JAARVERSLAG 2023

FUNCTIONARIS GEGEVENSBESCHERMING

Gemeente Woudenberg

Inhoudsopgave

1. Inleiding en terugblik

Het jaar 2023 is voor de organisatie een jaar geweest waarin hard is gewerkt aan de bestendiging van de formatie. Veel vacatures zijn inmiddels ingevuld.

Hybride werken is inmiddels de norm geworden, waar de huidige organisatievorm ook op is ingericht. Er wordt gewerkt met laptops die uitgegeven en beheerd worden door de eigen organisatie. Eind 2023 is ook de telefonie aangepast aan de huidige praktijk. Door MS Teams ook in te zetten als telefooncentrale is een stap gemaakt naar een verbeterde bereikbaarheid en tegelijkertijd meer regie van werknemers over de tijden waarop deze bereikbaar zijn voor telefoontjes.

In 2023 is met name de focus gelegd op enkele bijzondere wetten (WOO/WPG) die een duidelijke link hebben met de AVG. Er is geïnvesteerd in het aanstellen van een aparte WOO-functionaris zodat er in beginsel door de FG meer tijd over blijft om te besteden aan de onafhankelijke toezichtstaak.

Er is samen met een aantal collega's van Coöperatie De Kleine Schans (uitvoeringsorganisatie Sociaal Domein) deelgenomen aan een cursus AVG/Privacy in het sociaal domein. In het kader van privacy- en informatiebeveiliging awareness wordt iedere week een mail verstuurd naar alle medewerkers met een stelling over een privacy- of informatiebeveiligingsvraag. De Functionaris Gegevensbescherming heeft samen met de CISO en collega's veiligheid bijdragen aan de heraudit in het kader van de WPG. De resultaten van deze hercontrole laten een beeld zien van een organisatie die, binnen de kaders van beschikbare capaciteit, serieus bezig is met informatieveiligheid en de bescherming van persoonsgegevens.

In bijgevoegd jaarverslag vindt u op hoofdlijnen de weerslag van de verrichtte werkzaamheden, de bevindingen over het afgelopen jaar en aanbevelingen voor het komende jaar.

2. Aandachtspunten uitvoering AVG

Bij de aanschaf van nieuwe applicaties wordt getoetst of de leverancier voldoet aan de benodigde beveiligingsvereisten. Dit is echter niet zozeer AVG-gerelateerd, maar meer vanuit richtlijnen zoals de BIO of andere wetgeving over de technische beveiligingseisen van cloudapplicaties.

Recent uitgevoerde audits op bijvoorbeeld de SUWI-applicatie en de applicaties van burgerzaken laten zien dat met name procesbeschrijvingen (het niet alleen kunnen vertellen dat een maatregel getroffen is, maar dit ook aantoonbaar op papier hebben staan) nog verbeterd moeten worden. Waar voorheen veel meer de focus lag op het bestaan van applicaties en het checken of die voldoen aan de vereisten (Third Party Memorandum) volstaat dit niet meer. We voldoen weliswaar aan de minimale normen om de audits te halen, maar willen in 2024 pro actiever handelen. De basis daarvoor zijn de aanbevelingen die gegeven zijn in de verschillende auditrapporten.

Het afgelopen jaar zijn er vier AVG-verzoeken binnen gekomen. De verzoeken die binnen zijn gekomen zijn vooral inzagevragen op welke wijze wij persoonsgegevens wel/niet registreren. Binnen de daarvoor geldende termijnen worden AVG-verzoeken afgehandeld. Tegen de afgehandelde verzoeken is geen bezwaar gemaakt.

