GEMEENTE VEERE

Privacybeleid gemeente Veere

Domburg, mei 2022
Versie 1.1
21B.10132

Inhoud

Wat is er gewijzigd?

Versie 1.0 van het gemeentelijk privacybeleid is vastgesteld in mei 2018. In versie 1.1 is de opmaak aangepast door in de tekst bijzonderheden en voorbeelden in zogenaamde tekstballonnen op te nemen. Ook zijn wat afbeeldingen toegevoegd om het geheel wat levendiger te maken.

De belangrijkste inhoudelijke wijziging is de expliciete benoeming van de gemeenteraad als verwerkingsverantwoordelijke. In de eerste versie van het gemeentelijke privacybeleid was de gemeenteraad wel benoemd maar niet vanuit de rol als verwerkingsverantwoordelijke. Inmiddels is het duidelijk dat de gemeenteraad zelfstandig verwerkingsverantwoordelijke is voor een aantal verwerkingen. Omdat het college van burgemeester en wethouders beter geëquipeerd is, voert het college de operationele privacy taken ook voor de gemeenteraad uit.

Verder zijn in versie 1.1 een aantal onderwerpen verder toegelicht, uitgebreid of aangescherpt. Zo is bijvoorbeeld in paragraaf 4.10.1.2.2.4 opgenomen dat de voorzitter van de raads- of commissievergadering er op toe ziet dat insprekers niet over personen spreken. En raads- en commissieleden stellen geen vragen aan insprekers over personen.
Ook is opgenomen dat ook de gegevens die vallen onder de Wet politiegegevens binnen de scope van het gemeentelijk privacybeleid vallen en dat de Functionaris Gegevensbescherming daar toezicht op houdt.

Verder spreekt het privacybeleid nog steeds voor zich. Het geeft aan hoe de gemeente Veere uitvoering geeft aan de Algemene Verordening Gegevensbescherming en dat de gemeente Veere in al haar geledingen zorgt voor een goede bescherming van de aan haar toevertrouwde persoonsgegevens.

Mei 2022

Samenvatting

Tegelijkertijd met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) in mei 2018, is het gemeentelijk Privacybeleid vastgesteld. In ruim 3 jaar is gebleken dat het belang van en de aandacht voor privacy onveranderd groot is, het is misschien zelfs nog wel toegenomen.
Datalekken en gijzelsoftware bij grote bedrijven laten de kwetsbaarheid zien als persoonsgegevens in verkeerde handen komen of niet meer bereikbaar zijn. Ook grote gebeurtenissen zoals de coronapandemie grijpen diep in in de persoonlijke levenssfeer van mensen. Privacyschending ligt dan op de loer of tenminste bestaat het gevoel dat de privacy mogelijk geschonden wordt.

De juiste naleving van de privacyregels is dus onverminderd belangrijk. De AVG is hiervoor het belangrijkste wettelijk kader. Voor de uitvoering hiervan in onze eigen gemeentelijke organisatie is het gemeentelijk Privacybeleid het document waarin is vastgelegd 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

Ieder gemeentelijk bestuursorgaan is formeel verantwoordelijk voor de verwerking van persoonsgegevens, ieder voor zijn afzonderlijke specifieke (wettelijke) taken.
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 wenselijk dat er een portefeuillehouder privacy is. Deze bestuurder, in casu de burgemeester, is het aanspreekpunt voor en namens alle bestuursorganen, de organisatie, de politiek, burgers, media en de functionaris voor de gegevensbescherming (FG) voor 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 en moet er een FG aangesteld zijn. 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 een uitgangspunt van 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, de UAVG, de WPG en het Privacybeleid zijn hiervoor de norm. De FG is voor iedereen bereikbaar via FG@Veere.nl

Dit is de tweede versie van het Privacybeleid. Door nieuwe inzichten, veranderende omstandigheden en jurisprudentie is het van belang om minimaal iedere twee jaar het Privacybeleid te actualiseren.

1. Inleiding

De aandacht voor privacy is groot. Iedereen heeft er ook in meer of mindere mate mee te maken. Iedereen heeft er ook wel een beetje 'verstand' van of denkt dat in ieder geval te hebben. Soms wordt privacy ervaren als een zegen, omdat we de zekerheid hebben dat onze persoonsgegevens niet zomaar voor allerlei doeleinden worden gebruikt. Maar soms ervaren we het ook als een last, bijvoorbeeld als een foto niet gebruikt mag worden of als we eindeloos cookie-meldingen moeten wegklikken.
Ook binnen de organisatie van de gemeente Veere is de belangstelling en de aandacht voor privacy verschillend. 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, eigendom, 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. Voorheen was het de Wet bescherming persoonsgegevens (Wbp) die het mogelijk maakte om voor bepaalde doeleinden persoonsgegevens te verwerken. Per 25 mei 2018 is 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.

Een ander voorbeeld van een wet die bepaalde privacyrechten doorbreekt is de Coronawet. Op basis van deze wet kunnen/konden we worden beperkt in het recht om te gaan en te staan waar en wanneer we willen, denk daarbij aan de avondklok en de beperkingen om elkaar te kunnen ontmoeten. Ook de invoering van de CoronaCheck-app betekent een beperking van onze vrijheid. Er is dus wetgeving nodig om dat mogelijk te maken.

Regelgeving omtrent bescherming van persoonsgegevens is 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 heeft dus 16 jaar bestaan. 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 in de AVG is wel dat er meer aandacht is voor governance, compliance en met name 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.

De overtreder van de privacyregels riskeert een boete van de toezichthoudende autoriteit. Afhankelijk van de overtreding kan die boete oplopen tot maximaal € 20 miljoen. Voor de gemeente Veere is dat echter niet de doorslaggevende reden om de aandacht aan privacy te schenken. Bescherming van persoonsgegevens doen we niet omdat het moet maar omdat het kan en omdat we het willen! Een goede basis om dit waar te maken is het vaststellen van de uitgangspunten die we hiervoor in de gemeente Veere hanteren.

De AVG beantwoordt de vraag of een organisatie persoonsgegevens mag verwerken, en geeft, als dat mag, het kader voor de verplichtingen die dat met zich meebrengt en welke rechten de betrokkenen in dat geval hebben.

De concrete uitwerking van hoe dat in de gemeente Veere wordt toegepast is beschreven in dit Privacybeleid.

