Gemeente Borne

GEMEENTEBLAD

Officiële uitgave van de gemeente Borne

Nr. 454410

26 oktober

2023

Privacybeleid gemeente Borne 2023

1. Aanleiding

Na de komst van de Algemene Verordening Gegevensbescherming (AVG) in 2018 is in 2020 het privacybeleid gemeente Borne 2019 vastgesteld. Inmiddels is er aanleiding om het privacybeleid te wijzigen. De afgelopen jaren zijn er zowel landelijk als lokaal veel ontwikkelingen geweest op het gebied van privacy. Er ontstonden diverse richtlijnen en handreikingen, waardoor steeds beter invulling kan worden gegeven aan de uitvoering van de AVG. Gemeente Borne heeft een aantal belangrijke stappen gezet om te voldoen aan privacy wet- en regelgeving. Borne heeft ook een ambitie uitgesproken in wat zij op welke termijn wil bereiken op het gebied van privacy. Het privacybeleid sluit momenteel niet aan bij die ambitie en kan daarom niet gebruikt worden als 'kapstok'. Dit heeft geleid tot het privacybeleid gemeente Borne 2023.

2. Inleiding privacy

Gemeente Borne beschikt over veel persoonsgegevens van haar inwoners, medewerkers en derden (waaronder ondernemers, bezoekers en contactpersonen). Deze persoonsgegevens worden onder meer gebruikt indien dit noodzakelijk is voor het uitvoeren van publieke taken van de gemeente, om te voldoen aan wettelijke verplichtingen, om uitvoering te geven aan (arbeids)overeenkomsten en voor de bedrijfsvoering van de gemeentelijke organisatie.

Inwoners, medewerkers en derden moeten erop kunnen vertrouwen dat de gemeente zorgvuldig, veilig, proportioneel en vertrouwelijk met hun persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Gemeente Borne acht het van groot belang om haar verantwoordelijkheid hierin te nemen en neemt maatregelen om de bescherming van persoonsgegevens te waarborgen.

Bij de verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Naast het belang van de individuele burger, is er het publieke (algemeen) belang en zijn er belangen van inwoners ten opzichte van elkaar. Dat vraagt om een zorgvuldige afweging. Deze afweging dient gemeente Borne te maken binnen de kaders van de privacywetgeving.

Er zijn een aantal wetten die bepalen hoe gemeenten persoonsgegevens mogen gebruiken. Dit zijn de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), de Wet basisregistratie personen (Wet BRP) en de Wet Politiegegevens (Wpg). De Autoriteit Persoonsgegevens (AP) houdt toezicht op of gemeenten zich aan deze wetten houden.

In dit privacybeleid wordt beschreven hoe gemeente Borne invulling geeft aan wet- en regelgeving op het gebied van privacy, met name de AVG.

2.1 Begrippen

Een aantal begrippen die voorkomen in de AVG en/of in dit beleid zullen nader worden toegelicht:

- **Persoonsgegevens**: alle gegevens die direct of indirect herleidbaar zijn tot een natuurlijke persoon. Gegevens zoals naam, contactgegevens, inloggegevens en locatiegegevens betreffen reguliere persoonsgegevens. Gevoelige persoonsgegevens, zoals financiële gegevens, dienen met extra zorgvuldigheid te worden verwerkt. Aan de verwerking van strafrechtelijke gegevens en het BSN heeft de AVG extra voorwaarden verbonden. Gegevens van rechtspersonen of van overleden personen zijn geen persoonsgegevens in de zin van de AVG.
- **Bijzondere persoonsgegevens**: gegevens die door hun aard bijzonder gevoelig zijn en extra beschermd dienen te worden:
  - ras of etnische afkomst
  - politieke opvattingen
  - religieuze of levensbeschouwelijke overtuigingen
  - lidmaatschap van een vakvereniging
  - gezondheidsgegevens
  - seksueel gedrag of seksuele gerichtheid
  - genetische gegevens;

- biometrische gegevens
  Bijzondere persoonsgegevens mogen door de gemeente verwerkt worden als de verwerking valt onder de wettelijk genoemde uitzonderingen.

