Controleplan Privacy Opsterland 2026



gemeente Opsterland

Inhoud

.....1
H1 – Inleiding.....3
H1.1 Doel van het toezicht.....3
H1.2 Kaders toezicht.....3
H1.3 Risicomanagement.....4
H1.4 De OWO-samenwerking.....4
H1.5 Het AVG Borgingsproduct van de IBD.....4
H2 – Inrichting van de controles door de FG.....5
H2.1 De 7 thema's van gegevensbescherming.....5
H3 – De uitvoering van het controleplan.....8
H3.1 Controlemethodiek.....8
H3.2 Controlespoor.....8
H3.3 Risicogericht.....8
H3.4 Controlestappen.....8
H3.5 Ad hoc en gepland.....9
Bijlage 1 – Uit te voeren audits in 2026.....10

H1 – Inleiding

In dit document staat de inrichting van het controleplan van de Functionaris Gegevensbescherming (FG) centraal. Het controleplan geeft inzicht in de manier waarop de controles van de FG zijn vormgegeven.

Waarom een controleplan?
Als gemeente willen wij graag dat mensen erop kunnen vertrouwen dat hun persoonsgegevens bij ons in goede handen zijn. Er wordt vaak direct gedacht aan de gegevens van inwoners (terecht), maar het gaat uiteraard ook om de gegevens van medewerkers. In totaal gaat het om alle persoonsgegevens die de gemeente verwerkt of laat verwerken.

De risicobeheersing rondom privacy is dynamisch. Nieuwe wet- en regelgeving, wijzigingen in processen en nieuwe applicaties zijn maar een paar voorbeelden waarmee rekening gehouden moet worden. Er wordt dan ook hard gewerkt om de privacy van betrokkenen zo goed mogelijk te blijven borgen in de organisatie. Het is aan de Functionaris Gegevensbescherming om inzicht te verkrijgen in hoeverre de gemeente aan wet- en regelgeving rondom privacy voldoet. Daarvoor heeft de FG onder andere een toezichthoudende taak. Voor het toezicht is dit controleplan opgesteld.

Hieronder worden enkele elementen uit het controleplan verder uitgewerkt.

H1.1 Doel van het toezicht

Het belangrijkste is dat de privacy van de personen van wie de gemeente gegevens verwerkt voldoende geborgd is. Daarvoor is het belangrijk dat de wet- en regelgeving in de paktijk gebracht worden. Naast dat het wettelijk verplicht is om toezicht uit te voeren, is het ook wenselijk. De moeilijkheid is om wet- en regelgeving een paktische uitvoering te geven. Door toezicht wordt het mogelijk om te zien of er aan de wet- en regelgeving voldaan wordt. Maar nog belangrijker is dat er bij het toezicht kennisdeling gedaan wordt met de medewerkers, waardoor die meegenomen worden in de ontwikkelingen in het vakgebied. Het toezicht helpt om de regels uit te leggen naar de praktijk. Dat is geen éénrichtingsverkeer, maar een gezamenlijke opdacht voor de gehele organisatie. Soms is de toepassing van de wet- en regelgeving in de praktijk weerbastig en zal gezamenlijk gezocht worden naar een passen de oplossing. Een belangrijk uitgangspunt van de wet- en regelgeving is dat er steeds een belangenafweging gemaakt wordt. Er wordt dan ook niet zwart of wit naar de wet- en regelgeving gekeken.

Door toezicht uit te oefenen wordt duidelijk waar de organisatie zich verder in moet ontwikkelen en kunnen adviezen gegeven worden.

Het toezicht maakt het mogelijk om verantwoording af te leggen. Samen met onder andere de adviezen zorgt dit ervoor dat het management goed overwogen beslissingen kan maken. De verantwoording maakt het ook mogelijk voor het college van B&W en de raad om hun rol te vervullen.

H1.2 Kaders toezicht

Eén van de taken van de FG is toezien op de naleving van de wet- en regelgeving (art 39 AVG). Naast de AVG moet toezicht gehouden worden op andere relevante privacywet- en regelgeving. Daarbij kan geacht worden aan de Uitvoeringswet AVG en de Wet politiegegevens (Wpg), maar ook specifieke materiewetgeving zoals de Jeugdwet. Ook moet er toezicht gehouden worden op het eigen privacybeleid van de gemeente Opsterland. Aandachtspunten daarbij zijn: toewijzing van verantwoordelijkheden, bewustmaking en

opleiding van het bij de verwerking betrokken personeel en de betreffende audits. De FG kan op basis van het reglement van de FG de controles uitvoeren. Voor meer informatie over de positie en de taken en bevoegdheden van de FG wordt naar het reglement verwezen.

