GEMEENTE VEERE

Privacybeleid gemeente Veere

Domburg, mei 2018
Versie 1.0
18B.02170

Inhoud

Samenvatting

Op 25 mei 2018 vervangt de Algemene Verordening Gegevensbescherming de Wet bescherming persoonsgegevens. Alhoewel dit t.a.v. de bescherming van persoonsgegevens geen aardverschuiving betekent is het wel noodzakelijk om een aantal zaken goed te regelen en te organiseren. Het vaststellen van gemeentelijk Privacybeleid is één van die zaken.
In het gemeentelijk Privacybeleid legt het college van burgemeester en wethouders vast wie verantwoordelijk is voor de bescherming van persoonsgegevens, op welke manier de verantwoordelijke er voor zorgt dat persoonsgegevens worden verwerkt volgens de wet- en regelgeving en hoe de verantwoordelijke aantoont dat dit ook werkelijk zo gebeurt.

Verantwoordelijke

Het college van burgemeester en wethouders en de burgemeester afzonderlijk voor zijn speciale wettelijke taken, zijn formeel verantwoordelijk voor de verwerking van persoonsgegevens.
In het Privacybeleid is vastgelegd dat ten aanzien van die verantwoordelijkheid de bescherming van persoonsgegevens het uitgangspunt is bij al ons handelen en bij al onze dienstverlening. Privacy first!
De toegenomen aandacht voor privacy en de risico's die zijn verbonden aan het niet naleven van de privacyregelgeving, maken het noodzakelijk dat er een portefeuillehouder privacy wordt aangewezen. Deze bestuurder is het aanspreekpunt voor de organisatie, de politiek, burgers en media over alle onderwerpen die te maken hebben met het verwerken van persoonsgegevens.

Voldoen aan wet- en regelgeving

De AVG verplicht de gemeente om een aantal materiële zaken beschikbaar te hebben of te organiseren. Zo moet er bijvoorbeeld een verwerkingenregister ingericht zijn; moeten er verwerkersovereenkomsten afgesloten zijn; moet er een procedure voor datalekken beschikbaar en bekend zijn; moeten betrokkenen hun rechten kunnen uitoefenen (bijvoorbeeld het recht op inzage); moet er een DPIA (privacyrisico analyse) uitgevoerd kunnen worden. Daarnaast zijn er regels nodig die ervoor zorgen dat bescherming van persoonsgegevens het uitgangspunt is bij al ons handelen en bij al onze dienstverlening. Dat betekent bijvoorbeeld dat bij het actief en passief openbaar maken van informatie geen persoonsgegevens worden verstrekt, tenzij het evident is dat het belang van openbaarmaking zwaarder weegt dan het belang van de eerbiediging van de persoonlijke levenssfeer.

Verantwoording

Zeggen wat je doet is niet voldoende, je moet ook aantoonbaar doen wat je zegt. Ook dat is nieuw in de AVG. De bescherming van persoonsgegevens moet blijken uit documenten, rapportages, audits, DPIA's, maatregelen, privacyverklaring op de website, etc. De Functionaris Gegevensbescherming (FG) heeft hierin een belangrijke rol. Deze onafhankelijke functionaris houdt toezicht op de naleving van de privacyregelgeving en rapporteert en adviseert hierover aan de verantwoordelijke. De AVG en het Privacybeleid zijn hiervoor de norm.
De eerste versie van het Privacybeleid is nu vastgesteld. Door nieuwe inzichten, veranderende omstandigheden en jurisprudentie zullen in de toekomst ongetwijfeld meerdere versies volgen.

1. Inleiding

Privacy staat erg in de belangstelling. Voor sommigen is dat warme belangstelling, voor anderen is dat meer lastige noodzakelijke belangstelling. Ook binnen de organisatie van de gemeente Veere zal die belangstelling verschillend zijn. Dat neemt niet weg dat we ervoor moeten zorgen dat privacy in de gemeente Veere goed geregeld is. De juiste aandacht voor privacy zorgt voor goede en integere dienstverlening.
De burger heeft er recht op dat we zorgvuldig met persoonsgegevens omgaan, het vertrouwen daarin mogen we niet beschamen!

Privacy is een ruim begrip en de gemeente is niet verantwoordelijk voor de volle betekenis van dit begrip. Privacy wordt ook wel omschreven als het recht om met rust gelaten te worden. Bij die "rust" kunnen vele invullingen bedacht worden. Het kan bijvoorbeeld gaan om rust in de sfeer van relaties, lichaam/gezondheid, territorium, communicatie en informatie. In deze notitie heeft privacy betrekking op de informationele privacy, en in dat verband is het beter om te spreken over bescherming van persoonsgegevens.

Het recht op privacy is verankerd in de Grondwet en het Europees Verdrag tot bescherming van de Rechten van de Mens:

Grondwet artikel 10
Lid 1: Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
Lid 2: De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

EVRM artikel 8
Lid 1: Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
Lid 2: Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien …..

Alleen een wet mag het recht op eerbiediging van de persoonlijke levenssfeer doorbreken. Op dit moment is het de Wet bescherming persoonsgegevens (Wbp) die het mogelijk maakt om voor bepaalde doeleinden persoonsgegevens te verwerken. Per 25 mei 2018 wordt deze wet vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG). Vanaf dat moment is de bescherming van persoonsgegevens in alle landen van de EU op dezelfde manier geregeld.

Regelgeving omtrent bescherming van persoonsgegevens is dus zeker niet nieuw. Vanaf 1 juli 1989 gold de Wet Persoonsregistraties. Deze wet is op 1 september 2001 vervangen door de Wet bescherming persoonsgegevens. De Wbp bestaat dus al 16 jaar. De hoofdlijnen van de Wbp zijn ook weer opgenomen in de AVG. In die zin is er niet zo heel veel nieuws onder de privacy-zon. Nieuw is wel dat er meer aandacht is voor governance, compliance en accountability. In gewoon Nederlands: de organisaties die persoonsgegevens verwerken moeten er voor zorgen dat duidelijk is wie er verantwoordelijk voor is; dat die verantwoordelijke er voor zorgt dat persoonsgegevens worden verwerkt volgens de wet- en regelgeving; en dat de verantwoordelijke steeds kan aantonen dat dit ook werkelijk zo gebeurt en dat waar nodig hiervoor passende maatregelen worden getroffen.

Nieuw is ook dat de toezichthoudende autoriteit hoge boetes kan uitdelen, tot maximaal € 20 miljoen. Voor de gemeente Veere is dat niet de reden om de goede aandacht aan Privacy te geven. Bescherming van persoonsgegevens doen we niet omdat het moet

maar omdat het kan! Een goede basis om dit waar te maken is het vaststellen van de uitgangspunten die we hiervoor in de gemeente Veere hanteren.
De Wbp en de AVG zijn voldoende duidelijk over de vraag of een organisatie persoonsgegevens mag verwerken, en als dat mag welke verplichtingen dat dan met zich meebrengt en welke rechten de betrokkenen in dat geval hebben.
Hoe dat in de gemeente Veere wordt toegepast is beschreven in het Privacybeleid gemeente Veere. Hiermee bereiken we de volgende doelen:

- het geeft de organisatie houvast voor het op een goede manier verwerken van persoonsgegevens
- het verschaft de betrokkenen inzicht en transparantie in de verwerking van persoonsgegevens, en geeft waarborgen voor de rechten die betrokkenen daarbij hebben
- het geeft invulling aan governance, compliance en accountability t.a.v. de verwerking van persoonsgegevens, zodat verantwoording kan worden afgelegd aan de toezichthouder.

Domburg, mei 2018

2. Visie

Persoonsgegevens zijn de olie en soms zelfs de brandstof voor de motor van de maatschappij. Zonder persoonsgegevens geen identiteit, en zonder identiteit kan de maatschappij niet functioneren.
Omdat persoonsgegevens zo belangrijk zijn, wordt er ook veel waarde gehecht aan de bescherming ervan. De overheid heeft daarbij een grote en bijzondere verantwoordelijkheid. Omdat in de meeste gevallen de persoonsgegevens worden verwerkt in verband met de uitvoering van een wettelijke verplichting of een algemene (publieke) taak, hebben de burgers geen keus in het wel of niet verstrekken van hun persoonsgegevens. Burgers moeten er dus op kunnen vertrouwen dat hun persoonsgegevens in goede en veilige handen zijn bij de gemeente Veere. Die verantwoordelijkheid rust op iedereen die werkzaam is binnen of onder verantwoordelijkheid van de Veerse organisatie.

Om die reden geldt voor het bestuur, management en medewerkers dat de bescherming van de persoonsgegevens uitgangspunt is bij al ons handelen en bij al onze dienstverlening.
De geldende privacywetgeving in combinatie met het Privacybeleid gemeente Veere is hiervoor het kader en de norm. Daarbij geldt dat in situaties waarbij het organisatiebelang niet parallel loopt met het belang van de bescherming van persoonsgegevens, gezocht wordt naar een evenwichtige oplossing. Dat betekent dat voor het behalen van het organisatiedoel er maatregelen zijn getroffen die de bescherming van de persoonsgegevens voldoende waarborgen.

3. Governance

In dit hoofdstuk beschrijven we wie verantwoordelijk is voor de taken en bevoegdheden t.a.v. de bescherming van persoonsgegevens. Naast de formele verantwoordelijkheid betreft dit ook de verantwoordelijkheid voor de praktische uitvoering in de dagelijkse praktijk. En tot slot is er de verantwoordelijkheid voor het toezicht op de naleving van de privacyregelgeving.

3.1 Verwerkingsverantwoordelijke

Volgens de AVG is de verwerkingsverantwoordelijke de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
In de praktijk is het college van burgemeester en wethouders de verantwoordelijke voor alle verwerkingen van persoonsgegevens. Uitzondering hierop zijn de verwerkingen die direct voortvloeien uit een wettelijk taak die uitsluitend aan de burgemeester is opgedragen, in dat geval is de burgemeester de verwerkingsverantwoordelijke.