Hiermee bereiken we de volgende doelen:
- het Privacybeleid 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, en
- 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 2022

2. Visie

Persoonsgegevens zijn de olie en vaak zelfs de brandstof voor de motor van de maatschappij. Zonder persoonsgegevens geen identiteit, en zonder identiteit kan de hedendaagse 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 burgers eigenlijk geen keuze 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. Dit is samengevat in het uitgangspunt: **privacy first!**

De geldende privacywetgeving in combinatie met het Privacybeleid gemeente Veere vormt 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, er gezocht moet worden naar een evenwichtige oplossing. Concreet betekent dit dat er altijd eerst maatregelen moeten worden getroffen die de bescherming van de persoonsgegevens voldoende waarborgen voordat uitvoering kan worden gegeven aan het behalen van het organisatiedoel.
Er is vanaf de invoering van het privacybeleid de nodige aandacht besteed aan dit uitgangspunt. Daardoor is de basis goed, maar aandacht, controle en volharding zijn nodig om een goed niveau van bescherming van persoonsgegevens te bereiken en te 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.
Ieder bestuursorgaan van de gemeente Veere is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens voor zijn of haar taken. In de praktijk is het college van burgemeester en wethouders de verantwoordelijke voor verreweg de meeste verwerkingen van persoonsgegevens binnen de gemeente Veere. Om die reden is het college van burgemeester en wethouders ook de initiator voor het opstellen van dit gemeentelijk privacybeleid. De gemeenteraad heeft in juni 2021 besloten om zich te conformeren aan dit privacybeleid. De operationele privacy taken heeft de gemeenteraad om praktische redenen overgedragen aan het college van burgemeester en wethouders. De burgemeester heeft als bestuursorgaan ook een aantal zelfstandige wettelijke taken waarbij persoonsgegevens worden verwerkt. Het is vanzelfsprekend dat de burgemeester als lid van het college zich ook voor zijn eigen taken conformeert aan het gemeentelijk privacybeleid. Ook voor de verwerking van persoonsgegevens door andere (incidentele) bestuursorganen van de gemeente Veere, zoals de heffingsambtenaar, de invorderingsambtenaar, de ambtenaar van de burgerlijke stand, de rekenkamer, de commissie bezwaar en beroepschriften is het gemeentelijk privacybeleid van toepassing.

De gemeenteraad beschikt niet over voldoende capaciteit en/of kennis om de praktische privacy taken uit te voeren. Denk daarbij aan het behandelen van een verzoek om inzage of het afhandelen van een datalek. Hiervoor is het zeer efficiënt om gebruik te maken van de kennis en kunde van de ambtelijke organisatie van het college van burgemeester en wethouders, zonder dat afbreuk wordt gedaan aan de zelfstandige rol van de gemeenteraad.

De heffingsambtenaar kan als bestuursorgaan ook te maken krijgen met een verzoek om inzage of een Woo-verzoek. Bij de behandeling daarvan houdt de heffingsambtenaar zich aan het gemeentelijk privacybeleid.

3.2 Portefeuillehouder Privacy

Uit de beschreven visie blijkt dat de bescherming van persoonsgegevens een belangrijk 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 daarom ondergebracht bij één portefeuillehouder. Omdat privacy nauwelijks politieke aspecten kent en relevant is voor alle beleidsterreinen is het goed om de burgemeester als vaste portefeuillehouder Privacy

aan te wijzen. Deze bestendige rol komt ook de relatie en het constructieve overleg met de toezichthouder ten goede.
De portefeuillehouder Privacy is bestuurlijk verantwoordelijk en het aanspreekpunt voor het onderwerp Privacy, zowel intern als extern. 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 deskundig 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 privacy bewustzijn 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.

Vanaf de start van de AVG wordt de rol van FG ingevuld door een externe deskundige. Dat is zeer succesvol gebleken en wordt om die reden ook voortgezet. De inzet van een externe deskundige benadrukt de onafhankelijkheid van de FG, en de inzet van de FG is op die manier ook enigszins flexibel. Uitgangspunt is een urenbesteding van 120 uur per jaar.
De gemeente Veere hecht veel waarde aan de bekendheid van de FG met en in de organisatie en we zetten in op een duurzame relatie met de FG.

In de AVG zijn de volgende taken van de FG 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. Adviezen van FG kunnen door het bestuursorgaan alleen onderbouwd worden afgewezen.

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 houdt toezicht op 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 (in goed Nederlands een gegevensbeschermingseffectbeoordeling genoemd) wordt uitgevoerd. De FG ziet er op toe dat de DPIA's worden uitgevoerd en beoordeelt de uitkomst en geeft advies over de uitvoering 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 haar 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 haar advies niet of niet voldoende worden opgelost.

Voor haar informatie-, advies en toezichttaak heeft de FG periodiek overleg (minimaal 1x per half jaar) met de portefeuillehouder Privacy. Op basis van dit overleg doet de FG daarna verslag aan de verwerkingsverantwoordelijken, respectievelijk het college van B&W en de gemeenteraad.

De FG is bij de Autoriteit Persoonsgegevens aangemeld als FG van de gemeente Veere. Formeel moet ieder bestuursorgaan als verwerkingsverantwoordelijke een FG aanstellen. Het college van burgemeester en wethouders en de gemeenteraad hebben dat expliciet gedaan. Voor de overige bestuursorganen geldt deze aanstelling impliciet door de brede aanmelding bij de AP.
Naast de AVG valt ook de Wet Politiegegevens (WPG) binnen de scope van de FG.

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 zij zich niet met de dagelijkse uitvoerende privacywerkzaamheden bezighouden. Deze taken zijn daarom strikt 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 praktische eerstelijns aanspreekpunt is voor alle privacyvraagstukken. Uiteraard blijft ook voor de organisatie de mogelijkheid bestaan om zich direct tot de FG te wenden.

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 samen met taakverantwoordelijke binnen de organisatie 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. In overleg met de FG beoordelen van datalekken en deze zo nodig melden bij de AP en de betrokkene;
i. Bijhouden van het verwerkingenregister en het datalekregister;
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 jaar wordt dit onderwerp besproken in aanwezigheid van de FG.

3.6 Rol werkgroep Informatiebeveiliging

De werkgroep Informatiebeveiliging (werkgroep IB) bestaat uit de beveiligingsfunctionaris, de Ciso, de integriteitscoördinator en de PO.
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. Hier wordt ook de FG bij betrokken.

