarvoor de persoonsgegevens zijn verzameld of op grond van de bepalingen uit de Archiefwet. 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 en Wpg, sectorale wetgeving, de Archiefwet en de 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 door ontwerp en standaardinstellingen ook wel ‘privacy by design en default’ genoemd besteedt gemeente Ridderkerk al tijdens de ontwikkeling van processen en de implementatie van beleid, applicaties en systemen aandacht aan privacy verhogende maatregelen. Privacy by design betekent dat we al bij het ontwerpen van diensten rekening houden met privacy. Privacy by default houdt in dat we standaard de privacy-instellingen zo instellen dat alleen noodzakelijke gegevens worden verzameld.

Alleen functionarissen waarvan het voor de directe taakuitoefening noodzakelijk is, mogen persoonsgegevens verwerken. Daarbij wordt gezorgd voor passende organisatorische en technische beveiliging van 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
Gemeente Ridderkerk 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 wordt ernaar gestreefd om voor die verwerking te kiezen. Op deze manier wordt de inbreuk op de persoonlijke levenssfeer van de betrokkene zo beperkt mogelijk.

Het uitgangspunt geldt dat gemeente Ridderkerk geen bijzondere persoonsgegevens registreert die aanleiding kunnen geven tot discriminatie. Gemeente Ridderkerk registreert geen bijzondere persoonsgegevens over burgers waaruit bijvoorbeeld hun 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 en het college en/of de burgemeester hiermee instemt. Ook hier geldt weer dat deze situaties gemotiveerd worden voorgelegd. Een wettelijke verplichting is er bijvoorbeeld bij het register van burgerlijke stand, ontheemden, jeugdhulpverlening, Wmo en verwarde personen (bij laatste drie worden gezondheidsgegevens verwerkt).

Ambitie
De gemeente Ridderkerk streeft ernaar om te voldoen aan de geldende wet en-regelgeving en een hoger niveau van privacybewustzijn. De gemeente Ridderkerk heeft haar ambities in kaart gebracht en streeft ernaar de naleving van de privacywetgeving structureel binnen de organisatie te borgen.

Dit vormt de basis om te bepalen waar we nu staan en waar we naartoe willen groeien. Het beoogde hogere niveau houdt in dat de gemeente niet alleen voldoet aan de geldende wet- en regelgeving, maar ook een proactieve aanpak hanteert om grip te krijgen op gegevensverwerkingen.

Dit betekent dat de gemeente:
- Inzicht heeft in de risico's die gepaard gaan met gegevensverwerking;
- Deze risico's bewust beheert op bestuurlijk niveau; en
- Privacy integreert in processen, systemen en beleid.

Om deze ambitie waar te maken, wordt samengewerkt met de DBP. Dit uit zich in acties als het vergroten van kennis en bewustwording binnen de organisatie, het adviseren over implementatie van passende technische en organisatorische maatregelen en het versterken van de samenwerking tussen het team Privacy en de proceseigenaren van de gemeente.

De DBP zal de gemeente Ridderkerk ondersteunen door te adviseren, te controleren en te rapporteren over de voortgang en naleving. Dit zal plaatsvinden doormiddel van kwarttaalrapportages. In overeenstemming met de AVG vereist dit de implementatie van passende organisatorische en technische maatregelen en het aantoonbaar maken van deze maatregelen.

Opbouw privacybeleid
Hoofdstuk 2 van het privacybeleid gaat in op de uitgangspunten van gemeente Ridderkerk 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 gemeente Ridderkerk. In hoofdstuk 4 wordt de aanpak op het gebied van privacy beschreven, waarna het beleid zich richt op de verschillende privacy onderwerpen (hoofdstuk 5). Tot slot gaat hoofdstuk 6 over de Wet politiegegevens.

2. UITGANGSPUNTEN EN KADERS

Wettelijk kader
De wettelijke kaders voor het verwerken van persoonsgegevens zijn voor de gemeente Ridderkerk 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 politiegegeven en het Besluit politiegegevens Boa's.
- 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 gemeente Ridderkerk 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 gemeente Ridderkerk 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
Gemeente Ridderkerk 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).