De vraag of de organisatie voor een bepaald doel (b.v. onderzoek) (persoons)gegevens mag verzamelen en verwerken komt geregeld terug. Op zich is dit positief omdat dit aangeeft dat medewerkers zichzelf in elk geval al die vraag stellen. Met name binnen het sociaal domein speelt deze vraag. In goede samenwerking met de juridisch kwaliteitsmedewerker van Coöperatie De Kleine Schans wordt hier

door de FG antwoord op gegeven. Dit is nu nog casueel, het is de bedoeling om hier in 2024 een richtlijn voor op te stellen die meer richting geeft voor medewerkers die met deze vraag worstelen.

Onverkort blijft het binnen de organisatie wel nodig aandacht te besteden aan het alleen verzamelen en verwerken van persoonsgegevens voor van te voren bestemde doelen. En dit dan alleen voor zolang als dat voor dat doel nodig is.

2a. Sturing en monitoring
Doordat de organisatie medio 2023 op papier gekanteld is van een (deels) zelforganiserende organisatie naar een hybride vorm (vakteams ingedeeld in 3 clusters aangestuurd door een manager) heeft de focus gelegen op de inrichting van die teams. De medewerkers zelf zijn in de eerste plaats verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen hun taakveld plaats vinden. De Functionaris Gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming. (AVG)

Bij de uitvoering van deze werkzaamheden bekleedt de FG een onafhankelijke positie en ontvangt deze geen instructies over de uitvoering van het bijbehorende takenpakket.

3. Rol en taken functionaris voor de gegevensbescherming (FG)

Naast functionaris voor de gegevensbescherming (FG) voor de gemeente Woudenberg is ondergetekende ook de FG voor Coöperatie De Kleine Schans. Voor beide functies staat ondergetekende ingeschreven bij de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens. De rol en taken van de FG zijn in het afgelopen jaar niet veranderd.

3a. Rol en taken FG

Het takenpakket van de FG omvat onverminderd de volgende onderdelen:

- Het houden van toezicht op de toepassing en naleving van de AVG en het gemeentelijk beleid betreffende de bescherming van persoonsgegevens.
- De verantwoordelijkheid voor de opstelling en actualisering van het register van gegevensverwerkingen.
- Het verstrekken van advies, informatie en voorlichting over de verwerking van persoonsgegevens aan de ambtelijke organisatie en het bestuur.
- Het fungeren als in- en extern aanspreekpunt over de AVG en de bescherming van de persoonlijke levenssfeer bij vragen, klachten en ingediende verzoeken met daarbij de coördinatie van de tijdige afhandeling hiervan.
- Het optreden als de gemeentelijk contactpersoon voor de Autoriteit Persoonsgegevens.
- Het houden van toezicht op en adviseren over de uitvoering van de gegevensbescherming effectbeoordelingen (=Privacy impact analyses).
- Rapporteren aan directie en college over het gevoerde beleid, de toepassing en naleving van de AVG en opgetreden incidenten met betrekking tot gegevensverwerkingen.

4. Uitvoering taken FG

4a. Toezicht op toepassing en naleving AVG en het gemeentelijk beleid betreffende de bescherming van persoonsgegevens
In een kleine organisatie als die van Woudenberg is de rol van FG veelal uitvoerend van aard. De FG houdt toezicht door middel van het meewerken aan verschillende audits, het afhandelen van AVG-verzoeken en het meedenken en adviseren over privacy kwesties.

Een verbetering die verder ontwikkeld moet worden is het meer “vooraf” in het proces komen van de CISO/FG. Bij de aanschaf van applicaties is het niet standaard dat er ook gekeken wordt vanuit de AVG of er voldaan wordt aan de vereisten. Veeleer zijn andere aspecten leidend zoals de vraag of de applicatie past binnen het gewenst applicatielandschap. Een toets op de inhoud vooraf (DPIA) is nog niet gebruikelijk. Hier gaat in 2024 nog een verbeterslag op gemaakt worden.