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.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

Bijzonder persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
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 de wettelijke vertegenwoordiger(s).

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Een samenhangend geheel aan bewerkingen vormt een bewerking, maar ook de afzonderlijke delen zijn verwerkingen die moeten voldoen aan de AVG.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
Wie bepaalt de functionele en operationele activiteiten?
Ieder bestuursorgaan van de gemeente Veere is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens voor zijn of haar 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.

*Verwerkersovereenkoms*t: Als de verwerkingsverantwoordelijke een verwerker inschakelt dan moet er altijd een verwerkersovereenkomst afgesloten worden. Deze overeenkomst bevat met name bepalingen t.a.v. de bescherming en beveiliging van de persoonsgegevens.

4.2 Verwerkingenregister

De AVG schrijft voor dat de verwerkingsverantwoordelijke een register bijhoudt van alle verwerkingsactiviteiten. Vanuit praktische overwegingen en om redenen van beheersbaarheid, is binnen de gemeente Veere gekozen om dit te doen door het clusteren van verwerkingsactiviteiten. De verwerkingsactiviteiten die met elkaar één verwerkingsdoel vormen zijn als één verwerking geregistreerd. Het verwerkingsdoel bepaalt dus de registratie in het verwerkingenregister. Zo bestaat bijvoorbeeld het verwerkingsdoel Omgevingsvergunningen uit verschillende verwerkingsactiviteiten. Deze activiteiten worden in het verwerkingenregister bij de verwerking Omgevingsvergunningen beschreven.

Voor het verwerkingenregister wordt gebruik gemaakt van een speciaal daarvoor ingerichte applicatie. 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 informatiewaarde van het verwerkingenregister vergroten. Een voorbeeld van een verwerking in het verwerkingenregister is opgenomen in bijlage 1.
In verband met het uitoefenen van de rechten van betrokkenen is in ieder geval als aanvullend gegeven “de wijze van informeren van de betrokkene” in het register opgenomen.
Het verwerkingenregister wordt periodiek (minimaal 1x per 2 jaar) gecontroleerd op volledigheid en actualiteit. Tussentijds gemelde wijzigingen worden direct verwerkt.

4.3 Verwerkersovereenkomst

Wanneer een bestuursorgaan van de gemeente een opdracht verstrekt aan een organisatie of onderneming die niet onder direct gezag staat van de gemeente Veere en 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 aan de verwerker het standaardmodel aan, zoals opgenomen in bijlage 2. Dit model is gebaseerd op het

standaard model van de Informatiebeveiligingsdienst voor gemeenten (IBD). Relevante wijzigingen in het IBD-model worden overgenomen in het gemeentelijk model.
Het voordeel van standaardisatie is dat het zeker is dat in al onze verwerkersovereenkomsten de noodzakelijke onderwerpen op dezelfde wijze zijn opgenomen. Dit vereenvoudigd de controle en het toezicht. Alleen in uitzonderlijke gevallen wordt afgeweken van het standaard 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 komen de privacy risico's naar voren op basis waarvan passende maatregelen kunnen worden genomen. Het kan ook betekenen dat vanwege de privacy risico's de voorgestelde verwerking van persoonsgegevens niet uitgevoerd kan worden.

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 heeft een lijst opgesteld met verwerkingen waarvoor een DPIA verplicht is, maar deze lijst is niet uitputtend. De afweging voor het wel of niet uitvoeren van een DPIA (los van de verplichte verwerkingen) ligt nadrukkelijk bij de verwerkingsverantwoordelijke.

Voor de bestaande verwerkingen in de gemeente Veere waarbij bijzondere persoonsgegevens worden verwerkt wordt periodiek een DPIA uitgevoerd.
Verder wordt een DPIA uitgevoerd voor de verwerkingen waarvoor dit door de FG wordt geadviseerd.

In 2019 is een DPIA uitgevoerd op de verwerking van persoonsgegevens door Porthos. De uitkomsten daarvan zijn ook gebruikt voor risico beperkende maatregelen voor de Nieuwe Toegang Wmo/Jeugd.
Andere in het oog springende DPIA's zijn die voor de inzet van bodycams door de BOA's en het invoeren van het nieuwe vergunningparkeren.

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.

4.4.1 Risico's bij de verwerking van persoonsgegevens

De AVG schrijft voor dat de verwerkingsverantwoordelijke adequate en passende maatregelen neemt om de risico's van het verwerken van persoonsgegevens te voorkomen of te beperken.
Het risico bestaat uit de ongewenste gevolgen van zowel de rechtmatige als de onrechtmatige verwerking van persoonsgegevens. De kans op en de schade van die gevolgen bepalen de hoogte van het risico. Hoe hoger het risico, hoe hoger de eisen aan de maatregelen ter beveiliging.

Zowel de betrokkene als de organisatie kan schade oplopen door het (on)rechtmatig verwerken van persoonsgegevens. De ernst van die schade is van diverse factoren afhankelijk en kan o.a. bestaan uit imagoschade, identiteitsfraude, financiële benadeling, fysieke schade en/of (levens)bedreiging.

De risico's bij de verwerking van persoonsgegevens zijn in te delen in 4 klassen:

- *Risicoklasse 0; publiek niveau*.
Dit betreft persoonsgegevens die in principe algemeen bekend en toegankelijk zijn, vergelijkbaar met het telefoonboek. Voor deze gegevens geldt de normale zorgvuldigheid zoals de cleandesk policy en het gebouw afsluiten na kantoortijd. Iedere medewerker heeft toegang tot deze gegevens.

- *Risicoklasse 1; basis niveau.*
Dit betreft persoonsgegevens die door de context en de omvang een meer specifiek karakter hebben en in de regel alleen bekend zijn bij de betrokkene en de organisatie die de persoonsgegevens verwerkt. Vergelijkbaar met een klantenbestand van de plaatselijke supermarkt met daarin de naw-gegevens van de klant en de producten die hij/zij koopt. Voor deze gegevens geldt een gemiddelde zorgvuldigheid waarbij de persoonsgegevens in een afgesloten omgeving worden opgeborgen. De digitale inlog is voor meerdere mensen beschikbaar, er is vertrouwen dat iedereen de nodige zorgvuldigheid in acht neemt.