Gemeente Ridderkerk 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 nemen vanuit bestuurlijk niveau.

Het in kaart brengen van mogelijke privacyrisico's gebeurt aan de hand van risicoanalyses en zal vastgelegd worden in onder andere het Register van verwerkingen en het Algoritmeregister. De bevoegdheid van het clustermanagement is om naar aanleiding van uitgevoerde risicoanalyses besluiten te nemen om risico's te accepteren, te beperken en te vermijden (door de verwerking te staken). Deze bevoegdheid is gemandateerd aan de ambtelijke organisatie en DBP in de vorm van de proceseigenaren, het verantwoordelijke cluster en het verantwoordelijke team. Zie de Mandaatbesluitregeling 2024 van de gemeente Ridderkerk voor de gemeentesecretaris en medewerkers van de gemeente en de BAR-organisatie, De Bedrijfsvoeringspartner.

Om het risicomanagement te versterken hanteert gemeente Ridderkerk drie verdedigingslinies.

De eerste verdedigingslinie richt zich op het identificeren van mogelijke risico's tijdens de uitvoering van werkprocessen binnen de afdeling, onder verantwoordelijkheid van de clustermanager. Dit omvat het in kaart brengen van hoogrisicoverwerkingen, het op orde brengen en documenteren van werkprocessen, het opstellen van passende werkinstructies en het werken volgens vastgelegde afspraken. Hieronder vallen ook integriteitsrichtlijnen bij werving, het uitvoeren van het personeelsbeleid en aansturing van medewerkers.

De tweede verdedigingslinie draait om advisering en de borging en controle van beheersmaatregelen binnen de lijn, uitgevoerd door bijvoorbeeld kwaliteitsfunctionarissen, rechtmatigheidscontrollers, teamleiders of privacy officers van DBP. Het doel is vast te stellen dat werkprocessen conform de af-

spraken verlopen, deze te evalueren en waar nodig aan te passen. Voor privacy wordt dit gecoördineerd door het Informatiebeveiliging & Privacy team van DBP en uitgevoerd volgens een controleplan.

De derde verdedigingslinie bestaat uit onafhankelijke audits uitgevoerd door Team Control. Deze omvatten de interne controles van artikel 33 van de Wet Politiegegevens, DigiD, BRP en ENSIA-audits (onder andere ten behoeve van Suwinet, het register burgerlijke stand, DigiD). De audits evalueren de effectiviteit van de eerste en tweede linies en bieden onafhankelijke assurance (zekerheid) over de interne controle en risicobeheersing, met aanbevelingen voor verbeteringen waar nodig.

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

Plan: Het inrichten en documenteren van beheersmaatregelen en de organisatiebrede aanpak van privacy voor gemeente Ridderkerk, gebaseerd op geldende normen, wettelijke vereisten en risicobeoordelingen (in termen van interne controle: de 'opzet', 1e verdedigingslinie).

Do: Het aantonen van de uitvoering van de beheersmaatregelen en de organisatiebrede aanpak van privacy (in termen van interne controle: het 'bestaan', 1e verdedigingslinie).

Check: Het controleren en evalueren van de beheersmaatregelen en de organisatiebrede privacyaanpak. Hierbij worden criteria als volledige uitvoering en effectiviteit gehanteerd, waarbij ook de voortschrijdende ontwikkeling van technologie en nieuwe bedreigingen worden meegenomen. Dit omvat zowel interne als externe audits (de werking, 2e en 3e verdedigingslinie).

Act: Het aanpassen en/of verbeteren van de beheersmaatregelen en de privacyaanpak van gemeente Ridderkerk op basis van de evaluatie (in termen van interne controle: de opzet en werking, 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
Gemeente Ridderkerk 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 als gemeente Ridderkerk zelf. Het gaat daarbij bijvoorbeeld om IT-leveranciers, maar ook ketenpartners in bijvoorbeeld Wmo en Jeugdzorg, zoals zorginstellingen. Dit wordt gewaarborgd in juridische privacy overeenkomsten.