- **Betrokkene**: de persoon op wie de persoonsgegevens betrekking hebben en van wie de gegevens worden verwerkt. Dit kunnen inwoners, medewerkers of derden (zoals ondernemers, bezoekers en contactpersonen) zijn.
- **Verwerken**: alles wat je met persoonsgegevens kan doen, zoals vastleggen, raadplegen, wijzigen, opslaan, verstrekken en verwijderen.
- **Verwerkingenregister**: de gemeente is verplicht tot het bijhouden van een verwerkingenregister, waarin informatie staat over de verwerkingen van persoonsgegevens van de gemeente.
- **Verwerkingsverantwoordelijke**: de persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Binnen de gemeente is dit meestal het college van burgemeester en wethouders of de burgemeester.
- **Verwerker**: de persoon of organisatie die de persoonsgegevens verwerkt voor de verwerkingsverantwoordelijke, waarbij de verwerkingsverantwoordelijke het doel en de middelen bepaalt. Vaak betreft dit een applicatie die gebruikt wordt om gegevens te verwerken.
- **Verwerkersovereenkomst**: in een verwerkersovereenkomst leggen de verwerkingsverantwoordelijke en de verwerker afspraken vast over de verwerking van persoonsgegevens door de verwerker. In beginsel gebruiken we als gemeente de standaard verwerkersovereenkomst van de VNG.
- **DPIA (Data protection impact assessment)/Gegevensbeschermingseffectbeoordeling)**: Een DPIA is een instrument om vooraf bij nieuwe of bestaande verwerkingen risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De AVG verplicht de uitvoering van een DPIA voor verwerkingen met een hoog privacyrisico.
- **Datalek**: Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
- **PDCA-cyclus (plan-do-check-act-cyclus)**: een zich steeds herhalende cyclus van een plan opstellen, uitvoeren, evalueren en verbeteren.

3. Ambitie en doel

De komende jaren wil gemeente Borne groeien richting een organisatie die zich privacyvolwassen kan noemen. Sinds 2021 brengen we jaarlijks in kaart hoe de gemeente er voor staat voor wat betreft het beschermen van persoonsgegevens en voldoen aan de AVG, met behulp van de AVG compliance meting van de Vereniging Nederlandse Gemeenten (VNG). Deze mate van compliance kan gekoppeld worden aan het volwassenheidsmodel, opgesteld door het Centrum Informatiebeveiliging en Privacybescherming (CIP)[1]. Dit model onderscheid vijf volwassenheidsniveaus, waarbij 5 staat voor een geoptimaliseerd proces. In de praktijk wordt niveau 3 als basisniveau aangeduid, waarbij aan de wettelijke verplichtingen wordt voldaan. Bij niveau 4 kan gesteld worden dat volledig aan de AVG wordt voldaan, omdat op dit niveau maatregelen en processen ook geëvalueerd worden.

Gemeente Borne heeft zich als doel gesteld om te groeien naar volwassenheidsniveau 3 in 2024. Dat wil onder meer zeggen dat er sprake is van vastgestelde processen rondom privacy, dat aantoonbaar aan verplichtingen wordt voldaan, dat rollen en verantwoordelijkheden actief worden opgepakt en dat beheersmaatregelen gedocumenteerd zijn en consistent en gestructureerd worden uitgevoerd. De gemeente wil doorgroeien naar volwassenheidsniveau 4 in 2026. Dat wil onder meer zeggen dat er sprake is van een voorspelbaar proces, dat de effectiviteit van beheersmaatregelen periodiek wordt geëvalueerd in een Plan-Do-Check-Act-cyclus (PDCA-cyclus), dat de kwaliteit van het beleid en processen meetbaar en inzichtelijk is op ieder niveau en er sprake is van optimaal lerend vermogen. Wanneer dit niveau wordt bereikt, kan gesteld worden dat gemeente Borne AVG compliant en privacyvolwassen is. Dit privacybeleid vormt de basis om deze ambitie waar te maken.

Het doel van dit privacybeleid is het bieden van een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Met dit kader kan gemeente Borne groeien naar een privacyvolwassen organisatie.

1) Centrum Informatiebeveiliging en Privacybescherming (2017). *Privacy volwassenheidsmodel. https://www.cip-overheid.nl/product-categorieen-en-workshops/producten?product=handreiking-borging-van-privacy-en-volwassenheidsmodel.nl*

4. Reikwijdte

Dit privacybeleid is van toepassing op de gehele organisatie; op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het beleid is nader uitgewerkt in processen en werkinstructies voor een juiste implementatie. In dit stuk wordt geschreven over 'de gemeente', 'ons' of 'wij'. Dit refereert altijd aan gemeente Borne.

De gemeenteraad is verwerkingsverantwoordelijke voor een aantal eigen verwerkingen, bijvoorbeeld die van de griffie. Dit privacybeleid is hierop niet rechtstreeks van toepassing.

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente. Bij de inzet van verwerkers of in geval van samenwerkingsverbanden vormt dit privacybeleid het uitgangspunt bij het maken van afspraken met betrekking tot de omgang met persoonsgegevens.