H1.3 Risicomanagement

Risicomanagement voor privacy en informatiebeveiliging (P&IB) is verder uitgewerkt in het document Opzet cluster Privacy en informatiebeveiliging. Ik het kort komt het erop neer dat de uitvoerende teams zelf verantwoordelijk zijn voor het risicomanagement en daarbij ondersteund worden door de Privacy Officer (PO) en Chief Information Security Officer (CISO) en dat de FG onafhankelijk toezicht houdt.

De FG moet informatie verkrijgen vanuit de organisatie, zodat er een beeld verkregen kan worden over waar de gemeente Opsterland staat met betrekking tot het veilig verwerken van (persoons-) gegevens. De informatie kan verbeterd worden en daaraan wordt ook gewerkt.
Informatie kan komen uit werkzaamheden van bijvoorbeeld kwaliteitsmedewerkers. Bij VTH is voor de Wpg in 2025 een kwaliteitsmedewerker gestart en zijn mooie stappen gezet in de beheersing van de risico's rondom de Wpg. Ook binnen het eigen cluster worden de werkzaamheden van de PO en CISO gebruikt als informatiebron. Voor de informatiebeveiliging is de ENSIA verantwoording en de implementatie van de BIO van belang als input. De FG kan daar kennis van nemen en reviews en eigen deelwaarnemingen doen. Het risicomanagement zit in de opbouwfase. De FG probeert een bijdrage te leveren door bij audits en reviews adviezen te geven om het risicomanagement en tegelijk de informatiestroom te verbeteren.

H1.4 De OWO-samenwerking

De gemeente Opsterland werkt samen met Weststellingwerf en Ooststellingwerf in de OWO-samenwerking. Zeker op het gebied van Privacy en Informatiebeveiliging is deze samenwerking intensief. Voor veel van de systemen waarin persoonsgegevens verwerkt worden ligt de hoofdverantwoordelijkheid bij één van de drie gemeenten. Iedere gemeente heeft een eigen cluster privacy en informatiebeveiliging. Dat is nodig voor advisering per gemeente en ook voor het uitvoeren van de wettelijke taken. Uiteraard wordt waar mogelijk samengewerkt. Er zijn dan ook vaste periodieke overleggen en wordt beleid waar mogelijk gezamenlijk opgesteld. De samenwerking zorgt er ook voor dat er lokaal andere accenten gelegd worden en er bij de gemeente overstijgende werkzaamheden samengewerkt wordt.

H1.5 Het AVG Borgingsproduct van de IBD

Voor de jaarlijkse verslaglegging wordt gebruik gemaakt van het AVG borgingsproduct. Het borgingsproduct is een instrument, ontwikkeld door de Informatiebeveiligingsdienst (IBD), dat gemeenten helpt om structureel aan de AVG te voldoen. Het borgingsproduct is een toetsingskader en bestaat uit verschillende vragen die per thema zijn ingedeeld. De uitgangspunten van het borgingsproduct worden waar mogelijk meegenomen in de audits. Omdat de thema's meer overkoepelend zijn dan de meeste audits, worden er onderdelen van in specifieke audits betrokken. In samenwerking met de PO, CISO en FG wordt het borgingsproduct jaarlijkse gevuld mede op basis van de audits. De uitkomsten van het borgingsproduct worden gebruikt voor het jaarverslag van de FG.

H2 – Inrichting van de controles door de FG

Voor de controle op het naleven van de AVG maakt de FG gebruik van de kwaliteitscyclus.

De kwaliteitscyclus bestaat uit 7 thema's die gezamenlijk alle aspecten van gegevensbescherming dekken. In onderstaande afbeelding is dit visueel weergegeven:



H2.1 De 7 thema's van gegevensbescherming

Hieronder worden de thema's kort toegelicht en wordt aangegeven hoe de FG deze bij de audits kan betrekken.

1. Beleid

De organisatie moet de processen en bijbehorende verantwoordelijkheden en risico's weten en vastgelegd hebben in beleidsstukken. Deze stukken moeten voor alle werknemers goed vindbaar en begrijpelijk zijn.

De kunst is om de wet- en regelgeving op een praktische manier door te vertalen in beleid zodat de medewerkers die in de praktijk kunnen brengen. Gelukkig zijn de uitgangsbeginselen in de AVG uitgewerkt, waarmee er een goede uitgangsbasis is voor alle processen. Op sommige verwerkingen is specifieke wet- en regelgeving van toepassing.

