FG Jaarrapportage 2024

Gemeente Veere

CLASSIFICATIE: Intern
VERSIE: 1.1
DATUM: 9 januari 2025

Managementsamenvatting

Dit document bevat de jaarrapportage van de Functionaris voor Gegevensbescherming (FG) van de gemeente Veere. De FG fungeert als toezichthouder en adviseur omtrent de naleving van de Algemene verordening gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). Tevens dient de FG als aanspreekpunt voor alle betrokkenen.

Voor de jaarrapportage heeft de FG de privacymaatregelen getoetst die de gemeente Veere in 2024 heeft genomen. Hiernaast geeft de rapportage een overzicht van de uitgevoerde toezichtactiviteiten, DPIA's en documentbeoordelingen. De vooruitgang is gemeten aan de hand van opvolging van de thema's van de Privacy Baseline van het Centrum Informatiebeveiliging en Privacy (CIP). Voor de Wpg is gecontroleerd aan de hand van de beheersmaatregelen vanuit het NOREA normenkader voor de Wpg.

De ambitie van de gemeente Veere is om privacyvolwassenheidsniveau 3, "Vastgesteld", te behalen op alle thema's van de Privacy Baseline. Voor de getoetste privacy onderdelen komt de gemeente Veere uit op minimaal niveau 3. Voor onderdeel verwerkingsregister komt de gemeente uit op volwassenheidsniveau 4. De gemeente Veere voldoet hiermee aan de eisen die de AVG aan haar stelt. Het register voldoet aan de wettelijke vereisten uit artikel 30 AVG en de gemeente borgt dat periodieke herziening volgt. Zo is het register actueel en kloppend. Voor onderdeel DPIA's komt de gemeente Veere uit op volwassenheidsniveau 3. De DPIA systematiek werkt binnen de organisatie en medewerkers zijn goed op de hoogte van de te nemen stappen bij een nieuwe verwerking. Ten aanzien van het periodiek herzien van DPIA's kan de gemeente nog stappen te zetten om op niveau 4 uit te komen.

Voor het toezicht op de Wpg geldt dat deze de beheersing van de getoetste onderdelen laat zien. De periodieke controle en uitkomsten van de interne audit laten zien dat de Wpg vereisten binnen de gemeente Veere worden nageleefd. Wanneer afwijkingen worden geconstateerd, wordt gecontroleerd waar de afwijking vandaan komt. Waar nodig worden extra maatregelen genomen om herhaling te voorkomen. Een algemene aanbeveling is om beleid en werkinstructies op te stellen voor de artikel 9 verwerkingen en de vereisten uit artikel 11 en artikel 13 Wpg. De gemeente heeft nu nog niet te maken met deze verwerkingen, maar verwerkt alleen politiegegevens volgens artikel 8 Wpg. De kans is groot dat in de toekomst wel verwerkingen anders dan artikel 8 gaan voorkomen. Door tijdig over te gaan tot het opstellen van deze documenten wordt geborgd dat de gemeente Veere goed voorbereid is op de andere verwerkingen.

Inhoudsopgave

1 Inleiding

1.1 Toezicht

Gemeente Veere heeft voor het interne toezicht op de Wet politiegegevens (Wpg) en voor de Algemene Verordening Gegevensbescherming (AVG) contactpersoon mevrouw mr. Ismay Elferink van adviesbureau L2P aangesteld als functionaris voor gegevensbescherming (FG). De FG werkt nauw samen met de Privacy Officer van gemeente Veere en brengt jaarlijks verslag uit over de werkzaamheden, bevindingen en aanbevelingen.

1.2 Privacyvolwassenheid

De beoordeling van het privacyvolwassenheidsniveau is gebaseerd op het referentiekader van de Privacy Baseline (versie 3.3) en het Privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Bij het bepalen van het privacy volwassenheidsniveau volgens de normen van het CIP, wordt uitgegaan van 5 niveaus. Deze schaalverdeling is gebaseerd op wereldwijde best practices en geeft zodoende een goed algemeen beeld van een organisatie en daarnaast biedt deze methode de mogelijkheid tot het benchmarken met andere organisaties. Artikel 5 lid 2 en artikel 24 lid 1 en 2 AVG verplichten een organisatie aantoonbaar te voldoen aan de voorwaarden van de AVG (de 'verantwoordingsplicht'). Dit betekent dat op basis van het onderstaande volwassenheidsmodel een verwerkingsverantwoordelijke uiteindelijk in ieder geval niveau 3 dient te behalen. Zo heeft de organisatie voldoende zekerheid over het naleven van de AVG en de UAVG en kan het dit aantoonbaar maken.