- *Risicoklasse 2; verhoogd risico.*
Dit betreft persoonsgegevens die door de context, de omvang en de gevoeligheid een ander karakter hebben. Er zijn veel gegevens over de persoon bekend en er is sprake van bijzondere persoonsgegevens, zoals gezondheid, geaardheid, politieke voorkeur, geloofsovertuiging, etc.
Vergelijkbaar met het klantenbestand van een zorgverlener met daarin veel directe persoonsgegevens en gegevens over ziekten en aandoeningen. Voor deze gegevens geldt een hoge zorgvuldigheid waarbij de persoonsgegevens voortdurend achter slot en grendel zitten en alleen door geautoriseerde personen verwerkt worden.

- *Risicoklasse 3; hoog risico.*
Dit betreft persoonsgegevens die door de context, de omvang, de hoge gevoeligheid en de verbanden met andere verwerkingen met een verhoogd of hoog risico, een zeer uitzonderlijk karakter hebben. Er zijn veel gegevens over de persoon bekend, er is sprake van bijzondere persoonsgegevens en door de verbanden met andere verwerkingen is een uitgebreid profiel van de betrokkene te maken.
Vergelijkbaar met de administratie van de belastingdienst met daarin veel directe persoonsgegevens van de betrokkene en gerelateerde, financiële gegevens, eigendomsgegevens, medische gegevens, etc. Voor deze gegevens geldt een zeer hoge zorgvuldigheid waarbij de persoonsgegevens voortdurend achter slot en grendel zitten, alleen door geautoriseerde personen verwerkt worden en waarvoor een bijzondere geheimhoudingsplicht geldt.

De maatregelen ter beveiliging van de persoonsgegevens zijn afgestemd op de risicoprofielen.

Als er sprake is van een inbreuk in verband met persoonsgegevens (datalek) dan wordt op basis van de risicoklasse bepaald of het datalek gemeld wordt bij de Autoriteit Persoonsgegevens (AP) en/of bij de betrokkene. Zie hiervoor paragraaf 4.9.

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. Al tijdens het ontwerp van bijvoorbeeld nieuwe diensten wordt er 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. Dat voorkomt problemen bij de implementatie en zorgt ervoor dat privacy al vanaf de teken- of beleidstafel wordt meegenomen.
Het verantwoordelijk afdelingshoofd, de adviseur informatiebeleid, de systeembeheerder en de inkoopadviseur hebben hierbij een belangrijke initiële taak.

Privacy by default houdt kort gezegd 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 bijvoorbeeld 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.
De grondslag toestemming kan wel aan de orde zijn in het kader van zorg- en hulpverlening waarbij de betrokkenen zelf geen verzoek doet maar professionals zorg of hulp toch noodzakelijk achten. In een dergelijk geval is toestemming nodig van de betrokkene het gaat immers om een inmenging in de persoonlijke levenssfeer.
Voor het verwerken van persoonsgegevens op basis van toestemming wordt binnen de gemeente Veere grote terughoudendheid betracht. Voor een dergelijke verwerking wordt vooraf altijd 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 daarom kan toestemming doorgaans 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 gegeven. 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.

Drang en dwang
In het Sociaal Domein komen soms situaties voor waarbij een persoon geen beroep doet op de inzet van zorg of ondersteuning terwijl die inzet wel noodzakelijk is. Als een bevoegde autoriteit of professional binnen de wettelijke kaders vaststelt dat het vanwege een vitaal belang van de betrokkene of zijn omgeving noodzakelijk is dat zorg of ondersteuning wordt ingezet dan kunnen de persoonsgegevens ook zonder toestemming van de betrokkene verwerkt worden. Zodra dit kan en verantwoord is wordt de betrokkene geïnformeerd over de verwerking van de persoonsgegevens en over zijn of haar privacyrechten.

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. Die transparantie is nodig zodat de betrokkene gebruik kan maken van de rechten die de AVG toekent (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. Deze zogenaamde privacyrechten zijn opgenomen in de privacyverklaring van de gemeente Veere.

4.7.1 HET RECHT OM GEÏNFORMEERD TE WORDEN

Het recht om geïnformeerd te worden volgt uit de verplichting van de verwerkingsverantwoordelijke om betrokkenen actief te informeren over de verwerkingen die uitgevoerd gaan worden.
Op het moment dat de persoonsgegevens in een verwerking worden opgenomen moet de betrokkene hierover dus 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 dat de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar de privacyverklaring 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 dat de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacyverklaring 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 dat de persoonsgegevens worden verwerkt en dat de gegevens overeenkomstig de AVG worden verwerkt. Daarbij wordt verwezen naar het privacyverklaring 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 privacyverklaring 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 teksten die gebruikt kunnen worden voor het informeren van de betrokkenen.
In het verwerkingenregister is 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 4.7.1.1 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 privacyverklaring 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 privacyverklaring en het privacybeleid op de website van de gemeente Veere.

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

4.7.1.3 Uitzonderingen op de informatieplicht

Op grond van de AVG kan de informatie achterwege blijven als de betrokkene al over de informatie beschikt. Bij het toepassen van deze uitzondering moet het in alle gevallen 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/haar 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 is gemotiveerd opgenomen of er sprake is van een uitzondering op de informatieplicht en op welke grond.

Als het verwerken van persoonsgegevens in grote mate voorspelbaar is bij het uitvoeren van de publieke taken door de gemeente, dan kan het actief informeren achterwege blijven. Bij twijfel wel altijd informeren.
Bij bijvoorbeeld het aanvragen van een stookontheffing is het zeer voorspelbaar dat de persoonsgegevens van de aanvrager worden verwerkt. Actieve informatie is dan niet nodig. Omdat in e-mail en ontvangstbevestigingen wordt gewezen op de privacyverklaring op de website, wordt de betrokkene toch gewezen op zijn privacy rechten.

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.

Uit jurisprudentie blijkt dat met een kopie niet een letterlijke kopie van de gegevens wordt bedoeld. Als dat nuttig is kan het wel een letterlijke kopie zijn, maar het kan ook een samengesteld overzicht zijn.

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 taak van algemeen belang of in het kader van openbaar gezag, 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 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 niet in behandeling genomen.