4b. Register gegevensverwerkingen
Het huidige verwerkingsregister dateert uit 2018. Sindsdien is deze niet meer aangepast. In 2023 is bij een audit van de WPG geconstateerd dat er geen apart WPG-verwerkingsregister is. Deze is alsnog opgesteld. Voor het huidige verwerkingsregister geldt dat deze aan een herziening toe is. In de praktijk volstaat de huidige versie nog. Werkprocessen zijn echter aan verandering onderhevig, zodat een herziening van dit register voor 2024 op de planning staat.

4c. Verwerkersovereenkomsten
Gemeenten zijn op basis van de AVG wettelijk verplicht een verwerkersovereenkomst (VWO) af te sluiten met alle opdrachtnemers die namens hen persoonsgegevens verwerken. Tijdens de algemene ledenvergadering van de Vereniging van Nederlandse Gemeenten werd op 5 juni 2019 besloten om de door de Informatiebeveiligingsdienst (IBD) opgestelde standaard verwerkersovereenkomst per 1 januari 2020 verbindend te verklaren voor alle Nederlandse gemeenten. Met de vaststelling van deze standaard VWO hebben alle gemeenten gekozen voor uniforme afspraken over het verwerken van persoonsgegevens. Deze standaard is in overleg met landelijke leveranciers ontwikkeld door én voor gemeenten. Met deze overeenkomst wordt uitgesloten dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. In de verwerkingsovereenkomst worden onderwerp, duur, aard en doel van de verwerking vastgelegd met daarbij de soort persoonsgegevens en de getroffen technische en organisatorische maatregelen om de verwerkingen veilig te stellen en de persoonsgegevens en privacy van betrokkenen te beschermen.

Het afgelopen jaar zijn een aantal verwerkersovereenkomsten voorgelegd aan de FG ter beoordeling. Registratie van de aantallen die worden voorgelegd, worden niet bijgehouden. Het aantal jaarlijks afgesloten verwerkersovereenkomsten wisselt sterk. Veelal zijn het leveranciers of externe partners die een verwerkersovereenkomst voorbereiden zodra er een dienst wordt afgenomen. De FG checkt of de verwerkersovereenkomst voldoet aan de standaard die de IBD heeft opgesteld. Afwijken is mogelijk indien beide partijen hiermee in kunnen stemmen.

De FG is verantwoordelijk voor het blijvend verzorgen van awareness bij de medewerkers. Er is een procesbeschrijving aanwezig wanneer er wel/niet een verwerkersovereenkomst opgesteld moet worden.

4d. Advisering, informatieverstrekking en voorlichting over AVG
In een kleine organisatie als Woudenberg met veel éénpitters is goed bekend wie de FG is waarbij advies kan worden gevraagd. Adviesaanvragen over de verwerking van persoonsgegevens komen van alle beleidsterreinen.

De FG heeft ook een zelfstandige rol als het gaat om het afhandelen van AVG-verzoeken. Zoals eerder genoemd is aantal AVG-verzoeken (4) in 2023 zeer gering geweest. We zien daarentegen dat het aantal WOO-verzoeken toeneemt waarbij eveneens de AVG toegepast moet worden (anonimiseren van documenten). Met het aantrekken van een aparte WOO-functionaris en het aanschaffen van een nieuwe anonimiseringstool is er dit jaar een stap voorwaarts gezet.

Waar voor wat betreft de AVG stappen te maken zijn, dat is het uitvoeren van DPIA's. Voor applicaties met persoonsgegevens die in beheer zijn bij externe samenwerkingspartners (b.v. een centrumgemeente) wordt vaak een DPIA uitgevoerd door de verwerker. Hier kan meer regie op worden uitgevoerd door de eigen organisatie.

Er is een privacybeleid dat dit jaar is aangepast door ook de WPG als een apart onderdeel op te nemen. Het huidige beleid dateert uit 2018 en alhoewel deze nog grotendeels actueel is, staan de ontwikkelingen niet stil. Een update van dit beleid is dan ook wenselijk en zal in 2024 voor besluitvorming aan het college worden voorgelegd.