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

Het college van burgemeester en wethouders is bestuurlijk eindverantwoordelijk voor de privacy- en informatiebeveiligingsdoelstellingen van gemeente Ridderkerk. Het college stelt het beleid vast en ziet toe op de realisatie hiervan via de uitvoerende lagen binnen de organisatie, zoals de directie en het lijnmanagement.

De directie zet de koers uit door het beleid om te zetten in doelstellingen, plannen en middelen, en houdt toezicht op de naleving ervan. De clustermanagers en teamleiders zijn verantwoordelijk voor de integratie van dit beleid in de dagelijkse processen en zorgen voor de uitvoering en aansturing van medewerkers. Daarnaast is de directie verantwoordelijk voor de evaluatie en bijstelling van de aanpak van privacy en beheersingsmaatregelen. De uitvoering van privacy wordt ondersteund door:

- Alle medewerkers, die verantwoordelijk zijn voor het uitvoeren van het privacybeleid als onderdeel van hun professionele verantwoordelijkheid.
- Leidinggevenden/proceseigenaren van gemeente en DBP, 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) van DBP, die:
  - Het opstellen, de uitvoering, evaluatie en bijstelling van het privacybeleid en de jaarlijkse verbetercycli coördineert;
  - De implementatie, uitvoering en borging van beheersmaatregelen coördineert en hierover rapporteert;
  - Over datalekken rapporteert;
  - De afhandeling en evaluatie van datalekken en verzoeken van betrokkenen coördineert;
  - Privacybewustzijn bevordert in de gehele organisatie;
  - De activiteiten van PO's inhoudelijk coördineert.

- 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:
  - Gemeente Ridderkerk informeert en adviseert over de verplichtingen uit de AVG;
  - Toeziet op de naleving van de AVG binnen de gemeente;
  - Op verzoek advies geeft over risicoanalyses;
  - Samenwerkt met de toezichthouder (Autoriteit Persoonsgegevens);
  - Optreedt als contactpunt voor de Autoriteit Persoonsgegevens;
  - Rechtstreeks verslag uitbrengt aan het college van burgemeester en wethouders (B&W) van Gemeente Ridderkerk;
  - 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 en rechtstreeks verslag kan doen aan de directie van gemeente Ridderkerk;
  - 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.

- Team Control van DBP, die:
  - Interne audits coördineert, zoals de Wpg audits en ENSIA-audits;
  - Externe audits coördineert, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening.

- De concerncontroller van de gemeente die in het kader van de algehele Governance, Risk & Compliance (GRC) voor de gemeente altijd vooraf geïnformeerd over en betrokken bij nieuwe adviezen over IV&P, rapportages en audits.
- Gemeentesecretaris Ridderkerk: heeft de overkoepelende verantwoordelijkheid voor de dagelijkse uitvoering van informatieveiligheids- en privacymaatregelen.

- Clustermanager F&R van DBP: Ambtelijk verantwoordelijk voor de integratie van informatieveiligheid en privacy in de gemeentelijke processen.
- Teamleider Control van DBP: verantwoordelijk voor de naleving en controle van de interne processen, waaronder privacy- en informatieveiligheidsbeleid.

4. DE AANPAK VAN PRIVACY

Jaarcyclus

Om de borging van het privacybeleid en de daarvan afgeleide plannen te realiseren, doorloopt gemeente Ridderkerk de onderstaande Plan, Do, Check, Act (PDCA)-cyclus, zowel organisatiebreed als per beheersmaatregel. Er wordt vanuit het IV&P team binnen DBP samen met de gemeente Ridderkerk een jaarplan opgesteld waarin ook het advies van de Functionaris Gegevensbescherming (FG) uit de jaarrapportage wordt meegenomen. Vervolgens worden het jaarplan en de bijbehorende beheersmaatregelen uitgevoerd en worden borgings-/controleacties uitgevoerd om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd. Zo kijkt gemeente Ridderkerk of deze effectief zijn en waar nodig, moeten worden bijgestuurd. Indien nodig kijkt gemeente Ridderkerk naar herprioritering en/of aanvullende maatregelen waarbij aanbevelingen worden gedaan voor het verbeterplan.