5. Samenhang andere wetten en beleidsterreinen

De AVG is een Europese verordening welke rechtstreeks van toepassing in is Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG). Hierin is bijvoorbeeld de Autoriteit Persoonsgegevens benoemd als toezichthouder.

In beginsel is in sectorspecifieke wetgeving al vastgelegd hoe moet worden omgegaan met persoonsgegevens. Er kan bijvoorbeeld sprake zijn van een beroepscode of geheimhoudingsplicht. Ook is soms specifiek vastgelegd welke gegevens nodig zijn voor het uitoefenen van de taak. Deze wetgeving moet voldoen aan de kaders van de privacywetgeving. Wanneer in deze sectorspecifieke wetgeving iets niet is geregeld, dienen de AVG-kaders te worden toegepast.

De Wet basisregistratie personen (Wet BRP) regelt het juiste gebruik van de gegevens die zijn opgenomen in de basisregistratie personen. Daarbij gaat het onder meer om de handelswijze van gemeenten bij het opnemen, wijzigen en verstrekken van persoonsgegevens in de BRP. Dit betekent niet dat de AVG niet van toepassing is, maar dat de AVG al is uitgewerkt in deze wet. Daar waar de BRP zelf niets heeft geregeld, wordt de AVG op zichzelf toegepast.

De Wet politiegegevens (Wpg) zie toe op de verwerking van politiegegevens. Binnen gemeente Borne kunnen buitengewoon opsporingsambtenaren politiegegevens verwerken in het kader van hun opsporingstaak. De verwerking van politiegegevens is uitgewerkt in het beleid Wet politiegegevens gemeente Borne.

De Wet justitiële en strafvorderlijke gegevens (Wjsg) regelt het verwerken van justitiële gegevens in persoonsdossiers en voor de verklaring omtrent gedrag (VOG). De wet regelt ook de verwerking van strafvorderlijke gegevens.

De bescherming van persoonsgegevens en informatiebeveiliging zijn onlosmakelijk met elkaar verbonden. De nadere invulling van informatieveiligheid is opgenomen in het informatiebeveiligingsbeleid. Het privacybeleid en het informatiebeveiligingsbeleid sluiten op elkaar aan.

6. Privacy governance

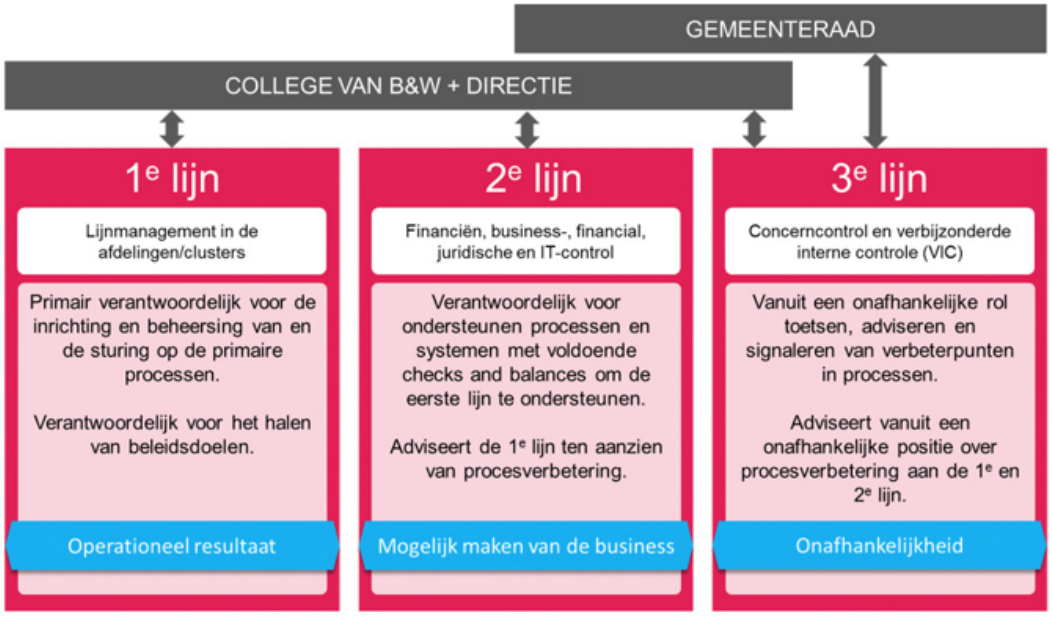
Het beschermen van persoonsgegevens betreft een gezamenlijke verplichting van iedereen die voor gemeente Borne werkt en vergt inspanningen van het bestuur, management en medewerkers. Hierbij kennen we verschillende rollen en verantwoordelijkheden.