De 5 privacyvolwassenheidsniveaus luiden als volgt:

1. **Informeel**: de privacy werkzaamheden worden op verwerkingsniveau informeel uitgevoerd.
2. **Beheerst**: de privacy werkzaamheden worden beheerst uitgevoerd (herhaalbare processen).
3. **Vastgesteld**: de privacy werkzaamheden worden binnen de organisatie volgens een vastgestelde werkwijze uitgevoerd.
4. **Voorspelbaar**: de privacyprestaties worden gemeten, vergeleken met de branche en gebruikt voor een optimaal lerend vermogen.
5. **Geoptimaliseerd**: uitingen ten aanzien van de prestaties maken optimaal (en integraal) onderdeel uit van de bedrijfsstrategie en -uitingen.

1.3 NOREA normenkader Wpg

De beoordeling van de Wpg beheersmaatregelen volgt het normenkader van de NOREA. Hierbij wordt gebruik gemaakt van de Handreiking Privacy audit Wpg. Er wordt gecontroleerd op opzet, bestaan en werking van beheersmaatregelen.

2 Terugblik op 2024

In 2024 heeft de FG vijf toezichtacties uitgevoerd, waarvan twee op de AVG en drie toezichtacties op de Wpg. Hieronder licht de FG de inhoud van de toezichtacties toe en geeft zij een overzicht van de bevindingen en bijbehorende aanbevelingen.

2.1 Toezichtactie: Controle verwerkingsregister

Het bijhouden van een verwerkingsregister is conform artikel 30 AVG een wettelijke verplichting voor de gemeente Veere. De toezichthouder, de Autoriteit Persoonsgegevens, kan het verwerkingsregister bijvoorbeeld opvragen voor bijvoorbeeld controledoeleinden. Hiernaast maakt het register deel uit van de aantoonbaarheidsplicht die op verwerkingsverantwoordelijken rust.

De gemeente Veere heeft een verwerkingsregister waarin de doeleinden en rechtvaardigingsgronden van de verwerkingen zijn vastgelegd. Voor dit verwerkingsregister wordt de applicatie 'AVG Register' van Key2Control gebruikt. Het verwerkingsregister bevat alle verplichte onderdelen en is actueel en up to date. Het register wordt periodiek gecontroleerd en waar nodig herzien. Alle verwerkingen zijn gekoppeld aan verschillende interne processen van de gemeente Veere. Proceseigenaren blijven betrokken bij het juist invullen van het register, waardoor de kwaliteit van het register bewaakt wordt.

De gemeente Veere komt op dit onderdeel uit op privacy volwassenheidsniveau 4, 'Voorspelbaar', en er is sprake van een laag risico. De gemeente Veere voldoet hiermee aan de vereisten die de AVG haar stelt.

2.2 Toezichtactie: Uitvoering van DPIA's

Als de gemeente van plan is persoonsgegevens te verwerken waarbij waarschijnlijk een hoog risico voor betrokkenen speelt, is de gemeente verplicht om een DPIA uit te voeren. In een DPIA worden de privacyrisico's beoordeeld en volgt een beschrijving van de genomen maatregelen die de risico's kunnen mitigeren. Een DPIA moet voor advies aan de FG worden voorgelegd.

De gemeente Veere heeft een DPIA methodiek opgesteld welke is beoordeeld. De uitvoering van DPIA's en de bijbehorende methodiek voldoet aan de gestelde norm. Hoewel er niet heel veel DPIA's worden uitgevoerd, zijn de opgestelde werkinstructies passend voor de organisatie en medewerkers zijn goed op de hoogte van hun eigen rol bij de invulling van de (pre-)DPIA. De Privacy Officer wordt altijd betrokken bij het proces en kan waar nodig nog bijsturen. Er zijn nog stappen te zetten in de periodieke herziening van DPIA's.

De gemeente Veere komt op dit onderdeel uit op privacy volwassenheidsniveau 3, 'Vastgesteld', en er is sprake van een laag risico. De gemeente Veere voldoet hiermee aan de vereisten die de AVG haar stelt.

2.3 Toezichtactie Wpg: Doelbinding

Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.