Formeel gezien zou ook de gemeenteraad verwerkingsverantwoordelijke kunnen zijn. Maar de memorie van toelichting bij de Wbp gaat ervan uit dat alleen het college van burgemeester en wethouders en de burgemeester verwerkingsverantwoordelijke zijn. Verantwoordelijk is het bestuursorgaan onder wiens bevoegdheid de operationele gegevensverwerking plaatsvindt.
In het normaal maatschappelijk verkeer worden deze bestuursorganen ook geacht verantwoordelijk te zijn. Betrokkenen zullen de verwachting hebben daar hun rechten te kunnen uitoefenen.
Onder de AVG verandert dit uitgangspunt niet.

3.2 Portefeuillehouder Privacy

Uit de beschreven visie blijkt dat de bescherming van persoonsgegevens uitgangspunt is voor de gehele organisatie. Dat brengt met zich mee dat de verantwoordelijkheid hiervoor niet versnipperd kan zijn, dus niet verdeeld over verschillende clusters, managers en bestuurders.
Om de bescherming van de persoonsgegevens organisatiebreed te waarborgen is een centrale verantwoordelijkheid en aansturing noodzakelijk.
De bestuurlijke en politieke verantwoordelijkheid wordt ondergebracht bij één portefeuillehouder. Bij de start van iedere nieuwe collegeperiode wordt de portefeuillehouder Privacy aangewezen voor de duur van de collegeperiode.
De portefeuillehouder Privacy is bestuurlijk verantwoordelijk en het aanspreekpunt voor het onderwerp Privacy. Het onderwerp Privacy wordt periodiek in het stafoverleg besproken, en de portefeuillehouder voert periodiek gesprekken met de FG over dit onderwerp.

3.3 Functionaris Gegevensbescherming

Voor overheidsorganen is het aanstellen van een Functionaris Gegevensbescherming (FG) verplicht op grond van de AVG.
De FG is een professional en bovengemiddeld deskundige op het gebied van gegevensbescherming. De FG heeft:

- kennis van nationale en Europese privacywet- en regelgeving voor gegevensbescherming;
- begrip van de gegevensverwerkingen die gemeentelijke overheid uitvoert;
- begrip van IT en informatiebeveiliging;
- kennis van de gemeentelijke organisatie;
- vaardigheden om binnen de organisatie het privacybewustzijn op een goed niveau te brengen en te houden.

De FG functioneert onafhankelijk en kan voor de uitvoering van zijn taken niet ontslagen of gestraft worden. Deze status is vergelijkbaar met een lid van de Ondernemingsraad.

Omdat de FG voor de gemeente een nieuwe functionaris is, en de invulling van die rol en taken in de praktijk nog vorm moet krijgen, vullen we deze functie voor de korte termijn in met een externe deskundige. Op basis van prijs- en informatieopvraag wordt een geschikte FG aangesteld voor de duur van één jaar. Uitgangspunt is een urenbesteding van ongeveer 60 uur per jaar.
Jaarlijks wordt deze invulling geëvalueerd en overwogen of deze invulling wordt gecontinueerd. Het is dan ook mogelijk om te kiezen voor een FG met een vast dienstverband, eventueel in samenwerking met andere gemeenten.

In de AVG zijn de volgende taken van de AVG benoemd:

a. Informeren en adviseren over privacywet en –regelgeving
Vanuit zijn deskundigheid en kennis van de gemeentelijke organisatie geeft de FG gevraagd en ongevraagd informatie en advies over taken en onderwerpen waarbij persoonsgegevens worden verwerkt. De informatie en het advies is zwaarwegend en gericht op een juiste toepassing van de privacywet en-regelgeving.

b. Toezien op de naleving van de privacywet en –regelgeving, inclusief het gemeentelijk privacybeleid
De taak toezicht heeft een nauwe relatie met de taak informatie en advies. De FG controleert binnen de gehele organisatie of de verwerking van persoonsgegevens gebeurt overeenkomstig de privacywet en –regelgeving en het gemeentelijk Privacybeleid. Over zaken die niet in orde zijn informeert en adviseert de FG de verwerkingsverantwoordelijke.

c. Adviseren over en toezien op de uitvoering van DPIA's
De AVG schrijft voor dat in bepaalde situaties een DPIA wordt uitgevoerd. De FG ziet er op toe dat de DPIA's worden uitgevoerd en geeft advies over de uitvoering en de uitkomst van de DPIA.

d. Ombudsfunctie
Betrokkenen kunnen contact opnemen met de FG voor vragen, verzoeken, klachten en andere zaken die verband houden met het verwerken van hun persoonsgegevens.

e. Aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens (AP)
De FG is geen verlengstuk van de AP maar vervult een zelfstandige functie. De FG en de AP hebben hetzelfde belang, voldoen aan de privacywet en –regelgeving, maar kunnen daarin wel hun eigen inzicht hebben. Door zijn deskundigheid is de FG in staat om in het contact met de AP te motiveren en te overtuigen. Daarnaast is de FG ook een partner voor de AP om ervoor te zorgen dat het toezicht en het advies bijdragen een juiste toepassing van de privacywet en –regelgeving.
Zo nodig zal de FG ook onrechtmatigheden melden bij de AP als deze na zijn advies niet of niet voldoende worden opgelost.

Voor zijn informatie-, advies en toezichttaak heeft de FG periodiek overleg (minimaal 1x per kwartaal) met de portefeuillehouder Privacy. Op basis van dit overleg doet de FG daarna verslag aan de verwerkingsverantwoordelijke.

De FG wordt praktisch ondersteund door de Privacy Officer (PO). In veel gevallen is de PO ook het eerste aanspreekpunt en fungeert als oog en oor in de organisatie. De PO informeert de FG direct over alle zaken die horen tot de taken en verantwoordelijkheden van de FG. Daarnaast laat de FG zich ook persoonlijk informeren door periodiek te overleggen met het MT en het bezoeken van afdelingsoverleggen.
De FG en de PO zorgen samen voor een permanent programma om het privacybewustzijn op een goed niveau te brengen en te houden.

3.4 Privacy Officer

De FG heeft een wettelijke toezichthoudende taak. Om die reden kan en mag hij zich niet met de dagelijkse uitvoerende privacywerkzaamheden bezighouden. Dit is gescheiden. Met de dagelijkse werkzaamheden is de Privacy Officer (PO) belast. De functie PO is geen formele functie maar de werknaam voor de functionaris die zich bezighoudt met de praktische en uitvoerende privacywerkzaamheden. Het college van B&W legt wel in een besluit vast wie de rol van PO vervult. Daarmee is het voor de organisatie duidelijk wie het eerstelijns aanspreekpunt is voor alle privacyvraagstukken.

De PO heeft de volgende taken:

a. Aanspreekpunt voor en ondersteuning van de FG;
b. Verstrekken van informatie en advies over de dagelijkse praktijk aan de FG;
c. Samenwerken met de FG om de adviezen van de FG toe te passen en/of uit te voeren;
d. Initiëren en mede uitvoeren van DPIA's;
e. Contactpersoon voor betrokkenen voor vragen, verzoeken, klachten en andere zaken die verband houden met de verwerking van hun persoonsgegevens;
f. Eerstelijns vraagbaak voor de organisatie voor alle privacyvraagstukken;
g. Gevraagd en ongevraagd de organisatie adviseren over de juiste toepassing van de privacywet en –regelgeving;
h. Beoordelen van datalekken en deze zo nodig melden bij de AP en de betrokkene;
i. Bijhouden van het verwerkingenregister;
j. Het opstellen en afsluiten van verwerkersovereenkomsten.

3.5 Rol Managementteam

Het Managementteam (MT) is verantwoordelijk voor de directe aansturing van de medewerkers. De MT-leden, de afdelingshoofden en de gemeentesecretaris, geven dagelijks leiding aan de afdelingen en zien in die rol toe op de naleving van de privacywet en –regelgeving. Het niet-naleven wordt direct gecorrigeerd en het onderwerp privacy is een vast onderdeel in het resultaatgesprek. Periodiek, maar minimaal 1x per jaar wordt dit onderwerp besproken tijdens het afdelingsoverleg. Bij voorkeur gebeurt dit in aanwezigheid van de FG of de PO.
Ook in de MT-vergadering staat het onderwerp privacy periodiek op de agenda. Minimaal 1x per kwartaal wordt dit onderwerp besproken in aanwezigheid van de FG.

3.6 Rol werkgroep Informatiebeveiliging

De werkgroep Informatiebeveiliging (werkgroep IB) bestaat uit de gemeentesecretaris, de beveiligingsfunctionaris, de PO en de adviseur informatiebeleid.
De belangrijkste taak van de werkgroep IB is het opstellen, (laten) uitvoeren en verantwoorden van het jaarplan informatiebeveiliging. In dat jaarplan worden ook de beveiligingsaspecten rondom het verwerken van persoonsgegevens opgenomen.
De werkgroep IB adviseert het MT over te nemen maatregelen die het verwerken van persoonsgegevens veiliger maken.

De werkgroep IB is ook onderdeel van het Computer Security Incident Response team (CSIR-team). Het CSIR-team komt in actie als zich beveiligingsincidenten voordoen. In een urgente situatie onderneemt het CSIR-team direct actie om de gevolgen van een beveiligingsincident te voorkomen of te bestrijden. In gevallen die niet urgent zijn adviseert het CSIR-team het college van B&W of het MT om de nodige acties te ondernemen.

Als er sprake is van een beveiligingsincident waarbij persoonsgegevens zijn betrokken dan beoordeelt het CSIR-team de gevolgen van het datalek en bepaalt of het datalek gemeld moet worden bij de AP en de betrokkene.

4. Compliance

Dit hoofdstuk beschrijft op welke manier we uitvoering geven aan de materiële bepalingen uit de AVG. Het naleven en uitvoeren van deze bepalingen is controleerbaar en toont aan dat de bescherming van persoonsgegevens compliant is met de AVG.

4.1 Begrippen

Een aantal begrippen uit de AVG wordt ook in dit document gebruikt. Voor de duidelijkheid over de betekenis van deze begrippen worden deze in dit onderdeel toegelicht. Het is niet de letterlijke tekst zoals deze is opgenomen in artikel 4 en 9 van de AVG.

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Ieder gegeven dat herleidbaar is naar een natuurlijke persoon.

Bijzonder persoonsgegeven: persoonsgegeven waaruit ras of etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuiging of het lidmaatschap van een vakbond blijken. Deze gegevens mogen slechts onder bepaalde voorwaarden worden verwerkt. Dat geldt ook voor strafrechtelijke gegevens.