5. Bewustwordingsactiviteiten

De verschuiving van fysiek aanwezig zijn naar een organisatie die hybride werkt maakte dat de aandacht eerst gelegd is op het creëren van een omgeving die borgt dat er informatieveilig gewerkt kan worden. Voor veilig mailen is de tool Zivver in gebruik. De software zorgt er voor dat deze applicatie vanzelf wordt ingeschakeld wanneer er gevoelige gegevens in een mail zitten. Medewerkers kunnen dit handmatig weer uitschakelen. In hoeverre hiervan gebruik wordt gemaakt, is onduidelijk.

Door de wekelijkse privacy- en informatiebeveilingsvraag die alle medewerkers krijgen in hun mailbox is aan bewustwording gedaan. Ieder jaar wordt er minimaal 1 phishingmail gestuurd. Ook krijgen alle nieuwe vaste medewerkers een verplichte online training waarin zowel privacy als informatiebeveiliging worden behandeld.

6. Datalekken

Sinds 1 januari 2016 is de Wet meldplicht datalekken in werking. Een datalek is een inbreuk op de beveiliging waarbij een kans bestaat dat deze inbreuk ernstige gevolgen heeft voor de bescherming van de persoonsgegevens. Als er sprake is van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, de wijziging of de ongeoorloofde verstrekking van persoonsgegevens dan wel ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens en de persoonlijke levenssfeer van betrokkenen hierdoor is geschaad, moet een dergelijk datalek binnen 72 uur na ontdekking hiervan worden gemeld aan de toezichthoudend autoriteit, de Autoriteit Persoonsgegevens. De FG is verantwoordelijk voor de melding aan de Autoriteit Persoonsgegevens. Bij alle andere datalekken volstaat de melding aan FG.
Er is een apart e-mailadres gegevensbescherming@woudenberg.nl waarop inbreuken op de beveiliging gemeld kunnen worden. Dit kan gaan om datalekken, of een melding van vermoeden van een datalek.

De CISO/FG hebben vervolgens afstemming over de melding. Afhankelijk van de inbreuk en de getroffen/nog te treffen maatregelen bepalen zij of er een (voorlopige) melding van een datalek bij de Autoriteit Persoonsgegevens gedaan moet worden. Er is een procedure incidenten en datalekken vastgesteld die beschrijft op welke wijze hiermee wordt omgegaan.

Wanneer op basis van de melding wordt geconstateerd dat sprake is van een datalek, documenteert de FG de gemelde incidenten en worden deze met het oog op de op grond van de AVG bestaande verantwoordingsplicht opgenomen in het interne 'register datalekken'

In die situaties waarbij een datalek ontstaat bij een door de gemeente voor de uitvoering van bepaalde werkzaamheden ingeschakelde externe organisatie die als verwerker van persoonsgegevens optreedt, dient deze organisatie een beveiligingsincident zo snel mogelijk te melden aan de betreffende verantwoordelijke binnen de gemeente. Voor de afhandeling hiervan geldt eenzelfde procedure als bij de intern ontstane beveiligingsincidenten/datalekken. De betreffende organisatie dient het datalek zelf te melden aan de Autoriteit Persoonsgegevens.

6a. Register datalekken
Sinds 2018 wordt een register datalekken bijgehouden. In het register staat een beschrijving van de inbreuk, de mogelijke gevolgen hiervan, de getroffen corrigerende maatregelen en of hiervan een melding is gedaan aan de Autoriteit Persoonsgegevens en betrokkenen.

In 2023 werden 6 (mogelijke) datalekken gemeld. Er zijn geen datalekken gemeld aan de Autoriteit Persoonsgegevens, omdat er of bij nader inzien toch geen sprake was van een datalek, of omdat er met de betrokkenen was afgestemd en de melding adequaat was afgehandeld.