Plan: Team IV&P binnen DBP stelt een jaarplan met verbeterpunten op, rekening houdend met gemeente Ridderkerk haar strategie en -doelstellingen, 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 en publiceren 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 CPO van DBP rapporteert elk kwartaal daarover en over datalekken en andere relevante gebeurtenissen via de (Adjunct) Gemeentesecretaris vergezeld van verbetervoorstellen.

Naast interne controles worden er, waar nodig, ook externe audits uitgevoerd door gerectificeerde, geregistreerde auditoren om de effectiviteit en volledigheid van de beheersmaatregelen te evalueren. Deze audits worden uitgevoerd in overeenstemming met het jaarlijkse auditplan.

De FG geeft onafhankelijk advies over de naleving van de AVG tijdens de evaluaties in de Check-fase en rapporteert hierover aan het College van Burgemeester en Wethouders.

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 Gemeente Ridderkerk voor een continue verbetering van privacy.

6. PRIVACY BEHEERSMAATREGELEN

Bewustwording en training

De CPO van DBP stelt jaarlijks, in samenwerking met de CISO van DBP en in afstemming met de gemeente Ridderkerk, een bewustwordings- en trainingsplan op voor medewerkers 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

De gemeente Ridderkerk draagt de eindverantwoordelijkheid voor het onderhouden van een actueel en volledig register van verwerkingen binnen de interne werkprocessen. De clustermanagers zijn ervoor verantwoordelijk dat de teams tijdig de juiste gegevens aanleveren. Hierbij zal ondersteuning worden geboden door DBP. Het is de taak van de gemeente om een up-to-date overzicht van de verwerkings-

activiteiten te leveren. In het register worden per verwerking de vereiste gegevens opgenomen, conform de AVG en Wpg. De gemeente streeft ernaar het register zo in te richten dat het gemakkelijk kan worden geraadpleegd bij verzoeken, en uiteindelijk zal het register beschikbaar worden gesteld via de website.

Data Protection Impact Assessment
Voor (nieuwe) verwerkingen met een hoog privacyrisico binnen de gemeente Ridderkerk wordt een Data Protection Impact Assessment (DPIA) uitgevoerd. Hierbij wordt een integrale benadering gevolgd, waarbij niet alleen informatiebescherming maar ook informatiebeveiliging en informatiebeheer worden meegenomen. Op deze manier krijgt de gemeente een volledig overzicht van de risico's binnen een werkproces en de maatregelen die nodig zijn om deze te beperken. Dit is in overeenstemming met artikel 35 van de AVG, artikel 4c van de Wpg, en de richtlijnen van de gemeente Ridderkerk en de Autoriteit Persoonsgegevens.

De gemeente kan op advies van DBP in de rol van FG, CPO of CISO, besluiten om een DPIA uit te voeren. De proceseigenaar is eindverantwoordelijk voor de uitvoering van de DPIA en wordt hierbij ondersteund door de relevante stakeholders.

Datalekken
Medewerkers zijn verplicht om datalekken, beveiligingsincidenten en kwetsbaarheden te melden. Datalekken binnen de gemeente Ridderkerk worden centraal geregistreerd via Topdesk en indien nodig tijdig binnen de wettelijke termijn van 72 uur gemeld aan de Autoriteit Persoonsgegevens (AP) en/of betrokkenen.

Alle meldingen worden vastgelegd in een datalekregister, waarin per melding wordt aangegeven of er sprake is van een datalek, of melding aan de AP en/of betrokkenen verplicht is, en een schriftelijke onderbouwing van het incident. Daarnaast wordt de mogelijke acceptatie van risico's door het management gedocumenteerd.

Elk datalek wordt geëvalueerd om passende maatregelen te nemen die herhaling voorkomen. Jaarlijks worden alle datalekken geanalyseerd om trends en patronen te identificeren, zodat verdere preventieve maatregelen getroffen kunnen worden. Dit proces sluit goed aan bij de PDCA-cyclus (Plan-Do-Check-Act).