Betrokkene: de natuurlijke persoon op wie de persoonsgegevens betrekking hebben. Als de betrokkene minderjarig is dan is voor het uitoefenen van zijn rechten toestemming nodig van

Verwerking: alle bewerkingen die verricht worden met betrekking tot persoonsgegevens, zoals verzamelen, registreren, raadplegen, doorgeven, verspreiden, vernietigen, etc. Een samenhangend geheel aan bewerkingen vormt een bewerking, maar ook de afzonderlijke delen zijn verwerkingen die moeten voldoen aan de AVG.

Verwerkingsverantwoordelijke:
Het orgaan dat het doel van en de middelen voor de verwerking vaststelt. Wie bepaalt de functionele en operationele activiteiten? Voor de gemeente Veere is dat het college van burgemeester en wethouders en voor een aantal verwerkingen de burgemeester omdat deze verband houden met speciaal aan hem opgedragen taken.

Verwerker:
Een organisatie die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke. Bijvoorbeeld een ICT-bedrijf dat een cloud-dienst levert en persoonsgegevens opslaat voor de gemeente Veere.

4.2 Verwerkingenregister

De AVG schrift voor dat de verwerkingsverantwoordelijke een register bijhoudt van alle verwerkingsactiviteiten. Gelet op de betekenis van het begrip verwerking is dit in de praktijk niet uitvoerbaar. Voor het verwerkingenregister worden de verwerkingsactiviteiten die met elkaar één verwerkingsdoel dienen als één verwerking geregistreerd. Het verwerkingsdoel bepaalt dus de registratie in het verwerkingenregister. Bijvoorbeeld het verwerkingsdoel Omgevingsvergunningen bestaat uit verschillende verwerkingsactiviteiten. Deze activiteiten worden in het verwerkingenregister bij de verwerking Omgevingsvergunningen beschreven.

Voor het verwerkingenregister wordt gebruik gemaakt van de applicatie van Key2Control. In deze applicatie worden per verwerking de volgende verplichte gegevens geregistreerd:

a. naam en omschrijving van de verwerking
b. de verwerkingsverantwoordelijke
c. de grondslag voor de verwerking
d. het doel van de verwerking
e. categorieën van persoonsgegevens
f. categorieën van betrokkenen
g. categorieën van ontvangers van persoonsgegevens (waaronder verwerkers)
h. de bewaartermijn
i. informatie over doorgifte van informatie aan derde landen
j. de getroffen beveiligingsmaatregelen

Daarnaast worden in de applicatie aanvullende gegevens opgenomen die de informerende functie van het verwerkingenregister vergroten. Een beschrijving van deze aanvullende gegevens is opgenomen in bijlage 1 "Handleiding verwerkingsregister Key2Control".
In verband met het uitoefenen van de rechten van betrokkenen wordt in ieder geval als aanvullend gegeven "de wijze van informeren van de betrokkene" in het register opgenomen.

4.3 Verwerkersovereenkomst

Wanneer aan een organisatie of bedrijf dat of die niet onder direct gezag staat van de gemeente Veere, een opdracht verstrekt waarbij namens de gemeente persoonsgegevens worden verwerkt, is er sprake van een verwerker. In dat geval moet er een verwerkersovereenkomst afgesloten worden.
Het doel van de verwerkersovereenkomst is om te waarborgen dat de verwerker voldoende en passende maatregelen neemt en toepast voor de bescherming van de persoonsgegevens.

De gemeente als verwerkingsverantwoordelijke biedt hiervoor het model aan, zoals opgenomen in bijlage 2, aan de verwerker. Dit model is gebaseerd op het model van de Informatiebeveiligingsdienst voor gemeenten (IBD). Relevante wijzigingen in het IBD-model worden overgenomen in het gemeentelijk model.

4.4 Data Protection Impact Assessment (DPIA)

In de Nederlandse vertaling van de AVG wordt voor de DPIA de term gegevensbeschermingseffectbeoordeling gebruikt. Uit deze term valt op te maken dat het de bedoeling is om het effect op de bescherming van persoonsgegevens te beoordelen bij het verwerken van persoonsgegevens. Uit die beoordeling blijken de privacyrisico's en op basis daarvan kunnen passende maatregelen worden genomen, of wordt besloten om de verwerking van persoonsgegevens niet uit te voeren.

De AVG schrijft voor om een DPIA uit te voeren bij nieuwe verwerkingen waarbij sprake is van een hoog risico voor de bescherming van persoonsgegevens. Maar ook voor bestaande verwerkingen met een hoog risico voor de bescherming van persoonsgegevens is een DPIA verplicht.
De AP stelt een lijst op met verwerkingen waarvoor een DPIA verplicht is en een lijst met verwerkingen waarvoor een DPIA niet verplicht is.

Voor de bestaande verwerkingen in de gemeente Veere waarin bijzondere persoonsgegevens worden verwerkt wordt zo spoedig mogelijk maar in ieder geval binnen een jaar na de inwerkingtreding van de AVG een DPIA uitgevoerd.
Verder wordt een DPIA uitgevoerd voor de verwerkingen waarvoor dit door de FG wordt geadviseerd.

Voor het uitvoeren van een DPIA wordt het model gebruikt zoals opgenomen in bijlage 3.
Als de DPIA maatregelen oplevert om de bescherming van persoonsgegevens te waarborgen dan worden deze maatregelen uitgevoerd en nageleefd. Periodiek maar minimaal eenmaal per jaar wordt de uitvoering en de naleving getoetst door of namens de FG.

4.5 Privacy by design en Privacy by default

Privacy by design houdt in dat al bij het ontwerpen van producten en diensten rekening wordt gehouden met de bescherming van persoonsgegevens. Dit lijkt veel op de DPIA, maar een DPIA wordt alleen uitgevoerd als er sprake is van hoog risico. Privacy by design wordt toegepast op alle nieuwe verwerkingen. Voor de start van de verwerking wordt nagedacht over alle aspecten die betrekking hebben op de bescherming van persoonsgegevens, zoals de juiste grondslag, de noodzaak om persoonsgegevens te gebruiken, het informeren van de betrokkenen, de bewaartermijn, etc. Pas als alles in orde is wordt de verwerking gestart.
Het verantwoordelijk afdelingshoofd, de adviseur informatiebeleid, de systeembeheerder en de inkoopadviseur hebben hiervoor een signalerende taak.

Privacy by default houdt in dat bij het verzamelen van persoonsgegevens niet meer gegevens worden gevraagd dan noodzakelijk voor het doel van de verwerking.
Ook wordt bij een keuzemogelijkheid, een keuze niet vooraf ingevuld. Op de website wordt bijvoorbeeld het vakje 'Ja, ik wil de nieuwsbrief ontvangen' niet vooraf aangevinkt.
Privacy by default is met name van belang bij diensten op het gebied van social media.

4.6 Toestemming

Toestemming van de betrokkene is één van de 6 grondslagen in de AVG voor het verwerken van persoonsgegevens. Omdat de gemeente bijna uitsluitend persoonsgegevens verwerkt op basis van een wettelijke verplichting of de uitvoering van een taak van algemeen belang of openbaar gezag, is de grondslag toestemming vrijwel nooit aan de orde.
Toestemming kan aan de orde zijn in het kader van zorg- en hulpverlening waarbij de betrokkenen zelf geen verzoek doet maar professionals toch een noodzaak voor zorg of hulp noodzakelijk achten. In een dergelijk geval is toestemming nodig van de betrokkene.
Voor het verwerken van persoonsgegevens op basis van toestemming wordt terughoudendheid betracht. Voor een dergelijke verwerking wordt vooraf advies gevraagd aan de FG.

Als er sprake is van toestemming dan dient deze toestemming aan de volgende voorwaarden te voldoen:

a. *vrij*; vrij betekent dat de betrokkene ook de keus moet hebben om zijn toestemming te weigeren, zonder dat hier mogelijk negatieve gevolgen aan verbonden zijn. Als er sprake is van een afhankelijkheidssituatie (zoals tussen overheid en burger en tussen werkgever en werknemer) is er in de regel geen sprake van een vrije keuze, en kan toestemming niet dienen als grondslag voor de verwerking.

b. *specifiek en geïnformeerd*; het moet voor de betrokkene helemaal duidelijk zijn waarvoor hij toestemming geeft. Dit betekent dat goed uitgelegd moet worden voor welk doel de persoonsgegevens verwerkt worden. Dat doel moet specifiek zijn, als er sprake is van meerdere doelen dan moeten deze apart uitgelegd worden.
c. *ondubbelzinnig*; de toestemming moet ondubbelzinnig zijn. Uit een actieve handeling moet het 100% duidelijk zijn dat de betrokkene zijn toestemming heeft gegevens. Dat kan door een handtekening, een zelf geplaatst vinkje op een website, o.i.d. Voor het verwerken van bijzondere persoonsgegevens moet uit de verklaring blijken dat de toestemming geldt voor de verwerking van de bijzondere persoonsgegevens.

4.7 Rechten van betrokkenen

Transparantie is een belangrijk uitgangspunt in de AVG. Iedere betrokkene moet (kunnen) weten wie welke persoonsgegevens over hem verwerkt en met welk doel dat gebeurt. Om die transparantie te waarborgen zijn in de AVG een aantal rechten toegekend aan de betrokkene (artikel 13 t/m 22 AVG). Het is van belang dat het voor de betrokkene duidelijk is dat hij deze rechten heeft en op welke manier hij er gebruik van kan maken.
De communicatie met de betrokkene moet beknopt, open, begrijpelijk en gemakkelijk toegankelijk zijn. Duidelijke en eenvoudige taal.

4.7.1 HET RECHT OM GEÏNFORMEERD TE WORDEN

Eigenlijk is dit geen recht van de betrokkene maar een verplichting van de verwerkingsverantwoordelijke.
Op het moment dat de persoonsgegevens in een verwerking worden opgenomen moet de betrokkene hierover geïnformeerd worden. Daarbij zijn twee situaties te onderscheiden.