6.1 Three Lines Model

Om op het juiste niveau inzicht te krijgen in privacyrisico's is het nodig dat verantwoordelijkheden op ieder niveau duidelijk zijn. Net als veel andere gemeenten gebruikt gemeente Borne het 'Three Lines Model'[2] voor de inrichting van risicobeheersing. We hanteren hiervoor het volgende schema[3]:

2) The Institute of Internal Auditors (2020). *Het three lines model van het IIA.* https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-dutch.pdf

3) https://www.consultancy.nl/nieuws/43453/verbeter-het-first-time-right-percentage-van-gemeenteprocessen



Dit model kan ook worden toegepast bij de beheersing van privacyrisico's:

- De eerste lijn is de uitvoerende, operationele laag. Dit betreffen de vakafdelingen, met teamleiders als verantwoordelijke. Deze laag is ook eigenaar van de risico's die samengaan met het bereiken van de eigen doelstellingen.
- De tweede lijn adviseert over de risico's aan de eerste lijn en ondersteunt de eerste lijn bij het treffen van de juiste maatregelen voor die risico's. De werkzaamheden van onder andere de PO en de CISO passen in deze lijn.
- De derde lijn is de controlerende functie, zoals de FG en subteam kwaliteit & control. Deze lijn beoordeelt of de risico's en bijhorende maatregelen op een effectieve manier zijn ingericht.

Dit model zorgt ervoor dat risico's op het juiste niveau worden belegd en er op een adequate manier controle over wordt gevoerd. Dit is dan ook de basis om op een juiste (en integrale) manier te kunnen rapporteren.

6.2 Rollen en verantwoordelijkheden

Het college van burgemeester en wethouders is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het naleven van deze verplichtingen is gedeeltelijk gemandateerd aan de ambtelijke organisatie van de gemeente. Dit is geregeld in het mandaatbesluit. In het kader van gegevensbescherming lichten we de volgende functies dan wel rollen toe:

- **College van Burgemeester en Wethouders (het college)**: het college is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente en stelt het privacybeleid vast.
- **Directie**: gemeente Borne is ingericht middels een directiemodel. De directie is eindverantwoordelijk voor het functioneren van de ambtelijke organisatie.
- **Teamleiders**: de teamleiders zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid. Zij zijn ook verantwoordelijk voor het afwegen van risico's en accepteren van restrisico's bij in te zetten maatregelen.
- **Medewerkers**: iedere medewerker is in de uitvoering van zijn dagelijkse werkzaamheden verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens en het naleven van het privacybeleid.
- **Functionaris gegevensbescherming (FG)**: De AVG verplicht het benoemen van een functionaris gegevensbescherming, die vanuit een onafhankelijke positie een toezichthoudende en adviserende rol heeft.
- **Privacy officer (PO)**: Bij de privacy officer zijn diverse ondersteunende, coördinerende en uitvoerende taken neergelegd. De privacy officer is binnen de gemeente het eerste aanspreekpunt als het gaat om gegevensbescherming. Vragen kunnen worden gesteld via privacy@borne.nl.
- **Chief information security officer (CISO)**: de chief information security officer is het aanspreekpunt met betrekking tot informatieveiligheid en adviseert en ondersteunt vanuit zijn eigen rol bij de uitvoering van de taken op het gebied van gegevensbescherming.
- **Privacy ambassadeurs**: privacy ambassadeurs zijn aanspreekpunten binnen de teams, als het gaat om gegevensbescherming. Zij hebben korte lijntjes met de PO, ondersteunen de PO en dragen bij aan bewustwording en kennisoverdracht binnen het team.

- **Juridisch adviseurs**: ondersteunen de privacy officer en medewerkers bij privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
- **Communicatie**: de communicatieconsulent wordt betrokken in de gevallen waarbij (interne of externe) communicatie een rol speelt en ondersteunt en adviseert de privacy officer bij acties voor bewustwording en kennisoverdracht.

De rollen en verantwoordelijkheden op het gebied van gegevensbescherming zijn verder uitgewerkt en vastgelegd in 'Organisatie privacy: rollen en verantwoordelijkheden'. Deze structuur maakt onderdeel uit van dit privacybeleid en kan, indien gewijzigde rollen of taken hierom vragen, tussentijds gewijzigd worden.