Transparantie en Rechten van betrokkenen
Gemeente Ridderkerk informeert betrokkenen over de verwerking van hun persoonsgegevens en hun rechten. Het streven is om dit zo efficiënt mogelijk te doen door:
- Betrokkenen te informeren bij het eerste schriftelijke contact binnen een specifieke verwerking;
- Deze informatie duidelijk en uitgebreid op te nemen in de privacyverklaring op de website;
- Verzoeken van betrokkenen om hun rechten uit te oefenen tijdig binnen de wettelijke termijn en volgens de gemaakte afspraken binnen de Gemeente Ridderkerk af te handelen.

Geautomatiseerde besluitvorming, waaronder profilering
De gemeente Ridderkerk heeft als uitgangspunt geen gebruik te maken van geautomatiseerde besluitvorming, waaronder profilering, zoals bedoeld in artikel 22 van de AVG. Om dit te waarborgen, wordt via een Algoritmeregister inzicht gegeven in welke processen mogelijk algoritmes of profilering worden toegepast. Voor deze processen wordt een risicoanalyse uitgevoerd om de potentiële risico's te beoordelen, zoals beschreven in het onderdeel ‘risicomanagement’ hierboven.

VERWERKING VAN POLITIEGEGEVENS
Uitgangspunten en bereik
De gemeente Ridderkerk volgt het model voor beheersmaatregelen dat is opgesteld voor Wpg-audits (Wet politiegegevens), zoals beschreven in bijlage 3 en 4 van de NOREA-handreiking voor privacy audits voor Buitengewoon Opsporingsambtenaren (boa’s). Deze NOREA-handreiking is een richtlijn opgesteld door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en biedt specifieke richtlijnen en standaarden voor privacy-audits binnen het kader van de Wpg. Het document helpt organisaties de beveiliging van politiegegevens te waarborgen en ondersteunt bij het aantoonbaar naleven van de wettelijke privacy-eisen.

Indien een informatiesysteem wordt beheerd door een externe leverancier, zoals bij SaaS-oplossingen (Software as a Service), sluit de gemeente een verwerkersovereenkomst met de betreffende leverancier af. Deze overeenkomst waarborgt de bescherming van persoonsgegevens en bepaalt onder meer de verantwoordelijkheden van de leverancier ten aanzien van databeveiliging. Daarnaast is de leverancier verplicht een Third Party Memorandum (TPM) aan te leveren. Dit TPM-document, opgesteld volgens de NOREA-handreiking, biedt inzicht in de beveiligingsmaatregelen en de naleving van privacyrichtlijnen bij de leverancier.

Door gebruik te maken van deze NOREA-richtlijnen verzekert de gemeente Ridderkerk dat alle betrokken partijen voldoen aan de gestelde normen en richtlijnen voor de bescherming van politiegegevens en andere persoonsgegevens, conform de Wpg.

Voor elke verwerking van politiegegevens voert de gemeente Ridderkerk een verplichte Data Protection Impact Assessment (DPIA) uit, vanwege de gevoeligheid van deze gegevens en de ongelijkheidsrelatie tussen de boa en de verdachte.

De verwerking van politiegegevens door de gemeente Ridderkerk is gebaseerd op artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en de artikelen met betrekking tot het ter beschikking stellen en verstrekken van politiegegevens (artikelen 15-21 en 23-24). Daarnaast verwerkt de gemeente politiegegevens op basis van artikel 13 Wpg (ondersteunende taken), voor zover deze gegevens onder de verantwoordelijkheid van andere instanties vallen.

Gemeente Ridderkerk verwerkt geen gegevens op basis van de volgende artikelen van de Wpg:
- Artikel 9 Wpg (onderzoek in een specifiek geval), hoewel boa's wel medewerking verlenen aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten.
- Artikel 11 Wpg (geautomatiseerd vergelijken en zoeken in combinatie voor een onderzoek op basis van Artikel 9).
- Artikel 17a Wpg (doorgifte aan derde landen buiten de Europese Economische Ruimte). De gemeente maakt ook geen gebruik van geautomatiseerde besluitvorming, waaronder profilering zoals bedoeld in Artikel 7a Wpg.