4.7.1.1 DE PERSOONSGEGEVENS WORDEN BIJ DE BETROKKENE ZELF VERZAMELD.

In deze situatie moet de betrokkene op het moment van verzamelen geïnformeerd worden. Deze informatie moet het volgende inhouden:

a. informatie over de verwerkingsverantwoordelijke, het college of de burgemeester
b. contactgegevens van de FG
c. het doel en de rechtsgrond voor de verwerking
d. als de rechtsgrond een gerechtvaardigd belang is, het betreffende belang
e. indien van toepassing, de categorieën ontvangers van de persoonsgegevens
f. indien van toepassing, de doorgifte van de persoonsgegevens naar niet-EU landen, met daarbij de geboden waarborgen
g. de bewaartermijn van de persoonsgegevens
h. de rechten van de betrokkene (inzage, rectificatie, verwijdering, beperking, overdraagbaarheid, bezwaar, profilering)
i. het recht om een verleende toestemming in te trekken
j. de mogelijkheid om een klacht in te dienen
k. indien van toepassing, dat er sprake is van automatische besluitvorming op basis van profilering (zonder menselijke tussenkomst).
l. of de betrokkene een wettelijke of contractuele verplichting heeft om de gegevens te verstrekken, en wat de mogelijke gevolgen zijn als hij de gegevens niet verstrekt

De betrokkene wordt op één van de volgende manieren geïnformeerd:

i. Als de persoonsgegevens worden verkregen via een gemeentelijk aanvraagformulier, dan wordt op het aanvraagformulier in beknopte woorden vermeld voor welk doel de persoonsgegevens worden verwerkt en dat de

gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacystatement en het privacybeleid op de website van de gemeente Veere.

ii. Als de persoonsgegevens worden verkregen via een brief, e-mail of ander (digitaal) geschrift, dan wordt in de ontvangstbevestiging in beknopte woorden vermeld voor welk doel de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacystatement en het privacybeleid op de website van de gemeente Veere.

iii. Als de persoonsgegevens telefonisch worden verkregen dan wordt na afloop van het telefoongesprek een (ontvangst) bevestiging gestuurd met daarin in beknopte woorden vermeld voor welk doel de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacystatement en het privacybeleid op de website van de gemeente Veere.

iv. Als de persoonsgegevens telefonisch worden verkregen en er wordt na afloop van het telefoongesprek geen (ontvangst) bevestiging gestuurd, dan wordt in het telefoongesprek in beknopte woorden aangegeven dat de persoonsgegevens worden verwerkt met een verwijzing naar de gemeentelijke website voor het privacystatement en het privacybeleid. Deze boodschap kan ook voor of na het telefoongesprek op automatische wijze worden gegeven.

In bijlage 4 zijn een aantal voorbeelden opgenomen van de beknopte woorden die gebruikt kunnen worden voor het informeren van de betrokkenen.
In het verwerkingenregister wordt opgenomen op welke manier de betrokkene wordt geïnformeerd.

4.7.1.2 De persoonsgegevens zijn niet van de betrokkene verkregen.

In deze situatie moet de betrokkene binnen een redelijke termijn na de verkrijging van de persoonsgegevens geïnformeerd worden. In ieder geval uiterlijk binnen één maand. Dat kan het moment zijn van het eerste contact met de betrokkene (brief, e-mail, telefoon, etc.). Deze informatie moet het volgende inhouden:

a. de informatie zoals omschreven in 1.1 a. t/m k.
b. de betrokken categorieën van persoonsgegevens
c. de bron waar de gegevens vandaan komen en indien van toepassing, of de gegevens afkomstig zijn van openbare bronnen.

De betrokkene wordt op één van de volgende manieren geïnformeerd:

i. Als de persoonsgegevens worden gebruikt voor communicatie met de betrokkene, dan wordt in de brief, e-mail, telefoongesprek, etc., in beknopte woorden vermeld voor welk doel de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacystatement en het privacybeleid op de website van de gemeente Veere.

ii. Als de persoonsgegevens niet worden gebruikt voor communicatie met de betrokkene, dan wordt de betrokkene schriftelijk (brief of e-mail) en in beknopte woorden geïnformeerd over het doel waarvoor de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacystatement en het privacybeleid op de website van de gemeente Veere.

In bijlage 4 zijn een aantal voorbeelden opgenomen van de beknopte woorden die gebruikt kunnen worden voor het informeren van de betrokkenen.
In het verwerkingenregister wordt opgenomen op welke manier de betrokkene wordt geïnformeerd.

4.7.1.3 Uitzondering op de informatieplicht

Op grond van de AVG kan de informatie achterwege blijven als de betrokkene al over de informatie beschikt. Onder de Wbp gold geen informatieplicht voor de feiten die de betrokkene reeds kent of zou moeten kennen. De uitleg daarbij was dat de betrokkene

daarbij ook een zekere onderzoeksplicht heeft op basis van wat in het maatschappelijk verkeer redelijkerwijs van hem mag worden verwacht. Verder kan ook uit de gedragingen van de betrokkene worden afgeleid dat hij op de hoogte is.
In alle gevallen moet het voldoende duidelijk zijn dat de betrokkene op de hoogte is, alleen veronderstellen dat de betrokkene op de hoogte is is niet voldoende. Als de betrokkene geen kennis neemt van de verstrekte informatie dan is dat zijn eigen verantwoordelijkheid. Aan de informatieplicht is dan wel voldaan.
Verder geldt er geen informatieplicht wanneer de verwerking van de persoonsgegevens uitdrukkelijk bij wet is voorgeschreven of wanneer de informatieverstrekking aan de betrokkene onmogelijk blijkt of onevenredig veel inspanningen zou kosten.
In het verwerkingenregister wordt gemotiveerd opgenomen of er sprake is van een uitzondering op de informatieplicht.

4.7.2 Het recht op inzage

De betrokkene heeft het recht om zijn persoonsgegevens in te zien. Als de betrokkene een verzoek doet dan moet de volgende informatie verstrekt worden.

a. de verwerkingsdoeleinden
b. de betrokken categorieën van persoonsgegevens
c. de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt
d. zo mogelijk de bewaartermijn van de persoonsgegevens
e. de bron van de gegevens als de betrokkene deze niet zelf heeft verstrekt
f. de mededeling over het recht op rectificatie, verwijdering, beperking van de verwerking van de persoonsgegevens of bezwaar te maken tegen de verwerking
g. mededeling over het recht om een klacht in te dienen bij de AP
h. indien van toepassing, informatie over geautomatiseerde besluitvorming op basis van profilering
i. indien van toepassing, informatie over de doorgifte van de gegevens aan een niet EU-land en de bijbehorende passende waarborgen.

Van de persoonsgegevens wordt een kopie of compleet overzicht aan de betrokkene verstrekt. De kopie of het overzicht moet de betrokkene in staat stellen om zijn gegevens te controleren en te kunnen beoordelen of zijn gegevens rechtmatig worden verwerkt. De kopie of het overzicht mogen geen gegevens bevatten van anderen.

4.7.3 Het recht op rectificatie

De betrokkene heeft recht op correctie van zijn persoonsgegevens als deze onjuist zijn. Voor het aantonen van de onjuistheid moet de betrokkene deugdelijke bewijsstukken overleggen. Als de onjuistheid is vastgesteld wordt de correctie direct doorgevoerd.
De ontvangers van de persoonsgegevens worden hierover direct geïnformeerd.

4.7.4 Het recht op verwijdering (vergetelheid)

In een aantal gevallen heeft de betrokkene het recht op verwijdering van zijn persoonsgegevens.

a. als de persoonsgegevens niet langer nodig zijn voor het doel waarvoor ze zijn verzameld
b. als de betrokkene zijn toestemming voor de verwerking van de persoonsgegevens intrekt en er geen andere rechtsgrond is voor de verwerking
c. als de rechtsgrond voor de verwerking is de vervulling van een algemene publieke taak overheidstaak of de behartiging van een gerechtvaardigd belang, de betrokkenen tegen deze verwerking bezwaar maakt en er geen belang is voor de verwerking dat zwaarder weegt dan het belang van de betrokkene
d. als de persoonsgegevens onrechtmatig worden verwerkt
e. als de persoonsgegevens op basis van een wettelijke verplichting moeten worden verwijderd.

Als het verzoek tot verwijdering wordt gehonoreerd dan worden de verantwoordelijken die de persoonsgegevens hebben ontvangen hierover geïnformeerd. De andere verantwoordelijken kunnen dan overwegen om ook in hun verwerkingen de persoonsgegevens te verwijderen.
Bij het verzoek tot verwijdering wordt rekening gehouden met de uitzonderingen van artikel 17 lid 3 van de AVG.

4.7.5 Het recht op beperking van het verwerken van persoonsgegevens

De betrokkene heeft het recht op beperking van het verwerken van zijn persoonsgegevens. Dit houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt en niet gewijzigd worden. Als er sprake is van beperking van verwerking dan moet dan wordt hiervan een aantekening gemaakt in het betreffende bestand, zodat de beperking ook duidelijk is voor de ontvangers van de persoonsgegevens. Over de opheffing van de beperking wordt de betrokkene direct geïnformeerd. Wanneer de beperking weer wordt opgeheven, moet de betrokkene hiervan op de hoogte worden gebracht.
Beperking is mogelijk als:

a. de juistheid van de gegevens door de betrokkene wordt betwist
b. de verwerking onrechtmatig is maar de betrokkene wil (nog) niet dan zijn gegevens worden gewist
c. de bewaartermijn is verstreken maar de betrokkene heeft de gegevens nog nodig in verband met een rechtsvordering
d. de betrokkene heeft bezwaar gemaakt tegen de verwerking van zijn persoonsgegevens, maar er is nog niet op het bezwaar beslist.

4.7.6 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

De betrokkene heeft het recht om zijn persoonsgegevens te verkrijgen in een overdraagbare vorm, zodat hij zijn gegevens aan een andere verwerkingsverantwoordelijke kan overdragen. Dit recht geldt alleen als de persoonsgegevens door de betrokkene zijn verkregen met de toestemming van de betrokkene of voor de uitvoering van een overeenkomst.
Voor de vorm van de overdracht wordt zoveel mogelijk rekening gehouden met de wens van de betrokkene.

4.7.7 Recht van bezwaar

De betrokkene heeft het recht om bezwaar te maken tegen de verwerking van zijn gegevens. Dit is geen bezwaar zoals bedoeld in de Awb. De betrokkene kan dit recht alleen uitoefenen als het gaat om persoonsgegevens die worden verwerkt voor de uitoefening van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag of voor de behartiging van een gerechtvaardigd belang.
Als de betrokkene een beroep doet op dit recht wordt de verwerking van de persoonsgegevens gestopt, tenzij het belang van de verwerking zwaarder weegt dan het belang van de betrokkene.