7. Uitgangspunten bij de verwerking van persoonsgegevens

Op basis van de AVG gelden de volgende beginselen ten aanzien van de verwerking van persoonsgegevens:

- De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.
- De verwerking van persoonsgegevens moet een helder doel hebben dat is terug te leiden naar taken, verplichtingen, overeenkomsten of belangen.
- Het verwerken van persoonsgegevens moet noodzakelijk zijn ten opzichte van de beoogde doelen (proportionaliteit en subsidiariteit). Wanneer met geen, of minder (belastende) persoonsgegevens hetzelfde doel bereikt kan worden, moet daarvoor gekozen worden.
- De (verwerking van) persoonsgegevens moet(en) juist en van voldoende kwaliteit zijn.
- De (verwerking van) persoonsgegevens moet(en) goed zijn beveiligd en beschermd.
- Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk of verplicht is.

Gemeente Borne onderschrijft deze beginselen en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze beginselen. De beginselen zullen nader worden toegelicht.

7.1 Rechtmatige grondslag

Gemeente Borne verwerkt slechts persoonsgegevens indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. De AVG benoemt in artikel 6 AVG zes rechtsgronden op basis waarvan persoonsgegevens kunnen worden verwerkt:

1. Toestemming: deze grond doet zich in de praktijk nauwelijks voor bij de gemeente. Toestemming moet vrij kunnen worden gegeven en weer worden ingetrokken. Voorbeeld: als medewerker toestemming geven aan HR voor het delen van adresgegevens met collega's voor kaartjes e.d.
2. Overeenkomst: de gemeente gaat overeenkomsten aan waarvoor het noodzakelijk is persoonsgegevens te verwerken. Voorbeeld: arbeidsovereenkomsten met medewerkers.
3. Wettelijke verplichting: voor verschillende verwerkingen geldt dat de gemeente hiertoe wettelijk verplicht is. Voorbeeld: het beheren van de gemeentelijke basisregistratie, de BRP.
4. Vitaal belang: deze grond doet zich in de praktijk niet of nauwelijks voor bij de gemeente. Er moet sprake zijn van direct en onmiddellijk levensgevaar: Voorbeeld: hulpverlening bij een grootschalige ramp.
5. Taak van algemeen belang of openbaar gezag (publiekrechtelijke taak): voor de meeste verwerkingen van de gemeente geldt dat de gegevensverwerking noodzakelijk is voor het uitvoeren van een taak die bij de gemeente belegd is. Voorbeeld: uitvoeren van de Wet maatschappelijke ondersteuning (Wmo).
6. Gerechtvaardigd belang: bij sommige processen is het gerechtvaardigd om als gemeente bepaalde gegevens te verwerken om die taak uit te kunnen voeren. Voorbeeld: registreren van contactgegevens voor een terugbelverzoek. De gemeente kan echter de grondslag gerechtvaardigd belang niet gebruiken in het kader van de uitvoering van haar publieke taken.

De grondslag voor de verwerking van persoonsgegevens vloeit bij een gemeente meestal voort uit een wettelijke verplichting of een publiekrechtelijke taak.

Voor het BSN, voor strafrechtelijke gegevens en voor bijzondere persoonsgegevens is (alleen) bovenstaande grondslag onvoldoende. Hiervoor gelden aanvullende voorwaarden. Voor het BSN geldt dat we dit nummer als gemeente alleen mogen verwerken wanneer dit wettelijk verplicht is of wanneer dit nodig is voor de uitoefening van onze taken, bijvoorbeeld bij het doen van een aanvraag zodat kan worden vastgesteld om wie het gaat. Strafrechtelijke gegevens mogen alleen worden verwerkt als de verwerker zich naast een reguliere grondslag kan beroepen op een wettelijke uitzondering. De gemeente kan in bepaalde gevallen strafrechtelijke persoonsgegevens verwerken indien dit nodig is voor de uitoefening van onze taken, bijvoorbeeld onze taken met betrekking tot zorg- en veiligheid of bij de uitvoering van een toets op grond van de Wet Bibob. Voor het verwerken van bijzondere persoonsgegevens heeft een verwerker naast een reguliere grondslag uit artikel 6 AVG en extra grondslag uit artikel 9 AVG nodig. De gemeente kan bijzondere persoonsgegevens verwerken, bijvoorbeeld politieke opvattingen

die door raads- en collegeleden zelf openbaar worden gemaakt en medische gegevens indien dit noodzakelijk is voor de uitvoering van de sociale wetgeving.

7.2 Doelbinding

Persoonsgegevens mogen alleen worden verwerkt ten behoeve van een vooraf duidelijk en beschreven doel. Het doel waarvoor de gemeente persoonsgegevens verwerkt hangt samen met de grondslag. De gemeente verwerkt de meeste persoonsgegevens voor het uitvoeren van de primaire gemeentelijke overheidstaken. Deze taken staan in wetgeving, daarop gebaseerde regelgeving en beleid. Daarnaast voert de gemeente taken uit met als doel de bedrijfsvoering, het personeelsbeleid en de organisatie en het beheer van de gemeente. Wanneer het doel niet helder is zal dit eerst moeten worden bepaald voordat gestart kan worden met de verwerking van persoonsgegevens.