Aandachtspunten bij de audits zijn of de relevante beleidsstukken begrijpelijk en vindbaar zijn voor de medewerkers. Ook kan het beleid getoetst worden aan hogere wet- en regelgeving.

2. Processen

De organisatie moet de processen ingericht hebben volgens de beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Uiteraard moeten de processen actueel zijn en nageleefd worden.

Processen kunnen op verschillende manieren geheel of gedeeltelijk in audits betrokken worden. Daarbij kan getoetst worden aan de relevante genoemde beginselen.

3. Organisatorische inbedding

Bij organisatorische inbedding gaat het om het toewijzen van taken, verantwoordelijkheden en bevoegdheden en het creëren van bewustzijn.

Bij audits kan gekeken worden naar of duidelijk is wie de proceseigenaar is. En of er binnen het team van de proceseigenaar voldoende kennis, kunde en middelen zijn om aan de verantwoordelijkheden en bevoegdheden invulling te geven. Maar er kan bijvoorbeeld ook gekeken worden naar of de medewerkers voldoende op de hoogte zijn van privacy en informatiebeveiliging in hun werkveld. Kortom, staan er niet alleen uitgangspunten op papier, maar worden die daadwerkelijk zichtbaar toegepast?

4. Rechten van betrokkenen

Van belang is dat betrokkenen voldoende geïnformeerd worden over de verwerkingen en of ze makkelijk hun rechten onder de AVG kunnen uitoefenen.

Bij audits kan bijvoorbeeld gecontroleerd worden of een inwoner bij een aanvraag voldoende geïnformeerd wordt over de verwerking van persoonsgegevens. Een ander voorbeeld is een audit op uitgevoerde inzage verzoeken, zodat het proces daarbij beoordeeld kan worden.

5. Samenwerking

Bij verwerkingen door derden kan het noodzakelijk zijn om verwerkersovereenkomsten af te sluiten.

Bij audits kan gecontroleerd worden of verwerkingsovereenkomsten noodzakelijk zijn. Er kan ook beoordeeld worden of de afspraken voldoende zijn en er voldoende verantwoording is over de naleving daarvan.

6. Gegevensbescherming

In artikel 32 AVG staat dat een organisatie passende technische en organisatorische maatregelen moet nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. Dit doet de gemeente door de Baseline Informatiebeveiliging Overheid (BIO) uit te voeren. Om te voldoen aan de AVG, moet je ook voldoen aan de BIO.

Bij audits kan gecontroleerd worden in hoeverre voldaan wordt aan de beheersmaatregelen uit de BIO. Daarnaast is er een meldplicht voor inbreuk met persoonsgegevens (privacyincidenten). Daarom kunnen ook de datalekken en beveiligingsincidenten in de audits worden betrokken.

7. Verantwoording

De gemeente moet zelf aantonen in welke mate er voldaan wordt aan de privacyregels. Met een goede verantwoording wordt bijgedragen aan de bescherming van grondrechten van mensen op het gebied van privacy.

Per audit wordt er een rapportage opgesteld en toegestuurd aan de betreffende teammanager, relevante medewerkers en de concerncontroller. Eventuele aanbevelingen worden dan direct afgestemd met de leidinggevende, waarna die in de Audit & Control rapportage geplaatst worden om de verder afhandeling te monitoren. De A&C-rapportage wordt twee keer per jaar afgestemd in het MT breed inclusief de directie.

In het jaarlijkse verslag van de FG worden de voor de verslaglegging relevante bevindingen meegenomen. Bij het jaarverslag wordt gebruik gemaakt van het AVG borgingsproduct van de Informatiebeveiligingsdienst. Dit wordt verder toegelicht in het jaarverslag. Het jaarverslag wordt ter kennisname aangeboden aan het college.

H3 – De uitvoering van het controleplan

Tijdens de uitvoering van het controleplan staan enkele uitgangspunten centraal. Hieronder volgt de uitwerking hiervan.

H3.1 Controlemethodiek

De FG kan verschillende methodes hanteren om het toezicht uit te voeren, zoals:

- Onderzoek van documenten (bijvoorbeeld toetsing van processen aan wet- en regelgeving;
- Deelwaarnemingen van dossiers;
- Reviews
- Analyses van werkprocessen, systemen en gegevensstromen;
- Interviews;
- Observatie/eigen waarnemingen.