4.7.8 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling

De gemeente Veere neemt geen besluiten op basis van uitsluitend geautomatiseerde verwerking van persoonsgegevens, dus zonder menselijke tussenkomst.
Als de gemeente Veere besluit om deze vorm van besluitvorming wel toe te passen dan worden daarbij passende maatregelen getroffen die ervoor zorgen dat de bescherming van de gerechtvaardigde belangen van de betrokkenen zijn gewaarborgd. Deze

maatregelen worden vooraf ter toetsing voorgelegd aan de functionaris gegevensbescherming.

4.7.9 Spelregels voor het uitoefenen van de rechten van de betrokkene

a. Voor het gebruik maken van zijn rechten gebruikt de betrokkene bij voorkeur het verzoekformulier zoals dat beschikbaar is op www.veere.nl/privacy. Dit formulier stuurt de betrokkene (geautomatiseerd) naar het e-mailadres van de privacy officer privacy@veere.nl
b. Een verzoek van de betrokkene op een andere wijze dan het verzoekformulier op de website wordt alleen in behandeling genomen als de identiteit van de betrokkene voldoende is vastgesteld.
c. In zijn verzoek maakt de betrokkene zo specifiek mogelijk duidelijk op welke verwerking of verwerkingen zijn verzoek betrekking heeft.
d. Als na het verzoek van de verantwoordelijke de betrokkene zijn verzoek niet voldoende specifiek heeft gemaakt, wordt het verzoek afgewezen.
e. Als na het verzoek van de verantwoordelijke de betrokkene zijn belang niet voldoende specifiek heeft gemaakt, wordt het verzoek afgewezen.
f. Meer dan twee dezelfde verzoeken over dezelfde verwerking per kalenderjaar wordt aangemerkt als buitensporig en wordt om die reden afgewezen. Tenzij de aard van de verwerking het met zich mee brengt dat er frequent wijzigingen worden opgenomen.
g. Een verzoek van de betrokkene wordt schriftelijk (brief, e-mail) beantwoord. Op verzoek van de betrokkenen kan ook mondeling informatie worden meegedeeld, onder de voorwaarde dat de identiteit van de betrokkene is vastgesteld.
h. Een elektronisch ingediend verzoek om inzage wordt elektronisch afgedaan.
i. Een verzoek wordt binnen één maand na ontvangst afgedaan. Deze termijn kan maximaal met twee maanden worden verlengd. Verlenging is niet mogelijk als het verzoek niet wordt gehonoreerd.
j. Een afwijzing van een verzoek van de betrokkene wordt altijd per brief bekend gemaakt.
k. Het besluit op een verzoek van een betrokkene is een besluit in de zin van de Awb waartegen bezwaar en beroep mogelijk is.
l. Kennisgevingen aan ontvangers over correctie, wissing of beperking van persoonsgegevens worden zoveel mogelijk via een netwerkverbinding gedaan. Als dat niet mogelijk is dan wordt de kennisgeving schriftelijk (brief, e-mail) gedaan.

4.7.10 Het uitoefenen van zijn rechten als de betrokkene minderjarig is

Als de betrokkene minderjarig is geldt voor het uitoefenen van zijn rechten het volgende:

a. Als de betrokkene jonger dan 12 jaar is worden zijn rechten uitgeoefend door zijn wettelijke vertegenwoordiger.
b. Als de betrokkene 12 jaar of ouder is maar nog geen 16 jaar, dan oefent hij zijn rechten uit samen met zijn wettelijke vertegenwoordiger.
c. Als de betrokkene 16 jaar of ouder is dan oefent hij zijn rechten zelfstandig uit.

Vanaf 12 jaar is de stem van de minderjarige belangrijk. Als de minderjarige geen toestemming verleent dan vindt een belangenafweging plaats. Daarbij staat de bescherming van persoonsgegevens voorop.
Vanaf 16 jaar is de toestemming van de minderjarige vereist.

4.8 Beveiligingsmaatregelen

De verwerkingsverantwoordelijke heeft op grond van de AVG de plicht om passende technische en organisatorische maatregelen te treffen die ervoor zorgen dat de bescherming van persoonsgegevens gewaarborgd is. Passende maatregelen wil zeggen dat het niet altijd om de zwaarste maatregelen gaat, maar juist om de maatregelen die passen bij de aard, de omvang en het doel van de verwerking. Het onderzoek in het kader van privacy by design of de uitvoering van een DPIA geeft duidelijkheid over de passende beveiligingsmaatregelen.

Ten aanzien van de vertrouwelijkheid, de integriteit, de beschikbaarheid en de veerkracht van de verwerkingen en de systemen waarmee de persoonsgegevens verwerkt worden, hanteert de gemeente Veere het normenkader van de Baseline Informatiebeveiliging Gemeenten (BIG). Het voldoen aan de BIG garandeert dat de persoonsgegevens beveiligd zijn tegen verlies of onrechtmatige verwerking. Ook de beschikbaarheid en de veerkracht van de persoonsgegevens en de systemen waarmee deze verwerkt worden, zijn gewaarborgd door het voldoen aan de BIG.
Jaarlijks wordt het voldoen aan de BIG getoetst in het kader van ENSIA.

Voor de betrouwbaarheid en de actualiteit van de persoonsgegevens worden de systemen waarmee persoonsgegevens worden verwerkt zoveel mogelijk gekoppeld aan de Gegevensmakelaar. Dit garandeert het gebruik van persoonsgegevens zoals die in de diverse authentieke registraties zijn opgenomen. Aanvullende persoonsgegevens die niet in de Gegevensmakelaar zijn opgenomen, worden geactualiseerd na een melding van de betrokkene of gecontroleerd en zo nodig geactualiseerd bij een contactmoment met de betrokkene.

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor de gegevens zijn verzameld, daarbij wordt rekening gehouden met de bewaartermijnen zoals die in de betreffende wetgeving zijn opgenomen. De bewaartermijn wordt vastgelegd in het verwerkingenregister.
Bij de inrichting en het gebruik van taakspecifieke applicaties wordt rekening gehouden met de bewaartermijn.
Het MT neemt maatregelen die ervoor zorgen dat bestanden met persoonsgegevens buiten taakspecifieke applicaties (excel, word, acces, etc.) tijdig worden verwijderd.
Als de Archiefwet dit vereist kunnen persoonsgegevens langer bewaard worden. In dat geval wijzigt de verwerkingsgrondslag en het verwerkingsdoel en zijn de rechten van betrokkenen begrensd overeenkomstig artikel 43 lid 1 van de Uitvoeringswet Algemene Verordening Gegevensbescherming.

Het MT kan besluiten om aanvullende technische en organisatorische maatregelen te nemen die ervoor zorgen dat de risico's door het menselijk handelen ten aanzien van de bescherming van persoonsgegevens, worden beperkt.

De maatregelen van het MT zijn opgenomen in bijlage 5.

Het MT zorgt ervoor dat maatregelen, afspraken, instructies, etc., zo mogelijk en zo nodig worden opgenomen in procesbeschrijvingen, werkbeschrijvingen of werkafspraken.

4.9 Datalek

Een datalek is een beveiligingsincident waarbij persoonsgegevens zijn betrokken. Persoonsgegevens kunnen verloren zijn gegaan of gestolen, door bijvoorbeeld brand of hacking. Het kan ook zijn dat persoonsgegevens onrechtmatig zijn verwerkt door

bijvoorbeeld onbevoegde raadpleging of verzending naar een verkeerde e-mailgeadresseerde.

Een datalek moet binnen 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen, gemeld worden bij de AP. Deze melding is niet nodig als het datalek naar verwachting geen risico inhoudt voor de rechten en vrijheden van de bij het datalek betrokken personen.
Als er sprake is van een hoog risico voor de rechten en vrijheden van de bij het datalek betrokken personen dan moeten deze personen geïnformeerd worden. Er wordt dan meegedeeld wat er gebeurd is, wat de mogelijke gevolgen zijn en wat er gedaan is of wordt om de schade te beperken. Ook worden de betrokkenen verwezen naar de FG en andere organisaties voor meer informatie en voor eventueel hulp en ondersteuning.

Het MT heeft een procedure vastgesteld voor het beheer van informatiebeveiligingsincidenten waaronder ook datalekken. Deze procedure is onderdeel van het Privacybeleid gemeente Veere en wordt toegepast.
In deze procedure is beschreven welke functionarissen verantwoordelijk en betrokken zijn bij een beveiligingsincident. Verder is in de procedure beschreven op welke wijze de impact van het beveiligingsincident wordt beoordeeld. Op basis van die beoordeling wordt door de verantwoordelijke functionarissen besloten of het datalek gemeld wordt aan de AP en de betrokkenen.

De procedure is beschreven in het document 'Beheer van informatiebeveiligingsincidenten'. Dit document is opgenomen in bijlage 6.

4.10 Openbaar maken informatie (Wob)

De gemeente verzamelt, gebruikt en beheert informatie die in bepaalde gevallen ook openbaar gemaakt wordt. Als deze informatie persoonsgegevens bevatten dan gelden hiervoor een aantal voorwaarden en spelregels. T.a.v. het openbaar maken van informatie worden drie situaties onderscheiden: actieve verplichte openbaarmaking, passieve verplichte openbaarmaking en openbaarmaking uit eigen beweging. In alle situaties staat de bescherming van de persoonlijke levenssfeer voorop.
Persoonsgegevens worden alleen openbaar gemaakt als dat wettelijk verplicht is of in het geval het belang van openbaarmaking groter is dan het belang van de bescherming van de persoonlijke levenssfeer. Van dat laatste kan bijvoorbeeld sprake zijn als de informatie een benoeming in een openbare functie betreft (denk aan een toezichthouder) of als de persoonsgegevens van doorslaggevende betekenis zijn voor de inhoud van de informatie.
De terughoudendheid t.a.v. het openbaar maken van persoonsgegevens is ook van belang m.b.t. het principe 'eenmaal openbaar is altijd openbaar'. Het te lichtvaardig openbaar maken van persoonsgegevens kan een probleem opleveren als openbaarmaking op een later moment ongewenst is. Is de informatie eenmaal openbaar gemaakt dan kan een later verzoek tot openbaarmaking niet geweigerd worden.