In beginsel mogen persoonsgegevens alleen worden gebruikt voor dat doel waarvoor ze verzameld zijn. Soms mogen gegevens voor een verenigbaar doel worden gebruikt. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

7.3 Minimale gegevensverwerking

Als er sprake is van een rechtmatige grondslag en doelbinding, wil dat nog niet zeggen dat alle persoonsgegevens hiervoor verwerkt mogen worden. Persoonsgegevens mogen alleen worden verwerkt voor zover deze verwerking noodzakelijk is om het vastgestelde doel te bereiken (noodzakelijke gegevensverwerking), als het doel niet op een andere en minder ingrijpende manier kan worden bereikt (subsidiariteit) en als de inbreuk op de privacy in verhouding staat tot het te bereiken doel (proportionaliteit). Als het doel ook zonder of met minder persoonsgegevens kan worden bereikt of op een manier die minder inbreuk maakt op de privacy van de betrokkene, dan kiest gemeente Borne bij voorkeur voor die mogelijkheid. Bij bijvoorbeeld het openbaar maken van besluiten en onderliggende stukken zijn persoonsgegevens veelal niet noodzakelijk voor het bereiken van het doel (openbaarheid van bestuur) en worden deze geanonimiseerd. Hierbij vindt altijd een zorgvuldige afweging plaats.

7.4 Juistheid gegevens

Wanneer de gemeente persoonsgegevens verwerkt, is het van belang dat deze gegevens juist en actueel zijn. Gemeente Borne neemt maatregelen om te zorgen dat de juiste persoonsgegevens worden ontvangen, bijvoorbeeld door betrokkene een gespreksverslag te laten controleren of door bij een aanvraag te checken of de gegevens overeenkomen met de basisregistratie personen, en om te zorgen dat gegevens indien nodig geactualiseerd, gewijzigd of verwijderd worden. Wij maken in veel processen gebruik van het BSN om de aanvraag, het verzoek of de melding aan de juiste persoon te koppelen. Soms stellen we de identiteit van betrokkene vast met behulp van een legitimatiebewijs. Betrokkene heeft invloed op de juistheid van gegevens door gebruik te maken van zijn rechten met betrekking tot zijn persoonsgegevens.

7.5 Beveiligen

Persoonsgegevens dienen goed te worden beveiligd en beschermd tegen misbruik, onrechtmatig of ongeautoriseerd gebruik, onrechtmatige vernietiging of wijziging, verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking. Gevoelige en bijzondere persoonsgegevens behoeven extra bescherming. Gemeente Borne neemt hiervoor passende technische en organisatorische maatregelen. We handelen hierbij in overeenstemming met het informatiebeveiligingsbeleid en volgen hierbij de Baseline informatiebeveiliging overheid (BIO). Zo richten we zo goed mogelijk autorisaties in, zodat medewerkers, externen, leveranciers en partners alleen toegang hebben tot die gegevens die zij nodig hebben voor de uitoefening van hun taak. Daarnaast ondertekenen medewerkers een integriteitsverklaring en werken we indien nodig met geheimhoudingsverklaringen wanneer andere partijen betrokken zijn. We slaan gegevens goed beveiligd op in de hiervoor bedoelde systemen en als we gegevens delen, doen we dit op een veilige manier. We voeren audits en controles uit om te controleren of de informatieveiligheid op orde is.

7.6 Bewaren

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen en selectielijsten uit hoofde van de Archiefwet. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Wanneer de wet of selectielijst niet voorziet in de bewaartermijn, wordt deze vastgesteld op basis van noodzakelijkheid. De bewaartermijn wordt vastgelegd in het verwerkingenregister. Wanneer de bewaartermijn verloopt, worden de gegevens vernietigd. Soms is het wenselijk dat gegevens langer bewaard worden,

bijvoorbeeld voor onderzoek. Dan worden de persoonsgegevens geanonimiseerd, zodat identificatie van een persoon niet meer mogelijk is.

7.7 Transparant

Een belangrijk uitgangspunt van de AVG is dat degene die gegevens verwerkt, hierover transparant moet zijn naar de betrokkene. Gemeente Borne informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Dit doen wij via onze privacyverklaring op onze website, in onze communicatie met betrokkenen en waar nodig en mogelijk informeren we betrokkenen met betrekking tot een specifieke verwerking. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af. Dit kan bijvoorbeeld gedurende een lopend onderzoek of in het kader van veiligheid.