De uitvoering van de Wpg norm doelbinding is beoordeeld en voldoet. Er zijn geen afwijkingen van de wettelijke vereisten te zien en de gemeente Veere heeft in beleid en werkinstructies voorzien. Door de ingebouwde extra controle op de processen-verbaal, nader genomen maatregelen en door de interne audit wordt geborgd dat de gemeente Veere voldoet aan de vereisten. Een aanbeveling is om beleid en werkinstructies op te stellen voor de artikel 9 verwerkingen en de vereisten uit artikel 11 en artikel 13 Wpg. De gemeente heeft nu nog niet te maken met deze verwerkingen, maar de kans is groot dat dit in de toekomst wel voorkomt. Dat is ook zo beschreven in het beleid. Door tijdig over te gaan tot het opstellen van deze documenten wordt geborgd dat de gemeente Veere goed voorbereid is op de andere verwerkingen.

2.4 Toezichtactie Wpg: Autorisaties van Boa's

De uitvoering van de Wpg norm autorisaties is beoordeeld en voldoet. Uit de beoordeling volgt dat de gemeente Veere intern een goede controle heeft opgezet om onrechtmatige toegang tot politiegegevens te voorkomen. Door de verschillende momenten van controle worden afwijkingen tijdig opgespoord. Wanneer afwijkingen voorkomen wordt gecontroleerd waar dit aan ligt. Bij bijvoorbeeld uitdiensttreding wordt gecontroleerd of de toegang tot het account op juiste manier geblokkeerd is. Zo wordt geborgd dat onrechtmatig inzien van politiegegevens niet voorkomt.

2.5 Toezichtactie Wpg: Noodzakelijkheid en rechtmatigheid

Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.

De gemeente Veere heeft inzichtelijk gemaakt aan welke vereisten zij dient de voldoen zodat de verwerking van politiegegevens noodzakelijk en rechtmatig zijn. Er is beleid en werkinstructies opgesteld ten aanzien van artikel 8 Wpg verwerkingen. Hierin is opgenomen waar boa's rekening mee moeten houden bij het verkrijgen en vastleggen van politiegegevens. Uit de beoordeling volgt dat de gemeente Veere in 2024 slechts drie afwijkingen had, waarbij meer gegevens zijn vastgelegd dan noodzakelijk. Dit betreft een foto waarop naast het gewenste voertuig ook een ander voertuig met kenteken zichtbaar is. Dit wordt meegenomen als aandachtspunt. Een tweede aandachtspunt is in lijn met de aanbeveling onder 2.3. Ook voor dit onderdeel geldt de aanbeveling om beleid en werkinstructies op te stellen voor verwerkingen anders dan die van artikel 8 Wpg. Zo is de gemeente Veere goed voorbereid op deze verwerkingen en wordt niet ad hoc gereageerd.

2.6 Toezichtactie Wpg: Onderscheid feiten en persoonlijk onderdeel

Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.

Uit de interne audit en steekproef komt naar voren dat de gemeente Veere op dit onderdeel voldoet aan de gestelde vereisten. Hierbij worden de boa's geholpen door de gebruikte applicatie, welke het niet mogelijk maakt om meer of subjectieve gegevens vast te leggen. Daarnaast heeft de gemeente Veere voorzien in een extra controle door de senior boa. Deze heeft de rol van controleur gekregen, waardoor het vier ogen principe wordt gehandhaafd. Deze maatregel kan eventuele afwijkingen ongedaan maken. Uit de interne audit komt naar voren dat de senior boa controleur is en ook alle rollen beheert. Dit geeft een risico. Een aanbeveling is om in de wijziging van toegangsrechten de logging actief te monitoren. Zo worden eventuele onrechtmatige wijzigingen actief opgespoord.

2.7 Adviezen

De FG is in 2024 meerdere keren om advies gevraagd door de Privacy Officer en medewerkers van de gemeente Veere. De gevraagde adviezen zijn gegeven over datalekken, de rol van de gemeente bij het Zorg en Veiligheidshuis, inning van gelden bij Oekraïners, het anonimiseren van ingekomen stukken voor de gemeenteraad, belastingsamenwerking en over verwerkersovereenkomsten en gegevensdeling met derde partijen.

2.8 DPIA's

De gemeente Veere heeft in 2024 één DPIA uitgevoerd. De FG heeft deze DPIA beoordeeld en van commentaar voorzien. De DPIA in kwestie is:

- DPIA Cameratoezicht parkeerplaats

2.9 Datalekken

In 2024 zijn veertien incidenten voorgekomen binnen de gemeente Veere. Hiervan is één datalek gemeld aan de Autoriteit Persoonsgegevens en drie datalekken zijn gemeld aan de betrokkenen.

2.10 Rechten van betrokkenen

In 2024 zijn geen inzageverzoeken binnengekomen bij de gemeente Veere.