Toelichting bij d.
De gemeente verwerkt veel persoonsgegevens in diverse registraties. Op basis van de AVG moet bij een inzageverzoek inzage verleend worden in alle persoonsgegevens. Bij een algemeen, niet gespecificeerd verzoek betekent dat dat alle registraties, inclusief alle documenten, e-mails, etc. doorzocht moeten worden op het voorkomen van de persoonsgegevens. Het is zeer waarschijnlijk onmogelijk om bij een dergelijk verzoek volledig te zijn, maar in ieder geval is het een zeer tijdrovende en kostbare zoektocht. Een niet gespecificeerd verzoek vergt daardoor een onevenredige inspanning van de gemeente.

In overweging 63 bij de AVG is het volgende opgenomen: “Wanneer de verwerkingsverantwoordelijke een grote hoeveelheid gegevens betreffende de betrokkene verwerkt, moet hij de betrokkene voorafgaand aan de informatieverstrekking kunnen verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.”
In die zin biedt de AVG wel de ruimte om te vragen om een specificering van het inzageverzoek. Een soortgelijk uitgangspunt bestond ook onder de Wbp.
In de jurisprudentie is dit bekend onder de term ‘fishing expedition’, een algemeen en niet nader onderbouwd verzoek. Om te voorkomen dat de verwerkingsverantwoordelijke grote hoeveelheden bestanden en documenten moet doornemen mag de verwerkingsverantwoordelijke in een dergelijk geval om verduidelijking van het verzoek vragen.

e. Als na het verzoek van de verantwoordelijke de betrokkene zijn belang niet voldoende specifiek heeft gemaakt, wordt het verzoek niet in behandeling genomen.
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 Overheid (BIO). Het voldoen aan de BIO 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 BIO.
Jaarlijks wordt het voldoen aan de BIO 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. De Gegevensmakelaar is software die garandeert dat het gebruik van persoonsgegevens zoals die in de diverse authentieke registraties zijn opgenomen de basis vormt. 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.

Een van de pijlers van de AVG die van grote waarde is bij o.a. het beveiligen van persoonsgegevens, is dat de persoonsgegevens niet langer worden 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 eveneens rekening gehouden met de bewaartermijn.
Het MT neemt maatregelen die ervoor zorgen dat bestanden met persoonsgegevens buiten taakspecifieke applicaties (outlook, 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.

4.8.1 Informatietransport

De BIO bepaalt dat voor de bescherming van het informatietransport, via alle soorten communicatiefaciliteiten, regels, procedures en beheersmaatregelen zijn vastgesteld. In het gemeentelijk informatiebeleid zijn deze regels, procedures en beheersmaatregelen opgenomen. In aanvulling hierop geldt dat voor het transporteren van persoonsgegevens uitsluitend gebruik wordt gemaakt van transportmiddelen die in beheer en onder controle zijn van de gemeente (zoals een taakspecifieke digitale netwerkverbinding, e-mail en fysieke post).

Voorbeeld
Een beschikking wordt verstuurd via de normale fysieke post, via de berichtenbox op MijnOverheid of via MijnVeere op de gemeentelijke website.
Een afspraak voor een huwelijk wordt ingediend via het Klantportaal op de gemeentelijke website.
Een Wmo-ondersteuningsplan wordt via een beveiligde e-mail (bijvoorbeeld Zorgmail) naar de klant gestuurd. De klant kan het getekende ondersteuningsplan terugsturen via de uploadservice op de gemeentelijke website.

Whatsapp, Facebook en andere social media wordt alleen gebruikt voor algemene en anonieme informatie.

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 veel voorkomend datalek is het versturen van een e-mail naar een verkeerd e-mailadres. Door een verkeerde keuze in het adresboek wordt de e-mail naar een verkeerde persoon gestuurd.
Dit type datalek is lastig te voorkomen omdat het gaat om een menselijke fouten die nu eenmaal gebeuren. Met de inzet van diverse instrumenten wordt ingezet op het zoveel mogelijk voorkomen van deze fouten en het veilig verzenden van email.
Door directe terugkoppeling, instructies, berichten op Intranet, etc. brengen we dit steeds onder de aandacht. Technische hulpmiddelen zijn het gebruik van Zorgmail en automatische waarschuwingen bij het versturen van gevoelige gegevens. Daarnaast wordt elk datalek uiteraard individueel beoordeeld en teruggekoppeld in het kader van lessons learned.

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.

Een datalek waarbij naw-gegevens, geboortedatum, bsn en bankrekening zijn gelekt veroorzaakt een aanzienlijke kans op identiteitsfraude. De betrokkene moet hierover geïnformeerd worden zodat hij maatregelen kan treffen om fraude te voorkomen of daar in ieder geval alert op te zijn.

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

In deze procedure is beschreven welke functionarissen verantwoordelijk en betrokken zijn bij een beveiligingsincident.
Op basis van de risicoklasse (zie paragraaf 4.4.1) en de specifieke omstandigheden van het geval wordt bepaald of het datalek gemeld wordt bij de Autoriteit Persoonsgegevens (AP) en/of bij de betrokkene.

4.10 Openbaar maken informatie (Woo)

De gemeente verzamelt, gebruikt en beheert informatie die in bepaalde gevallen ook openbaar gemaakt wordt. Als deze informatie persoonsgegevens bevat 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 de benoeming van een raadslid) 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 verstrekking van de informatie niet geweigerd worden.

Als de eerdere openbaarmaking berust op een fout dan moet die fout niet herhaald worden. Het probleem hierbij is dat veel openbaarmakingen digitaal gebeuren (Internet), en het is onmogelijk om alle digitale sporen te wissen. In die zin heeft eenmaal openbaar, altijd openbaar ook een praktische (negatieve) betekenis.

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

Hoofdstuk 3 van de Wet open overheid (Woo), voorheen de Wet openbaarheid van bestuur (Wob), verplicht het bestuursorgaan dat het rechtstreeks aangaat om uit eigen beweging de bij het bestuursorgaan berustende informatie neergelegd in documenten voor eenieder openbaar te maken.

Dit hoofdstuk in de Woo 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 hoofdstuk 5 van de Woo, tenzij hiervoor in de betreffende bijzondere wetten specifieke aanwijzingen zijn gegeven. Ook de Bekendmakingswet houdt rekening met artikel 5.1 van de Woo.