8. Uitvoeren en verantwoorden

Gemeente Borne geeft op verschillende manieren uitvoering aan de beginselen van de AVG en aan de verplichting om aan te tonen dat aan deze beginselen voldaan wordt.

8.1 Privacyverklaring

Op de website van gemeente Borne staat onze privacyverklaring. Hiermee informeren wij betrokkenen onder andere over de gegevens die de gemeente in de uitoefening van haar diverse taken kan verwerken en voor welke doeleinden, hoe betrokkenen gebruik kunnen maken van hun rechten met betrekking tot hun persoonsgegevens en waar ze terecht kunnen met vragen of klachten. Waar nodig en mogelijk actualiseren we onze privacyverklaring.

8.2 Rechten van betrokkenen

Betrokkenen van wie persoonsgegevens verwerkt worden, hebben diverse rechten om invloed uit te kunnen oefenen op de verwerking van hun gegevens. Deze betreffen het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Deze rechten kunnen beperkt worden door wettelijke verplichtingen (een gemeente heeft bijvoorbeeld een archiveringsplicht en kan daarom niet zomaar allerlei gegevens vernietigen) of belangen van derden (kan een ander geschaad worden door bijvoorbeeld het geven van inzage). In de privacyverklaring op de gemeentelijke website staat hoe de verzoeken kunnen worden ingediend. Een digitaal verzoek kan rechtstreeks via de website worden gedaan. Aan de afhandeling van de verzoeken zijn wettelijke termijnen en voorschriften verbonden. De afhandeling van de verzoeken hebben we vastgelegd in de procedures voor rechten van betrokkenen. De PO coördineert de verzoeken.

Indien betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de reguliere klachtenprocedure. Betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

8.3 Verwerkers en samenwerkingen

Gemeente Borne schakelt soms derden in om persoonsgegevens te verwerken, waarbij de gemeente bepaalt wat er met deze gegevens moet gebeuren. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers in zogenaamde verwerkersovereenkomsten. De gemeente Borne gebruikt hiervoor in beginsel de standaardverwerkersovereenkomst van de VNG.

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

Met betrekking tot doorgifte hanteert de gemeente het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is en voldoet aan de eisen die de AVG daaraan stelt.

8.4 Privacy by Design en Privacy by Default

De gemeente dient bij de ontwikkeling van nieuwe diensten, systemen of processen al rekening te houden met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd.

Hieronder valt het minimaliseren, scheiden, abstraheren en verbergen van persoonsgegevens, het informeren van en controle geven aan betrokkenen, het afdwingen van een privacy-vriendelijke verwerking van persoonsgegevens en het kunnen aantonen van bovenstaande. De gemeente draagt er zorg voor dat concrete maatregelen (zoals anonimiseren of pseudonimiseren) zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk. Waar mogelijk nemen we Privacy by Design en Privacy by Default op in onze standaardprocessen.

8.5 Datalekken

Wanneer een onbevoegde toegang krijgt tot persoonsgegevens, of persoonsgegevens worden vernietigd, gewijzigd of verloren zonder dat dit de bedoeling is, is er sprake van een datalek. Een mogelijk datalek dient te worden gemeld bij de privacy officer via datalek@borne.nl. Bij een datalek zetten wij direct in op het beëindigen van het datalek en het beperken van de gevolgen. Een datalek moet, afhankelijk van het risico, worden gemeld bij de Autoriteit Persoonsgegevens en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Dit kunnen zowel technische als organisatorische maatregelen inhouden en we zetten ook in op bewustwording rondom datalekken. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure voor datalekken.

8.6 Verwerkingenregister

Gemeenten zijn op grond van de AVG verplicht tot het bijhouden van een verwerkingenregister. Het verwerkingenregister bevat informatie over de verwerkingen van persoonsgegevens die binnen gemeente Borne plaatsvinden. Het verwerkingenregister bevat onder meer informatie over het bestuursorgaan dat verantwoordelijk is voor de verwerking, de doelen en grondslagen van de verwerkingen, de categorieën persoonsgegevens die verwerkt worden, de herkomst van gegevens, de categorieën betrokkenen van wie persoonsgegevens verwerkt worden, de categorieën ontvangers aan wie de gegevens verstrekt kunnen worden en of gegevens buiten de EU gedeeld kunnen worden, de bewaartermijnen van de gegevens en een beschrijving van de beveiliging van de gegevens. Gemeente Borne legt in haar verwerkingenregister ook een link met de DPIA's die al uitgevoerd zijn of nog uitgevoerd moeten worden.