Uit de jurisprudentie blijkt dat het categorische weigeren van informatie niet is toegestaan. Van categorisch weigeren is sprake als vanwege één bepaalde uitzonderingsgrond in het geheel geen informatie wordt verstrekt. Dat is niet toegestaan, per document of per passage moet dan gemotiveerd worden waarom die informatie niet wordt verstrekt. Persoonsgegevens niet verstrekken door deze onleesbaar te maken is geen categorische weigering, de informatie wordt immers wel verstrekt. Als het verzoek juist is gericht op het verstrekken van persoonsgegevens, dan vindt een afweging van belangen plaats, zie onderdeel 4.10.2.2.

Met onleesbaar maken wordt bedoeld iedere aanpassing die ervoor zorgt dat de betreffende persoonsgegevens niet openbaar worden. Dat kan op een fysieke of digitale manier. Ook het anonimiseren van persoonsgegevens is een geaccepteerde manier van onleesbaar maken.

Op basis van deze uitgangspunten wordt het openbaar maken van informatie als volgt toegepast.

4.10.1 Actieve verplichte openbaarmaking

Artikel 8 van de Wet openbaarheid van bestuur (Wob) verplicht het bestuursorgaan dat het aangaat om uit eigen beweging informatie te verschaffen over het beleid, de voorbereiding en de uitvoering daarvan begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering.
Dit artikel in de Wob is voor een groot deel van de gemeentelijke informatie de kapstok voor openbaarmaking. Daarnaast worden in een aantal bijzondere wetten ook verplichtingen gegeven tot openbaarmaking van informatie. Denk hier bij aan de WABO, Wet Milieubeheer, Jeugdwet, etc.
Bij het actief verstrekken van informatie wordt in alle gevallen rekening gehouden met de uitzonderingsgronden van artikel 10 en 11 van de Wob, tenzij hiervoor in de betreffende bijzondere wetten specifieke aanwijzingen zijn gegeven.

4.10.1.1 Omgevingsvergunningen

In de bekendmakingen over aanvragen van en besluiten over omgevingsvergunningen worden geen persoonsgegevens opgenomen. Ook niet als de aanvrager in de aanvraag van een omgevingsvergunning heeft aangegeven geen bezwaar te hebben tegen publicatie. Deze toestemming is mogelijk niet vrij maar in ieder geval niet specifiek en de betrokkene is niet geïnformeerd over de betekenis van de toestemming. Hierdoor kan de toestemming niet dienen als grondslag voor de verwerking van persoonsgegevens.
In de bekendmaking zoals bedoeld in artikel 3.8 en 3.9 Wabo wordt naast de ontvangstdatum of de besluitdatum de aanduiding van de locatie van de betreffende Wabo-activiteit opgenomen.
De documenten in het omgevingsvergunningdossier worden niet actief openbaar gemaakt. Op verzoek worden de betreffende documenten toegestuurd. De persoonsgegevens in deze documenten worden onleesbaar gemaakt. Om deze reden kunnen de omgevingsvergunningdossiers niet ingezien worden.

4.10.1.2 Informatie ten behoeve van de gemeenteraad en raadscommissies

Voor de beraadslagingen van de gemeenteraad en de raadscommissies stelt het college informatie beschikbaar in diverse vormen. Het uitgangspunt is dat in deze informatie alleen persoonsgegevens worden opgenomen als deze dienstbaar en noodzakelijk zijn voor de beraadslagingen.
Er wordt onderscheid gemaakt tussen de informatie die direct beschikbaar wordt gesteld aan de gemeenteraad en de raadscommissies en de informatie die openbaar wordt gemaakt in het kader van een transparant openbaar bestuur.

4.10.1.2.1 Informatie die direct beschikbaar wordt gesteld aan de gemeenteraad en de raadscommissies

Voor de beraadslagingen van de gemeenteraad en de raadscommissies stelt het college de vergaderstukken via NotuBiz ter beschikking. Dit is een gesloten omgeving niet bedoeld en niet geschikt voor openbaarmaking. Voor de beraadslaging en de besluitvorming is het noodzakelijk dat de persoonsgegevens die in deze informatie zijn opgenomen, leesbaar blijven.

De leden van de gemeenteraad en raadscommissie delen deze informatie niet met derden.

4.10.1.2.2 Informatie die openbaar wordt gemaakt in het kader van een transparant openbaar bestuur

De vergaderstukken van de gemeenteraad en de raadscommissies worden via het open gedeelte van NotuBIz openbaar gemaakt. De videotulen maken ook deel uit van deze vergaderstukken. De persoonsgegevens die in deze informatie zijn opgenomen worden onleesbaar gemaakt, met uitzondering van de persoonsgegevens die van doorslaggevende betekenis zijn voor de inhoud van de informatie.
Bij het onleesbaar maken wordt rekening gehouden met de verschillende categorieën betrokkenen.

4.10.1.2.2.1 Bestuurlijke gezagsdragers

De persoonsgegevens van de bestuurlijke gezagsdragers: de burgemeester, wethouders, raadsleden en raadscommissieleden blijven leesbaar voor zover de persoonsgegevens betrekking hebben op het functioneren als bestuurlijk gezagsdrager.

4.10.1.2.2.2 Ambtenaren

De persoonsgegevens van ambtenaren die een formele functie bekleden: de griffier en de gemeentesecretaris blijven leesbaar voor zover de persoonsgegevens betrekking op het functioneren in de formele functie.
De persoonsgegevens van ambtenaren die een geattribueerde, gedelegeerde of gemandateerde bevoegdheid uitoefenen blijven leesbaar voor zover de persoonsgegevens betrekking hebben op het uitoefenen van die bevoegdheid.
De persoonsgegevens van ambtenaren die een adviserende functie hebben worden onleesbaar gemaakt.

4.10.1.2.2.3 Burgers die mondeling of schriftelijk contact maken met de Gemeente Veere

Als in de vergaderstukken persoonsgegevens voorkomen van burgers die mondeling of schriftelijk contact hebben gemaakt met de gemeente (vraag, aanvraag, klacht, petitie, etc.) dan worden die persoonsgegevens onleesbaar gemaakt. Als het contact betrekking heeft op één of meer andere burgers dan worden ook die persoonsgegevens onleesbaar gemaakt.
In de ontvangstbevestiging aan de betreffende burgers worden zij gewezen op dit beleid en overige relevante privacyaspecten.

4.10.1.2.2.4 Inspreekers tijdens de raadsvergadering en de raadscommissievergadering

Burgers die inspreken tijdens een vergadering van de gemeenteraad of een raadscommissie kiezen zelf voor de openbaarheid. Het is daardoor onvermijdelijk dat de persoonsgegevens openbaar gemaakt worden. In de vergaderstukken worden de persoonsgegevens van insprekers daarom niet onleesbaar gemaakt voor zover het de persoonsgegevens betreft die de inspreker zelf in de openbaarheid brengt (zoals bijvoorbeeld de toespraak van de inspreker).

4.10.1.2.2.5 Burgers die onderwerp zijn van of betrokken zijn bij de besluitvorming

Als in de vergaderstukken persoonsgegevens voorkomen van burgers die onderwerp zijn van of betrokken zijn bij de besluitvorming dan worden deze persoonsgegevens onleesbaar gemaakt.

4.10.2 Passieve verplichte openbaarmaking

Artikel 3, 6 en 7 van de Wet openbaarheid van bestuur (Wob) verplicht het bestuursorgaan informatie te verstrekken op verzoek. Dit wordt doorgaans aangeduid als een Wob-verzoek.
Bij het beslissen op een Wob-verzoek wordt in alle gevallen rekening gehouden met de uitzonderingsgronden van artikel 10 en 11 van de Wob.

Artikel 10 lid 1 aanhef en onder d van de Wob bepaalt dat geen informatie wordt verstrekt als er bijzondere persoonsgegevens (godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging). in de informatie zijn opgenomen. Dit is een absolute uitsluitingsgrond.
Artikel 10 lid 2 aanhef en onder e. van de Wob bepaalt dat geen informatie wordt verstrekt als het belang van de verstrekking niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer. Dit is een relatieve uitsluitingsgrond, dat betekent dat er een afweging van belangen moet plaatsvinden.

4.10.2.1 Informatieverstrekking op basis van een Wob-verzoek zonder uitdrukkelijk verzoek om verstrekking van persoonsgegevens

Als informatie wordt verstrekt op basis van een Wob-verzoek waarin niet uitdrukkelijk om de verstrekking van persoonsgegevens wordt gevraagd, dan worden de persoonsgegevens die in de informatie zijn opgenomen standaard onleesbaar gemaakt. In het besluit op het Wob-verzoek wordt hiervoor verwezen naar dit vaste beleid met als motivering de eerbiediging van de persoonlijke levenssfeer.

4.10.2.2 Informatieverstrekking op basis van een Wob-verzoek met uitdrukkelijk verzoek om verstrekking van persoonsgegevens

Als de indiener van een Wob-verzoek uit eigen beweging uitdrukkelijk verzoekt om verstrekking van de persoonsgegevens en daarbij aangeeft welk (algemeen) belang daarmee gediend is, vindt een afweging van belangen plaatst. In het besluit op het Wob-verzoek wordt deze afweging van belangen gemotiveerd.

4.10.2.3 Informatieverstrekking op basis van een Wob-verzoek met uitdrukkelijk verzoek om verstrekking van persoonsgegevens, maar zonder belang

Als de indiener van een Wob-verzoek uit eigen beweging uitdrukkelijk verzoekt om verstrekking van persoonsgegevens maar daarbij niet aangeeft welk (algemeen) belang daarmee gediend is, wordt de indiener verzocht om dat belang kenbaar te maken of zo nodig te verduidelijken. Als de indiener dit belang niet of niet voldoende duidelijk maakt en er wordt informatie verstrekt dan worden de persoonsgegevens in de informatie onleesbaar gemaakt. In het besluit op het Wob-verzoek wordt hiervoor verwezen naar dit vaste beleid met als motivering de eerbiediging van de persoonlijke levenssfeer.