Bekendmakingswet
Op 1 juli 2021 is de Wet Elektronische Publicaties (WEP) in werking getreden. De WEP is een wijziging van de Bekendmakingswet en tal van andere wetten waarin terinzagelegging en publicatie is voorgeschreven. Alle bekendmakingen moeten nu in het elektronisch Gemeenteblad worden opgenomen.

De Bekendmakingswet bepaalt dat bij de bekendmakingen rekening wordt gehouden met artikel 5.1 van de Woo. Concreet betekent dit dat in bekendmakingen geen persoonsgegevens opgenomen mogen worden. Alleen in het uitzonderlijke geval dat er een aantoonbaar belang is dat zwaarder weegt dan de privacy van de betrokkene mogen de persoonsgegevens openbaar gemaakt worden.
Dat betekent ook dat alle documenten die bekendgemaakt moeten worden geanonimiseerd moeten zijn. Alle informatie die te herleiden is naar een persoon moet in het document onleesbaar worden gemaakt. Dat kan dus meer zijn dan alleen naam, adres en woonplaats. Soms bevat een document zoveel directe en indirecte persoonsgegevens dat het document helemaal niet openbaar gemaakt kan worden.

Om veel werk te voorkomen is de organisatie geïnstrueerd om alle adviezen en besluiten zo anoniem mogelijk op te stellen: "*Noem éénmaal de naam van de betrokkene en schrijf daarna over de aanvrager, indiener, bezwaarmaker, vergunninghouder, betrokkene, klager, o.i.d. Als een dergelijk document gepubliceerd moet worden dan hoef je maar op één plaats de persoonsgegevens onleesbaar te maken. Het format voor het B&W-advies is hierop ingericht.*
Indieners van zienswijzen kan verzocht worden om ook een geanonimiseerd document in te leveren. Van professionele partijen mag verwacht worden dat ze niet onnodig persoonsgegevens in documenten opnemen. Zo nodig is het goed om ze daar nog eens op te wijzen."

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. Fysieke inzage kan om deze reden alleen op afspraak, de documenten moeten dan vooraf geanonimiseerd worden.

Zodra het E-depot van het Zeeuws Archief operationeel is kunnen burgers de technische gegevens uit de bouwdossiers raadplegen. Aanvraagformulieren en andere documenten met persoonsgegevens zijn daarin niet zichtbaar.
Het komt voor dat bij de technische gegevens de naw-gegevens van de opdrachtgever zijn vermeld. In dat geval hanteren we het uitgangspunt dat het belang van de openbaarheid zwaarder weegt dan het belang van de bescherming van de persoonlijke levenssfeer (artikel 5.1, lid 2 aanhef en onder e. Woo). Met name omdat het privacy risico van deze gegevens erg laag is.

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 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 worden de vergaderstukken via het Raadsinformatiesysteem (RIS) ter beschikking gesteld. De ontsluiting hiervan voor de commissie- en raadsleden gebeurt door de griffier. Het RIS 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 mogen deze informatie niet met derden delen.

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 het RIS openbaar gemaakt. De videotulen maken ook deel uit van deze vergaderstukken. De vergaderstukken zijn raadpleegbaar via de agenda van de raadsvergadering op de website. 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 en waarbij het belang van de openbaarheid zwaarder weegt dan het belang van de bescherming van de persoonlijke levenssfeer.
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. Zo worden de namen van deze gezagsdragers niet uit de stukken verwijderd.

4.10.1.2.2.2 Ambtenaren

Ook 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, bedrijven en organisaties die mondeling of schriftelijk contact maken met de Gemeente Veere

Als in de vergaderstukken persoonsgegevens voorkomen van burgers, bedrijven en particuliere organisaties, die mondeling of schriftelijk contact hebben gemaakt met de gemeente (vraag, aanvraag, klacht, petitie, inspraak, zienswijze, 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.
De Lijst Ingekomen Stukken (LIS) bestaat uit een anonieme overzichtslijst met daarop de ontvangstdatum, het onderwerp en de afhandelingswijze van het ingezonden stuk. De ingezonden stukken zelf worden niet openbaar gemaakt. In de ontvangstbevestiging aan de betreffende indieners wordt gewezen op dit beleid en overige relevante privacyaspecten.
Als de betreffende stukken worden opgevraagd dan gelden daarvoor de regels van openbaarmaking.

4.10.1.2.2.4 Insprekers tijdens de openbare vergaderingen waarin inspraak geboden wordt

Burgers die inspreken tijdens een openbare vergadering waarin de mogelijkheid tot inspreken wordt geboden 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).

Insprekers krijgen vooraf de instructie dat ze in de spreekbeurt niet over personen mogen spreken; niet over mede-burgers en ook niet over medewerkers van de gemeente Veere. De voorzitter van de vergadering ziet daar op toe. Zo nodig worden de betreffende passages in de opnames gewist. Een bestuurder mag in zijn rol als bestuurder wel aangesproken worden. Raadsleden en commissieleden stellen ook geen vragen aan de insprekers over personen.

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

Hoofdstuk 4 van de Wet open overheid (Woo) verplicht het bestuursorgaan informatie te verstrekken op verzoek. Dit wordt doorgaans aangeduid als een Woo-verzoek, voorheen een Wob-verzoek.
Bij het beslissen op een Woo-verzoek wordt in alle gevallen rekening gehouden met de uitzonderingsgronden van hoofdstuk 5 van de Woo.

Artikel 5.1 lid 1 aanhef en onder d van de Woo 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 5.1 lid 2 aanhef en onder e. van de Woo 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 Woo-verzoek zonder uitdrukkelijk verzoek om verstrekking van persoonsgegevens

Als informatie wordt verstrekt op basis van een Woo-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 Woo-verzoek wordt hiervoor verwezen naar dit vaste beleid met als motivering de eerbiediging van de persoonlijke levenssfeer.