De toegangsbeveiliging is zodanig ingericht dat alleen boa's en andere geautoriseerde personen toegang hebben tot de politiegegevens. Bij verzending worden de politiegegevens altijd versleuteld verstuurd.

Rollen, taken en bevoegdheden
De Privacy Officer van DBP beoordeelt jaarlijks of het bereik van de verwerking van politiegegevens is gewijzigd. Op basis hiervan worden dit beleid en het verwerkingenregister indien nodig aangepast.

De Teamleider van het team openbare orde en veiligheid (OOV) en Wijkteam 1 (leerplicht) is verantwoordelijk voor de implementatie en uitvoering van de Wpg. De taken omvatten onder andere:
- Medewerkers informeren over de handreiking en gedragsregels voor boa's en toezicht hierop houden.
- Een overzicht bijhouden van geautoriseerden.
- Het actueel houden van het verwerkingenregister met betrekking tot het team.
- Bijhouden van een lijst met veel voorkomende verstrekkingen en de onderbouwing van de grondslagen hiervoor.
- Zorgdragen voor de bewaartermijnen van Art. 8 gegevens:
  - Na 1 jaar alleen beschikbaar voor gericht zoeken.
  - Na 5 jaar beschikbaar voor audits en klachtenprocedures.
  - Na 10 jaar vernietigd.

- Boa's en leerplichtambtenaren autoriseren voor verwerking politiegegevens volgens Wpg Art. 6, lid 3, 4, 5 via het "Autorisatie verwerking politiegegevens"-formulier en de autorisatiematrix vast te stellen.

De Teamleider Informatiebeheer van DBP heeft de bevoegdheid om medewerkers te autoriseren voor digitale verwerking justitiële gegevens op grond van artikel artikelen 9 tot en met 13 van de Wet justitiële en strafvorderlijke gegevens en het Besluit justitiële en strafvorderlijke gegevens:

Het college en de burgemeester nemen aanwijzings- en autorisatiebesluiten voor verwerken politiegegevens en justitiële informatie ten behoeve van: openbare orde en veiligheid, APV en bijzondere wetten en sociaal domein.

De Teamleider heeft de bevoegdheid om:
- Autorisatiebesluiten te nemen volgens Wpg Art. 6, lid 3, 4, 5 via het "Autorisatie verwerking politiegegevens"-formulier.
- Toegang tot informatiesystemen met politiegegevens te regelen en de autorisatiematrix vast te stellen.

De Functionaris Gegevensbescherming (FG):
- Adviseert en informeert over de Wpg, waaronder DPIA's.
- Houdt toezicht op de uitvoering van de Wpg.

- Werkt samen met de AP en is het aanspreekpunt voor de AP.
- Stelt jaarlijks een verslag op met bevindingen.
- Voert controles uit.

Team Control van DBP coördineert interne en externe Wpg-audits.

Specifiek beleid cluster Veiligheid.
De gemeente Ridderkerk maakt gebruik van zowel bestursrechtelijke als strafrechtelijke middelen voor toezicht en handhaving in de openbare ruimte. Boa's zijn hiervoor aangesteld en de Wpg is van toepassing.

Specifiek beleid leerplichtwet.
Naast bestuursrechtelijke middelen gebruikt de gemeente Ridderkerk strafrechtelijke instrumenten voor handhaving van de leerplichtwet, specifiek Art. 16 lid 5 en Art. 26. Boa's zijn aangesteld en de Wpg is van toepassing.

Specifiek beleid participatiewet (Handhaving en toezicht)).
Voor toezicht en handhaving binnen de Participatiewet worden alleen bestuursrechtelijke middelen ingezet door het Team Handhaving en toezicht. Boa's zijn hier niet aangesteld en de Wpg is niet van toepassing.

Inwerkingtreding en intrekking
"Privacybeleid gemeente Ridderkerk 2025 – 2027" treedt in werking de dag na publicatie

Tegelijkertijd wordt ingetrokken "privacybeleid van de gemeente Ridderkerk 2019/2020".

Aldus besloten op 13 mei 2025,

Burgemeester en wethouders van Ridderkerk,

de secretaris,
mw. M. Kitselar

de burgemeester,
dhr. C.A. Oosterwijk