4.10.3 Openbaarmaking uit eigen beweging

Bekendmakingen zonder wettelijk grondslag betreffen meestal nieuws of huishoudelijke mededelingen met betrekking tot de gemeente Veere, zoals de openingstijden van het gemeentehuis, het rooster van de afvalophaaldienst, nieuws over activiteiten van de gemeente, informatie over producten en diensten, etc.
In deze bekendmakingen worden geen persoonsgegevens opgenomen, behalve de persoonsgegevens van:

a. bestuurlijke gezagsdragers voor zover de persoonsgegevens in het bekendgemaakte onderwerp betrekking hebben op het functioneren als bestuurlijk gezagsdrager;
b. de persoonsgegevens van medewerkers van de gemeente Veere die wegens hun functie in de openbaarheid treden voor zover de persoonsgegevens in het bekendgemaakte onderwerp daar betrekking op hebben;
c. medewerkers van de gemeente Veere die fungeren als contactpersoon voor het bekendgemaakte onderwerp en die voorafgaand toestemming hebben verleend voor het openbaar maken van hun persoonsgegevens
d. personen die betrokken zijn bij de inhoud van het bekendgemaakte onderwerp en die voorafgaand toestemming hebben verleend voor het openbaar maken van hun persoonsgegevens.

4.11 Video- en fotobeelden

Video- en fotobeelden worden voor diverse doeleinden gebruikt. Als de videobeelden (herkenbare) persoonsgegevens bevatten dan gelden hiervoor een aantal voorwaarden en spelregels. Niet in alle situaties zijn deze voorwaarden en spelregels even duidelijk toepasbaar. Uitgangspunt is de bescherming van de persoonlijke levenssfeer. Bij het maken van de afweging om wel of geen opnames te maken moet er altijd gestreefd worden naar een goede balans tussen het belang van de opnames en het belang van de bescherming van de persoonlijke levenssfeer.
Video- en fotobeelden worden uitsluitend gemaakt in de openbare ruimte, dus de plaatsen die voor het publiek toegankelijk zijn.

4.11.1 Vooraf informeren

Als bij het maken van opnames vooraf duidelijk is dat persoonsgegevens worden vastgelegd dan worden de betrokkenen daar ook vooraf over geïnformeerd. Voor het informeren kunnen verschillende manieren worden toegepast. De informatie moet zodanig zijn dat de betrokkenen op de hoogte kunnen zijn van het feit dat er opnames worden gemaakt, en daarover een beslissing kunnen nemen. Een verzoek door een betrokkene om niet beeld gebracht te worden of om de beelden onherkenbaar te maken, wordt altijd gehonoreerd.
Voorbeelden van vooraf informeren zijn: informatiebord bij de toegang, het tonen van de beelden op een monitor, het zichtbaar zijn van de camera (zonder dat de betrokkene al in beeld is), een mededeling in een uitnodiging of een ontvangstbevestiging.

4.11.2 Grondslag

Als met het maken van opnames persoonsgegevens worden verwerkt dan is dat alleen toegestaan als daarvoor een wettelijke grondslag bestaat.

4.11.2.1 Cameratoezicht (publiek)

Cameratoezicht wordt ingezet als dat noodzakelijk is voor het handhaven van de openbare orde. Dit is mogelijk op basis van artikel 151c van de Gemeentewet en artikel 2.77 van de APV Veere 2018. Deze vorm van cameratoezicht kan alleen betrekking hebben op openbare plaatsen, zoals straten, wegen, pleinen, plantsoenen, overdekt

winkelcentrum, vliegveld, etc. De toegang tot de openbare plaats moet geheel vrij zijn. Gebouwen zijn uitgesloten van deze vorm van toezicht.
In het besluit van de burgemeester wordt de noodzakelijkheid van de inzet van cameratoezicht vastgelegd. Het besluit van de burgemeester omvat verder alle elementen zoals die in artikel 151c van de Gemeentewet worden voorgeschreven. Het beheer en gebruik van de opnames is in handen van de politie.

4.11.2.2 CAMERABEWAKING (PRIVAAT)

Camerabewaking is toegestaan als dat noodzakelijk is voor het beschermen van eigendommen en personen. Dit valt onder het gerechtvaardigd belang zoals bedoeld in artikel 6, lid 1 onder f van de AVG.
De inzet van camerabewaking en –beveiliging gebeurt op basis van een besluit door of namens het college van B&W. Uit dat besluit moet blijken dat er ook andere beveiligingsmaatregelen zijn genomen en dat deze niet (voldoende) effectief zijn. Camerabewaking is dus een uiterst middel en moet noodzakelijk zijn.
Verder is het volgende in het besluit opgenomen:
- de eigendommen en/of personen die beschermd worden en dus in beeld gebracht worden;
- de duur van de camerabewaking;
- het beheer en gebruik van de opnames; wie beheert de opnames, wie heeft toegang tot de opnames en aan wie worden de opnames verstrekt;
- de bewaartermijn van de opnames (maximaal 4 weken);
- de manier waarop de betrokkenen worden geïnformeerd;
- de maatregelen die genomen worden om er voor te zorgen dat niet onnodig gebouwen, terreinen en zaken van anderen of de openbare weg in beeld worden gebracht;
- de beveiligingsmaatregelen die genomen worden om onbevoegde toegang tot de opnames onmogelijk te maken;
- de manier waarop betrokkenen gebruik kunnen maken van hun rechten; inzage, correctie en verwijdering.

Het besluit tot inzet van camerabewaking wordt op de gebruikelijke wijze bekendgemaakt.

4.11.2.3 VIDEOTULEN

Van de vergaderingen van de gemeenteraad en de raadscommissies worden live video-opnames gemaakt. Het doel van deze opnames is het vergroten van de betrokkenheid bij en de transparantie van de lokale politiek. De videotulen dienen ook als digitale verslaglegging van de vergaderingen en moeten om die reden ook gearchiveerd worden volgens de regels van de Archiefwet.
Deze doelen vallen onder het gerechtvaardigd belang zoals bedoeld in artikel 6, lid 1 onder f van de AVG.

In de opnames worden diverse personen in beeld gebracht:
- Raadsleden, commissieleden, burgemeester, wethouders, griffier, secretaris. Voor deze groep betrokkenen geldt dat een openbare functie bekleden en geacht worden bekend te zijn met het doel van de opnames. Er zijn geen verdere maatregelen nodig voor de bescherming van de persoonlijke levenssfeer.
- Ambtenaren. Deze groep betrokkenen bekleedt geen openbare functie maar wordt wel geacht bekend te zijn met het doel van de opnames. Het is de taak van het betreffende afdelingshoofd om de betrokkenen daarover te informeren. Op verzoek wordt de betrokkene niet in beeld gebracht of wordt het beeld onherkenbaar gemaakt.
- Journalisten en andere professionals. Deze groep betrokkenen wordt geacht bekend te zijn met het doel van de opnames. Op verzoek wordt de betrokkene niet in beeld gebracht of wordt het beeld onherkenbaar gemaakt.

- Insprekers en publiek. Deze groep betrokkenen moet vooraf geïnformeerd worden over de opnames en het doel ervan. Dat kan door bekendmaking in de uitnodiging en/of de agenda voor de vergadering. In het geval er sprake is van spontane insprekers of publiek kan de voorzitter melden dat er opnames worden gemaakt. Op verzoek wordt de betrokkene niet in beeld gebracht of wordt het beeld onherkenbaar gemaakt.

Van de betrokkene is geen toestemming nodig voor het maken van de opnames.

4.11.2.4 VRIJE NIEUWSGARING

Het recht op vrije nieuwsgaring is niet expliciet in de wet vastgelegd, dit recht is gebaseerd op het grondrecht vrijheid van meningsuiting. Iedereen is vrij om informatie te verzamelen en te verspreiden. Hooguit kan de rechter achteraf vaststellen dat dit onrechtmatig is.
De gemeente Veere maakt video- en fotobeelden voor de volgende doelen:
- Het bekendmaken van nieuws over zaken en gebeurtenissen die de gemeente aangaan;
- Het onder de aandacht brengen van zaken van algemeen belang
- Het verbeteren van de dienstverlening

Deze doelen vallen onder het gerechtvaardigd belang zoals bedoeld in artikel 6, lid 1 onder f van de AVG. Als met de opnames persoonsgegevens worden vastgelegd dan kan dit zonder toestemming van de betrokkenen. Wel moeten de betrokkenen zoveel mogelijk vooraf geïnformeerd worden over het doel van de opnamen. Dat is in ieder geval noodzakelijk als een betrokkene direct herkenbaar in beeld wordt gebracht. Als de opnames een min of meer massaal beeld van personen geeft dan is het niet mogelijk om (alle) betrokkenen te informeren. Het kunnen voldoen aan de informatieplicht hangt ook af van plaats en gelegenheid. Er moet gestreefd worden naar een goede balans tussen het belang van de opnames en het belang van de bescherming van de persoonlijke levenssfeer.
Op verzoek wordt de betrokkene niet in beeld gebracht of wordt het beeld onherkenbaar gemaakt. Betrokkenen kunnen ook een beroep doen op het portretrecht.

4.11.2.5 OPNAMES IN BESLOTEN OMGEVING

De gemeente Veere maakt video- en fotobeelden van personeelsactiviteiten. Hiervoor bestaat geen wettelijke grondslag. Voor de verwerking van persoonsgegevens is toestemming nodig van de betrokkene. Deze toestemming wordt vastgelegd bij de indiensttreding van de betrokkene of zo spoedig mogelijk daarna. De toestemming wordt vastgelegd in het personeelsdossier.
Als geen toestemming is verleend dan wordt daarmee rekening gehouden bij het maken van video- en fotobeelden.

4.11.3 LUCHTFOTO'S EN CYCLORAMA'S TEN BEHOEVE VAN DE GEMEENTELIJKE ADMINISTRATIES

De leveranciers van de luchtfoto's en de cyclorama's zorgen ervoor dat de persoonsgegevens op deze foto's worden geblurd.

5. Accountability

In dit hoofdstuk wordt beschreven op welke wijze de verwerkingsverantwoordelijke van de gemeente Veere aantoont dat hij voldoet aan de wettelijke verplichtingen ten aanzien van de privacywet en –regelgeving.