4.10.2.1.1 Belang van eerbiediging van de persoonlijke levenssfeer

Dit betreft persoonsgegevens van medewerkers van de gemeente Veere die betrokken zijn bij de behandeling van een procedure of proces en die in die hoedanigheid geen openbare functie bekleden.
De vermelding van deze persoonsgegevens heeft uitsluitend een externe communicatiefunctie voor de betrokkenen bij de procedure of het proces, of de persoonsgegevens hebben een interne functie om aan te geven wie de behandelaar van een procedure of proces is. Deze persoonsgegevens van medewerkers zijn niet van invloed op de inhoud van de informatie.
Openbaarmaking van deze persoonsgegevens is ongewenst omdat dit de betreffende medewerkers kan belemmeren in hun rol als gevraagd en ongevraagd adviseur van het bestuur. Medewerkers moeten in alle vrijheid hun beleidsopvattingen en adviezen kunnen geven. De wetenschap dat hun persoonsgegevens openbaar gemaakt worden kan hen daarin belemmeren. Medewerkers rekenen er ook op dat hun persoonsgegevens niet openbaar gemaakt worden. Dit uitgangspunt past bij en is in overeenstemming met de bedoeling van artikel 5.2 van de Woo.
Verder brengt openbaarmaking van persoonsgegevens van medewerkers het risico met zich mee dat misbruik van deze gegevens wordt gemaakt. Van de persoonsgegevens zelf of in combinatie met andere (persoons)gegevens. Dat kan zowel de werksfeer als de privésfeer betreffen. Het voorkomen en tegengaan van ondermijning speelt daarbij een belangrijke rol.

Persoonsgegevens van betrokkenen anders dan medewerkers van de gemeente Veere worden niet openbaar gemaakt tenzij deze gegevens nadrukkelijk van invloed zijn op de inhoud van de openbaar te maken informatie. In dat geval worden alleen de noodzakelijke persoonsgegevens openbaar gemaakt.
Als de persoonsgegevens niet van invloed zijn op de inhoud van de informatie, dan is openbaarmaking ondergeschikt aan het grondrecht eerbiediging van de persoonlijke levenssfeer.
Deze persoonsgegevens worden altijd openbaar gemaakt als de betrokkene daarvoor vooraf zijn specifieke en ondubbelzinnige toestemming heeft gegeven. De betrokkene moet weten en begrijpen dat éénmaal openbaar, altijd openbaar is.

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

Als de indiener van een Woo-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 Woo-verzoek wordt deze afweging van belangen gemotiveerd.

4.10.2.2.1 Belang van eerbiediging van de persoonlijke levenssfeer

In dit geval geldt voor de persoonsgegevens van medewerkers van de gemeente Veere dat deze niet openbaar worden gemaakt vanwege het belang zoals beschreven in 4.10.2.1.1.

Voor de persoonsgegevens van andere betrokkenen geldt dat deze gegevens alleen openbaar gemaakt worden als de gegevens nadrukkelijk van invloed zijn op de inhoud van de openbaar te maken informatie. Daarbij wordt rekening gehouden met het belang dat de indiener van een Woo-verzoek aangeeft.
Als de persoonsgegevens niet van invloed zijn op de inhoud van de informatie, dan is openbaarmaking ondergeschikt aan het grondrecht eerbiediging van de persoonlijke levenssfeer.
Deze persoonsgegevens worden altijd openbaar gemaakt als de betrokkene daarvoor vooraf zijn specifieke en ondubbelzinnige toestemming heeft gegeven. De betrokkene moet weten en begrijpen dat éénmaal openbaar, altijd openbaar is.

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

Als de indiener van een Woo-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 Woo-verzoek wordt hiervoor verwezen naar dit vaste beleid met als motivering de eerbiediging van de persoonlijke levenssfeer.

4.10.2.3.1 Belang van eerbiediging van de persoonlijke levenssfeer

In dit geval geldt voor de persoonsgegevens van medewerkers van de gemeente Veere dat deze niet openbaar worden gemaakt vanwege het belang zoals beschreven in 4.10.2.1.1.

Persoonsgegevens van betrokkenen anders dan medewerkers van de gemeente Veere worden niet openbaar gemaakt tenzij deze gegevens nadrukkelijk van invloed zijn op de inhoud van de openbaar te maken informatie. In dat geval worden alleen de noodzakelijke persoonsgegevens openbaar gemaakt.
Als de persoonsgegevens niet van invloed zijn op de inhoud van de informatie, dan is openbaarmaking ondergeschikt aan het grondrecht eerbiediging van de persoonlijke levenssfeer.
Deze persoonsgegevens worden altijd openbaar gemaakt als de betrokkene daarvoor vooraf zijn specifieke en ondubbelzinnige toestemming heeft gegeven. De betrokkene moet weten en begrijpen dat éénmaal openbaar, altijd openbaar is.

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 zoveel mogelijk 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, tenzij dit technisch vrijwel onmogelijk is of er zwaarwegende belangen zijn die het niet honoreren van het verzoek rechtvaardigen.
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 voor het verwerken van video- en fotobeelden

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 2022. 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. De beelden zijn politiegegevens en vallen onder de Wet politiegegevens. Het beheer en gebruik van de opnames is in handen van de politie.
In bijlage 7 is de te volgen procedure voor het inzetten van cameratoezicht opgenomen.

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 ze 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 via de rechter een beroep doen op het portretrecht.

Afbeelding: Een nieuwsfoto in het kader van de 'week van de zee'. Deze foto mag zonder toestemming gepubliceerd worden. Het verdient wel de voorkeur dat de fotograaf de gefotografeerde personen vraagt om toestemming. En t.a.v. kinderen moet sowieso altijd voorzichtigheid worden betracht.

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 vervaagd worden.

4.12 Delen van persoonsgegevens

Het verwerken van persoonsgegevens is noodzakelijk voor de uitvoering van de eigen taken van de gemeente. De rechtmatige grondslag voor het verwerken van persoonsgegevens is in de meeste gevallen het voldoen aan een wettelijke verplichting of de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (artikel 6, lid 1 onder c. en e. AVG). In een enkel geval worden de persoonsgegevens verwerkt op basis van een privaatrechtelijke overeenkomst (artikel 6, lid 1 onder b. AVG) of het behartigen van een gerechtvaardigd belang van de gemeente (artikel 6, lid 1 onder f. AVG). Sporadisch is de grondslag toestemming van de betrokkene van toepassing (artikel 6, lid 1 onder a.), zie hiervoor ook paragraaf 4.6.

De door de gemeente verzamelde persoonsgegevens zijn vaak ook nodig voor de uitvoering van de taken van en door andere organisaties. Op initiatief van de gemeente of op verzoek van de betreffende organisatie kunnen de persoonsgegevens gedeeld worden. De andere organisatie ontvangt dan persoonsgegevens van de gemeente om deze vervolgens zelfstandig te verwerken. De ontvangende organisatie is de verwerkingsverantwoordelijke voor de ontvangen persoonsgegevens.
De ontvangende organisatie is in deze situatie nadrukkelijk geen verwerker omdat de ontvangende organisatie zelf het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt.