7. Coördinatie indienen verzoeken door betrokkenen

De FG is het eerste aanspreekpunt bij vragen of klachten en de indiening van verzoeken door betrokkenen over de verwerking van hun persoonsgegevens en de bescherming van de persoonlijke levenssfeer/privacy (conform de artikelen 15 tot en met 18 en 20 + 21 van de AVG). Bij ontvangst van dergelijke verzoeken beoordeelt de FG welk soort verzoek het betreft, of betrokkene zich gelegitimeerd heeft en diens identiteit kon worden vastgesteld en of aan het verzoek voldaan kan worden. De FG is ook degene die een beslissing op het AVG-verzoek neemt.

8. Samenwerking CISO

De CISO en FG werken nauw samen op het gebied van informatieveiligheid. De CISO is verantwoordelijk voor het toezicht op het technisch waarborgen van informatieveiligheid, terwijl de FG meer zit op het toezicht of de organisatie handelt overeenkomstig de AVG. Bij meldingen van (mogelijke) inbreuken op de beveiliging wordt samen overlegd welke vervolgacties noodzakelijk zijn.

De CISO en FG zijn beide betrokken bij de uitvoering jaarlijkse audits (SUWI) en self assessments (ENSIA) waarbij ook de AVG een onderdeel is van de vragen die beantwoord moeten worden. Periodiek vindt afstemming plaats over de acties die in het kader van onder meer bewustwording en verantwoording uitgevoerd moeten worden.

9. Conclusies en aanbevelingen

Het privacy- en informatieveiligheidsbewustzijn binnen de organisatie is het afgelopen jaar op een acceptabel niveau gebleven. Het werken met persoonsgegevens is onlosmakelijk verbonden aan het werken voor een overheidsorganisatie. Dit brengt een extra zware verantwoordelijkheid met zich mee. De medewerkers zijn bewust van de noodzaak van bescherming van persoonsgegevens en weten de FG te vinden bij vragen over verwerking van persoonsgegevens.

De organisatie voldoet aan de eisen die de AVG stelt. Tegelijkertijd blijven de ontwikkelingen groot op het gebied van technologie, en daarmee gepaard gaande privacy vraagstukken. Het aantrekken van nieuwe medewerkers die nog geen overheidservaring hebben vraagt om een doordenking op welke wijze de aandacht voor privacy vastgehouden wordt. En om uitleg welke privacyregels en procedures er zijn, waar deze te vinden zijn, en hoe je er naar moet handelen.

De inbreuken op de beveiliging die zijn gemeld laten geen structureel patroon zien, maar zijn op zichzelf staande incidenten geweest. Per ongeluk een mail sturen naar een verkeerde afzender in de CC, of een brief die verkeerd bezorgd en geopend wordt, zijn weliswaar inbreuken op de beveiliging van persoonsgegevens, maar wel eenmaal en verklaarbaar geweest. Er is geen 100% zekerheid om datalekken te voorkomen. Wel is door preventie (voorlichting en weten waar je moet zijn voor privacy vragen) het eenvoudiger om snel maatregelen te treffen als een datalek zich voordoet.

Op het aantal AVG-verzoeken dat wordt ingediend kan geen invloed worden uitgeoefend. Ook hiervoor geldt dat op dit moment het aantal verzoeken zeer gering is, en er geen patroon in deze verzoeken te zien is.

10. Vooruitblik/speerpunten werkzaamheden FG 2024

Naast de toezichthoudende, adviserende, informerende en voorlichtende rol zijn de speerpunten voor 2024:

- Actualisatie van het verwerkingenregister
- Herziening van het privacybeleid
- Het inventariseren voor welke voor (nieuwe) werkprocessen waarin sprake is van risicovolle verwerkingen van persoonsgegevens het uitvoeren van een DPIA nodig is.
- Uitvoeren acties heraudit WPG
- Nieuwe bewustwordingsacties voor medewerkers opzetten

Woudenberg, 9 januari 2024