5.1 Toezicht op naleving van de AVG

Dit is een belangrijke taak van de FG. De FG is belast met het toezicht op de naleving van de privacywet- en regelgeving.
Om deze taak te kunnen uitvoeren moet de FG kunnen beschikken over de relevante informatie die hiervoor nodig is. Voor het op een gestructureerde manier beschikbaar stellen van deze informatie wordt gebruik gemaakt van de Governance, Riskmanagement & Compliance (GRC) applicatie van Key2Control. Deze applicatie bevat een Information Security Management System (ISMS) waarmee alle procedures en maatregelen op het gebied van informatiebeveiliging gemonitord en beheerd worden. De GRC-applicatie bevat ook een Privacy Control Framework. In dit framework zijn alle verplichtingen vanuit de AVG vertaald naar procedures, maatregelen en acties. Daarmee is dit framework een belangrijk instrument voor de FG voor zijn taak als toezichthouder.
Daarnaast wordt voor het verwerkingenregister ook een applicatie van Key2Control gebruikt. Dit register geeft de FG inzicht in de verwerkingen waarvoor de gemeente Veere verantwoordelijk is. Het register wordt door de FG gebruikt voor de controle op de juiste naleving van de AVG.

(Gereserveerd: Op advies van de FG zal dit onderdeel van het Privacybeleid gemeente Veere nog aangevuld worden.)

5.2 Onderzoek en advies

De FG kan gevraagd en ongevraagd onderzoek doen naar de toepassing van de privacywetgeving. Op basis van dat onderzoek adviseert de FG de verwerkingsverantwoordelijke en het management over het voorkomen van privacyrisico’s en het verbeteren van de bescherming van persoonsgegevens. De resultaten van de onderzoeken en de adviezen worden vastgelegd.

(Gereserveerd: Op advies van de FG zal dit onderdeel van het Privacybeleid gemeente Veere nog aangevuld worden.)

5.3 Documentatie

Zeggen wat we doen is niet voldoende. Voor de bewijslast is het nodig om vast te leggen wat we doen. Voor het toezicht op de naleving van de privacywet- en regelgeving beschikken we over een groot aantal documenten waarin is beschreven hoe die naleving is vormgegeven, uitgevoerd en gecontroleerd. Een belangrijk document is het Privacybeleid gemeente Veere waarin het privacybeleid is beschreven. Daarnaast gaat het om: privacystatement website, beschrijving werkprocessen (met aandacht voor privacy), aanvraagformulieren, verwerkingenregister, verwerkersovereenkomsten, uitvoeringsinstructies, integriteitsprotocol, etc. Al deze documenten worden opgenomen in de GRC-applicatie zodat de FG deze kan gebruiken bij zijn taak als toezichthouder.

(Gereserveerd: Op advies van de FG zal dit onderdeel van het Privacybeleid gemeente Veere nog aangevuld worden.)

5.4 Privacy bewustzijn

De AVG biedt een duidelijk formeel kader voor het verwerken van persoonsgegevens. In het Privacybeleid gemeente Veere en aanvullende documentatie is ook het materiële kader goed beschreven en ingericht, maar de uitvoering blijft mensenwerk. Het zijn mensen die de regels moeten toepassen en uitvoeren.
Die mensen zijn niet alleen de medewerkers maar het zijn ook de mensen in het management en in het bestuur.
Goede bescherming van persoonsgegevens is alleen mogelijk als iedereen het juiste besef heeft van het belang van privacy. Dat besef is niet bij iedereen intrinsiek aanwezig, dat besef moet gevoed en gestimuleerd worden. Dat blijft de grootste en ook een voortdurende uitdaging.

Naast de acties via Mind your step (intranet) besteden we minimaal eenmaal per jaar in de afdelingsoverleggen aandacht aan de onderwerpen informatiebeveiliging en privacy. Verder is privacy een onderdeel van de resultaatgesprekken en van de advisering aan MT, college en raad. Medewerkers worden betrokken bij het uitvoeren van een PIA waardoor ze concreet aan de slag gaan met privacy.
Aanvullende en nieuwe acties die het privacybewustzijn verbeteren worden geïnitieerd door de FG.

(Gereserveerd: Op advies van de FG zal dit onderdeel van het Privacybeleid gemeente Veere nog aangevuld worden.)

6. Slot

De privacyregelgeving bestaat al lange tijd maar het gemeentelijk Privacybeleid is nog niet eerder beschreven en toegepast. In het tijdperk van de Wbp is er onvoldoende aandacht geweest voor de wettelijke verplichtingen t.a.v. het verwerken van persoonsgegevens. Dat heeft niet tot incidenten geleid maar de bescherming van persoonsgegevens heeft niet altijd de juiste aandacht gehad.
De AVG maakt het noodzakelijk om hierin verandering aan te brengen. Bescherming van persoonsgegevens is niet (meer) vrijblijvend. De gemeente moet aantoonbaar voldoen aan de wettelijke verplichtingen. Het gemeentelijk Privacybeleid is daarvoor een belangrijk instrument
Omdat het Privacybeleid nieuw is, is het ook vanzelfsprekend dat bepaalde onderdelen al snel weer aangepast, aangescherpt of misschien wel versoepeld moeten worden. De dagelijkse privacypraktijk zal dat leren. Het nu vastgestelde Privacybeleid zal in 2018 voor het eerst geëvalueerd worden door de FG. Op basis van die evaluatie zal de FG voorstellen doen voor aanpassing van het Privacybeleid.
Door de jaarlijks evaluatie en aanpassing ontstaat een degelijk Privacybeleid dat waarborgt dat de bescherming van persoonsgegevens het uitgangspunt is bij al ons handelen en al onze dienstverlening.

Bijlage 1

Handleiding verwerkingsregister Key2Control”.

Deze handleiding is opgenomen in Corsa onder nummer 18B.02184

Bijlage 2

Model verwerkersovereenkomst

Dit model is opgenomen in Corsa onder nummer 18B.02185

Bijlage 3

Model Data Protection Impact Assessment (DPIA)

Dit model is nog in voorbereiding.

Bijlage 4

Voorbeelden voor het informeren van betrokkenen

Aanvraagformulier:

Privacy
Als u een aanvraag indient, worden uw persoonsgegevens verwerkt voor de administratie van de parkeervergunningen. Het verwerken van uw persoonsgegevens gebeurt volgens de Algemene Verordening Gegevensbescherming (AVG). Op basis van deze Europese wet heeft u een aantal privacyrechten. Voor meer informatie hierover verwijzen wij u naar de privacyverklaring op onze website www.veere.nl/privacy

Brief:

Privacy
Wij hebben uw persoonsgegevens overgenomen uit het Kadaster en de actuele adresgegevens gecontroleerd in de Basisregistratie Personen (BRP).
Uw persoonsgegevens worden door ons verwerkt voor het project grondgebruik. Zodra we het grondgebruik met u opgelost hebben worden uw gegevens verwijderd.
Wij verwerken uw persoonsgegevens volgens de Algemene Verordening Gegevensbescherming (AVG). Op basis van deze Europese wet heeft u een aantal privacyrechten. Voor meer informatie hierover verwijzen wij u naar de privacyverklaring op onze website www.veere.nl/privacy

Contract:

Privacy
De gemeente Veere verstrekt de persoonsgegevens (nader omschrijven) van alle personen die een dienstbetrekking hebben bij de gemeente Veere aan ArboUnie. De persoonsgegevens van nieuwe medewerkers worden direct bij aanvang van het dienstverband verstrekt.
De persoonsgegevens van alle personen zijn nodig i.v.m. de mogelijkheid voor een medewerker om buitenom de werkgever contact te hebben met de ArboUnie.
Op het moment van eerste registratie informeert ArboUnie de medewerker over de verwerking van zijn persoonsgegevens door ArboUnie. Die informatie houdt in ieder geval in het doel waarvoor ArboUnie de persoonsgegevens verwerkt.

ArboUnie verwerkt de persoonsgegevens overeenkomstig de Algemene Verordening Gegevensbescherming (AVG).
ArboUnie neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens die worden verwerkt te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze beveiligingsmaatregelen garanderen een passend beveiligingsniveau gelet op de verwerking van persoonsgegevens.
De toereikendheid van de informatiebeveiliging blijkt uit:
(nog nader in te vullen, bijvoorbeeld:
- Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II)
- ISO certificering)

ArboUnie is verantwoordelijk voor de afhandeling van beveiligingsincidenten waarbij persoonsgegevens verloren gaan of onrechtmatig worden verwerkt (datalek). Als een datalek, of een vermoeden van een datalek de persoonsgegevens van medewerkers van de gemeente Veere betreft dan informeert ArboUnie de gemeente Veere hierover direct.

Collegeadvies:

Uitvoering
Privacy
De papiercontainers bevatten een chip die gekoppeld is aan het betreffende adres. Met de chip wordt het type container herkend en wordt het aantal en het tijdstip van de ledigingen geregistreerd. Deze informatie is nodig voor een efficiënte bedrijfsvoering. Afhankelijk van het aanbod kan de ophaalfrequentie aangepast worden.
Door het adres zijn de gegevens herleidbaar naar een persoon waardoor er sprake is van een nieuwe verwerking van persoonsgegevens. In de flyer die wordt verspreid worden de betrokkenen hierover geïnformeerd. De verwerking wordt ook opgenomen in het verwerkingenregister.
Omdat de ZRD de registratie van de ledigingen bijhoudt is de ZRD hierdoor een verwerker van de persoonsgegevens. Hiervoor wordt met de ZRD een verwerkersovereenkomst afgesloten. De privacy officer onderneemt hiervoor de nodige acties.

Flyer:

Privacy
De papiercontainer bevat een chip die gekoppeld is aan uw adres. Met de chip wordt het type container herkend en wordt het aantal en het tijdstip van de ledigingen geregistreerd. Deze informatie is nodig voor een efficiënte bedrijfsvoering.
Uw privacy is gewaarborgd! De gemeente Veere houdt zich aan de regels van de privacywetgeving. Meer informatie hierover vindt u op www.veere.nl/privacy

Bijlage 5

Technische en organisatorische maatregelen van het MT

Het MT-besluit is opgenomen in Corsa onder nummer 17B.04464

Bijlage 6

Beheer van informatiebeveiligingsincidenten

Het document "Beheer van informatiebeveiligingsincidenten (inclusief meldplicht datalekken) is opgenomen in Corsa onder nummer 16B.00120