3 Vooruitblik 2024

3.1 Overloop

In het vorige hoofdstuk van deze rapportage heeft de FG beschreven welke toezichtacties zijn uitgevoerd in 2024 en wat de belangrijkste bevindingen hierbij waren. In 2024 zijn niet alle geplande AVG toezichtacties uitgevoerd. Daarom zijn een aantal toezichtacties in 2025 nogmaals opgenomen om uit te voeren, vanwege het belang om ook deze onderwerpen te controleren en een volwassenheidsniveau vast te stellen.

3.2 Toezichtacties

In 2025 worden in ieder geval de volgende toezichtacties uitgevoerd. De FG zal zich daarbij richten op de volgende thema's:

Controle bewaar- en vernietigingsbeleid

Uitgangspunt is dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk. Van belang is dat persoonsgegevens binnen de gemeente periodiek worden gecontroleerd om te voorkomen dat langer wordt bewaard dan noodzakelijk is. De volgende criteria zijn hierbij van belang:

- Welke wettelijke kaders hanteert de gemeente met betrekking tot het bewaren van persoonsgegevens?
- Hoe heeft de gemeente het beleid ten aanzien van het bewaren en vernietigen van persoonsgegevens ingericht? Wordt het bijvoorbeeld genoemd in het privacybeleid en/of in de privacyverklaring en is het bewaar- en vernietigingsbeleid geïmplementeerd in de werkprocessen?
- Zijn er specifieke procedures ingericht om te borgen dat persoonsgegevens niet langer worden bewaard dan nodig en de persoonsgegevens na de bewaartermijn worden vernietigd? Welke functie/afdeling is hier verantwoordelijk voor?

Controle betrokkenheid Ondernemingsraad

De FG beoordeelt in welke mate gemeente Veere de Ondernemingsraad (OR) op de hoogte houdt en actief betrekt bij vraagstukken rondom de bescherming van persoonsgegevens van medewerkers. De volgende criteria zijn hierbij van belang:

- De gemeente zorgt voor tijdige en proactieve informatievoorziening richting de OR over privacy- en gegevensbeschermingsbeleid met betrekking tot medewerkers.
- De gemeente vraagt de OR om instemming wanneer er regelingen worden ingevoerd die invloed hebben op de bescherming van persoonsgegevens van medewerkers.

Selectielijst e-mailbewaring

De FG beoordeelt in hoeverre gemeente Veere e-mailcommunicatie bewaart in overeenstemming met de geldende selectielijst. De beoordeling is gebaseerd op de volgende criteria:

- De gemeente heeft een bewaarbeleid geïmplementeerd voor e-mails volgens de Selectielijst e-mailbewaring.
- De gemeente heeft dit beleid duidelijk gecommuniceerd binnen de organisatie.
- De gemeente verwijdert e-mails op aantoonbare wijze zodra de bewaartermijn is verstreken.

Gebruik voertuigvolgsystemen

De FG beoordeelt in hoeverre voertuigvolgsystemen van gemeente Veere voldoen aan de privacy wet- en regelgeving. Daarbij worden de volgende punten in acht genomen:

- De gemeente kan aantonen waar, wanneer en met welk doel voertuigvolgsystemen worden ingezet.
- De gemeente heeft een uitgebreide risicoanalyse (DPIA) uitgevoerd met alvorens over te gaan tot het gebruik van voertuigvolgsystemen.
- De gemeente informeert de betrokkenen op een duidelijke, eenduidige en toegankelijke manier over het gebruik van deze systemen.

Beoordeling doelbinding Wpg

Op grond van de Wpg is de gemeente Veere verplicht om minimaal jaarlijks de doelbinding van de verwerkte politiegegevens te controleren. Politiegegevens mogen alleen worden verwerkt als dat nodig is voor de in de wet genoemde doeleinden. De FG zal beoordelen in hoeverre de gemeente waarborgt dat politiegegevens alleen worden verzameld en (verder) verwerkt worden voor gerechtvaardigde doeleinden. De volgende criteria zijn hierbij van belang:

- De gemeente heeft inzicht in de specifieke wettelijke kaders waaraan zij moet voldoen met betrekking tot doelbinding
- De gemeente waarborgt dat het principe van doelbinding wordt nageleefd binnen de gemeente

Hiertoe zal de FG door middel van een steekproef een aantal processen-verbaal opvragen en deze controleren op de doelbinding.

L2P
Stadsplateau 7
3521 AZ Utrecht

+31 (0) 26 848 3118
info@l2p.nl