H3.2 Controlespoor

Het is van belang dat de documentatie en de vastlegging van de controle voor een ander inzichtelijk en begrijpelijk is. Dit wordt ook wel het controlespoor of audittrail genoemd. Dat geldt ook voor controles die door een uitvoerend team zelf gedaan worden. Gedacht kan worden de vastlegging van de controle op rollen en autorisaties door de applicatiebeheerder (in opdracht van de eigenaar). Dit is van belang om naast opzet van een beheersmaatregel ook het bestaan en werking aan te tonen. De controles van de teams zelf kunnen door de FG betrokken worden in een review, zodat onafhankelijk een oordeel gevormd kan worden. Door een goed controlespoor wordt het mogelijk om een review te doen.

Ook voor de audits van de FG geldt dat deze goed vastgelegd moeten worden.

H3.3 Risicogericht

Eén belangrijk uitgangspunt van de wet- en regelgeving is dat er steeds gekeken wordt naar nut en noodzaak. Wat is er praktisch haalbaar? Ook bij de audits wordt gebruik gemaakt van gezond boerenverstand. De audits van de FG worden zoveel mogelijk met risicogerichte deelwaarnemingen, reviews en niet dossier toetsvragen (bijvoorbeeld controles op autorisaties of een analyse van een systeem) uitgevoerd.

H3.4 Controlestappen

Per audit zal bepaald worden wat de beste methode van onderzoek is. Bij de meeste audits zullen onderstaande stappen doorlopen worden:

Controlestappen

- Risicogerichte selectie verwerkingen.
- Relevante wet- en regelgeving (beleid) bepalen.
- Opstellen van een controleaanpak (toetsvragen).
- Opstellen werkprogramma (Excel voor vastlegging toetsvragen en bevindingen).
- Uitvoering controle (deelwaarneming en of niet dossier toetsvragen).
- Vastleggen controleresultaten.
- Rapportage (adviezen) afstemmen.
- Adviezen op de Audit & Control rapportage.

H3.5 Ad hoc en gepland

Ad hoc werkzaamheden

Bij de dagelijkse werkzaamheden zitten verschillende ad hoc of incident gedreven werkzaamheden. Zo kan de FG betrokken worden bij bijvoorbeeld datalekken, vragen, klachten en inzageverzoeken. Deze ad hoc werkzaamheden worden vastgelegd in verschillende registers, waarop de FG toezicht houdt.

Data Protection Impact Assessment (DPIA's) zijn vaak ad hoc en kunnen verplicht zijn bij nieuwe applicaties / processen. Daarbij wordt standaard het advies van de FG gevraagd (art 35, lid 2 AVG).

Deze ad hoc werkzaamheden worden gebruikt om inzicht verkrijgen in de mate waarin de organisatie aan de AVG voldoet en zijn ook een informatiebron voor het jaarverslag van de FG.

Geplande audits

Naast de ad hoc werkzaamheden zijn er de geplande audits. Dit jaar richt de FG zich vooral op het op orde brengen en het beoordelen van de basisprocessen zodat het risicomanagement verhoogd wordt. Daarvoor zijn audits gepland die beschreven staan in bijlage 1.

Bijlage 1 – Uit te voeren audits in 2026

Het plan is om over het jaar 2026 op onderstaande punten een audit uit te voeren:

1) Register van verwerkingen bij de Wet politiegegevens.

2) Register van verwerkingen AVG.

3) Register van rechten van betrokkenen.

4) Risico acceptatieregister.

5) Register van datalekken.

6) Proces DPIA's

In de AVG wordt bij het toezien op naleving van de wet- en regelgeving op het gebied van privacy aangegeven dat daarbij ook gekeken moet worden naar het toewijzen van verantwoordelijkheden, bewustmaking in opleiding van medewerkers en naleving van audits. Daarom zijn er jaarlijks audits op onderstaande onderdelen:

7) Toetsing naleving toewijzing verantwoordelijkheden.
   Hierbij wordt o.a. het privacybeleid gecontroleerd.

8) Toetsing naleving bewustmaking en opleiding.
   Hierbij wordt o.a. het privacybeleid gecontroleerd.

9) Toetsing naleving audits.
   Hierbij wordt o.a. de afhandeling van de Audit & Control rapportage betrokken.

Voor informatiebeveiliging wordt dit jaar aangeschoven bij de CISO om inzicht te verkrijgen in de ENSIA verantwoording en de BIO2 implementatie.