Het verwerkingenregister vormt het overzicht van verwerkingen van persoonsgegevens binnen de gemeente Borne en een belangrijke basis voor het onderzoek naar privacyrisico's, het verbeteren van de bescherming van persoonsgegevens en het uitvoeren van de verzoeken tot het uitoefenen van rechten van betrokkenen.

Het verwerkingenregister behoeft actualisatie bij wijzigingen. De vakafdelingen zijn verantwoordelijk voor het doorgeven van wijzigingen. De privacy officer heeft hierover periodiek contact met de privacy ambassadeurs.

8.7 DPIA

Als een verwerking mogelijk een hoog risico inhoudt voor de privacy van betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevensbeschermingseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd) uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Het management is verantwoordelijk voor het maken van keuzes op het gebied van privacyrisico's, zoals het treffen van mitigerende maatregelen en het accepteren van restrisico's. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De FG geeft een advies op de uitgevoerde DPIA en kan in het kader van toezicht controleren in hoeverre de voorgestelde maatregelen zijn opgevolgd.

Gemeente Borne heeft een werkproces ingericht voor het uitvoeren van een DPIA. Of een DPIA moet worden uitgevoerd, wordt bepaald met behulp van de checklist DPIA. Hierbij worden de richtlijnen van de Autoriteit Persoonsgegevens gevolgd. De Autoriteit Persoonsgegevens heeft een lijst opgesteld met verwerkingen waarvoor een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een lijst van negen criteria opgesteld om te bepalen of er sprake kan zijn van een hoog privacyrisico. Hierbij is de vuistregel dat een DPIA uitgevoerd dient te worden als de verwerking aan twee of meer van de criteria voldoet, maar ook in andere gevallen kan een (vorm van een) DPIA wenselijk zijn. De FG adviseert hierbij. DPIA's kunnen worden uitgevoerd voor bestaande en nieuwe verwerkingen. Voor bestaande verwerkingen voert de gemeente Borne DPIA's uit volgens een vastgestelde planning. Hierdoor ontstaat een cyclus van drie jaar, waarbij de DPIA's iedere drie jaar herhaald worden. Dit is tevens de termijn die de Autoriteit Persoonsgegevens aanraadt voor herhaling van de DPIA. Voor nieuwe of gewijzigde verwerkingen geldt dat voorafgaande aan de verwerking of wijziging een DPIA moet worden uitgevoerd.

8.8 Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Dit wordt uitgewerkt in een plan van aanpak voor bewustwording en kennisoverdracht. We voeren regelmatig bewustwordingsacties uit en voorzien de medewerkers via intranet van werkinstructies en procedures, uitleg en handige tips en actualiteiten. Er is een training beschikbaar waarmee medewerkers worden geïnformeerd over de basis van de AVG. Waar mogelijk wordt de samenwerking gezocht met informatieveiligheid.

8.9 Verantwoording
Onder de verantwoordelijkheid van zowel het college van B en W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren. De FG brengt jaarlijks een verslag uit aan de het college van zijn werkzaamheden, bevindingen en aanbevelingen.

Om de directie te informeren brengt de PO jaarlijks een jaarverslag uit over de privacyvragen, datalekken, DPIA's, verzoeken van betrokkenen en andere privacygerelateerde gebeurtenissen uit het afgelopen jaar. Tevens biedt de PO het verslag van de jaarlijkse AVG compliance meting aan aan de directie ter informatie en voor het nemen van maatregelen.

8.10 AVG compliance meting
Om te kunnen bepalen wat gemeente Borne moet doen om de bescherming van persoonsgegevens te verbeteren, is het noodzakelijk om regelmatig in beeld te brengen hoe de gemeente ervoor staat als het gaat om de omgang met persoonsgegevens conform de AVG. Hiervoor voeren we jaarlijks een AVG compliance meting uit met behulp van het borgingsproduct van de VNG. Het borgingsproduct is een normenkader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente. Hiermee krijgen we inzicht in de groei en de stappen die nog gezet moeten worden richting een privacyvolwassen organisatie.

8.11 PDCA Cyclus
De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus. Deze PDCA cyclus is ook vereist om volwassenheidsniveau 4 te behalen. Dit betekent dat we niet alleen processen hebben en maatregelen nemen, maar dat deze ook gemeten, geëvalueerd en verbeterd worden.

9. Inwerkingtreding, evaluatie en ondertekening

Dit privacybeleid treedt een dag na bekendmaking in werking. Het privacybeleid gemeente Borne 2019 wordt per die datum ingetrokken.

Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld door grote organisatorische veranderingen, wetswijzigingen of uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.

Dit beleid is vastgesteld op 5 september 2023 door het college van burgemeester en wethouders als eindverantwoordelijke voor de gemeentelijke gegevensverwerking.