Voorbeeld
De gemeente verstrekt salarisgegevens aan de Belastingdienst. Beide organisaties moeten voldoen aan een wettelijke verplichting en zijn ook beiden verwerkingsverantwoordelijke voor de eigen administraties.

Voorbeeld
De gemeente verstrekt klantgegevens aan de gecontracteerde leverancier van Wmo-hulpmiddelen. De gemeente moet voldoen aan een wettelijke verplichting en de leverancier vervult een taak van algemeen belang (leveren van toegekende zorg). Beide organisaties zijn verwerkingsverantwoordelijke voor de eigen administraties.

Voor het delen van persoonsgegevens gelden de volgende algemene uitgangspunten:
1. er is een rechtmatige grondslag om persoonsgegevens te delen;
2. de ontvangende organisatie heeft een rechtmatige grondslag om de te ontvangen persoonsgegevens te verwerken;
3. het delen van de persoonsgegevens past bij het doel waarvoor de gegevens zijn verzameld;
4. het delen van de persoonsgegevens is proportioneel, het middel staat in verhouding tot het doel;
5. het delen van de persoonsgegevens is nodig, het doel kan niet op een minder belastende manier bereikt worden.

4.12.1 Delen van persoonsgegevens op initiatief van de gemeente

Op basis van wet- en regelgeving heeft de gemeente de verplichting om in diverse situaties persoonsgegevens te delen met andere organisaties. Het staat dus op voorhand vast dat en met wie de persoonsgegevens gedeeld worden. In het verwerkingenregister wordt bij de betreffende verwerking vastgelegd met welke organisaties de persoonsgegevens gedeeld worden. Bij het voldoen aan de informatieplicht kan hiernaar verwezen worden.

Voor dit verplicht delen van persoonsgegevens zijn in de regel landelijke geautomatiseerde systemen ingericht die of verplicht gebruikt moeten worden zoals het BRP-berichtenverkeer voor het delen van opgenomen of gemuteerde gegevens in de Basis Registratie Personen; of waarvan het gebruik sterk wordt aanbevolen zoals het Gemeentelijk Gegevensknooppunt voor Wmo en Jeugdzaken.

Als voor het delen van persoonsgegevens geen geautomatiseerde systemen beschikbaar zijn, dan moet voor het delen een voldoende beveiligde manier gekozen worden. Zie hiervoor paragraaf 4.8.1.

4.12.2 Delen van persoonsgegevens op verzoek van een andere organisatie

Onder een andere organisatie wordt ook verstaan een afdeling of een medewerker van de gemeente Veere die niet verantwoordelijk is voor de betreffende verwerking van persoonsgegevens waaruit gegevens gedeeld worden.

Andere organisaties kunnen voor de uitvoering van hun taken incidenteel persoonsgegevens nodig hebben die door de gemeente worden verwerkt. Op basis van de AVG is deze gegevensdeling mogelijk. De algemene uitgangspunten zoals beschreven in paragraaf 4.12 zijn van toepassing.
Als dergelijke incidentele gegevensdelingen regelmatig terugkeren, dan kan overwogen worden om met deze organisatie afspraken te maken over actieve gegevensdeling. De gegevensdeling met deze organisatie wordt dan opgenomen in de betreffende verwerking in het verwerkingenregister.

Voorbeeld
De Stichting Welzijn Veere vraagt om de NAW-gegevens van de inwoners van 60 jaar en ouder om hen te attenderen op de diverse welzijnsactiviteiten voor ouderen.
Deze gegevensdeling is toegestaan omdat de gegevens uit de BRP o.a. zijn bedoeld voor de uitvoering van publieke taken van de gemeente.
De gemeente Veere heeft de taken op het gebied van jeugdwelzijnswerk en ouderenzorg uitbesteed aan de Stichting Welzijn Veere. SWV ontvangt hiervoor een subsidie van de gemeente. Voor het uitvoeren van de activiteiten zijn de NAW-gegevens nodig.

Als de gegevensdeling een ander doel heeft dan het doel waarvoor de gegevens zijn verzameld dan moet bij de afweging om de persoonsgegevens te delen, naast de

algemene uitgangspunten zoals beschreven in paragraaf 4.2, met het volgende rekening worden gehouden:

1. het verband tussen het doel waarvoor de persoonsgegevens zijn verzameld en het doel van de gegevensdeling;
2. de verhouding tussen de gemeente en de betrokkene;
3. de aard van de persoonsgegevens, is er sprake van bijzondere persoonsgegevens;
4. de mogelijke gevolgen van de gegevensdeling voor de betrokkene en
5. zijn er passende waarborgen mogelijk, zoals versleuteling en pseudonimisering.

Voorbeeld
De samenwerking Belastingen verstrekt op verzoek van de afdeling Openbare Ruimte de NAW-gegevens van de eigenaren van recreatiewoningen in een recreatiepark. De persoonsgegevens worden gebruikt om de eigenaren te informeren over geplande werkzaamheden in de straat.
Deze gegevensdeling is toegestaan omdat zowel de samenwerking Belastingen als de afdeling Openbare Ruimte de gegevens gebruiken om de eigenaren aan te schrijven voor een gemeentelijke aangelegenheid. De betrokkene verwacht dat de gemeente de betreffende gegevens kent en gebruikt. Er is geen sprake van bijzondere persoonsgegevens. De gegevensverstrekking heeft geen (nadelige) gevolgen voor de betrokkene.

Sociaal Domein
Gegevensdeling in het Sociaal Domein heeft steeds de aandacht. Er zijn vaak veel organisaties betrokken bij de uitvoering van de taken op dit terrein. Omdat er bijzondere persoonsgegevens en gevoelige (persoons)gegevens worden verwerkt, zijn de organisaties terecht voorzichtig met het delen van deze gegevens. Om duidelijkheid te geven over wat wel en niet mag t.a.v. gegevensdeling in het Sociaal Domein hebben de rijksoverheid en de VNG een aantal handreikingen en informatiedocumenten opgesteld. Op dit moment verdienen de volgende handreikingen aanbeveling:

- Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein
  Vindplaats: https://www.zorgenveiligheidshuizen.nl/doc/Handvat-Gegevensuitwisseling-ZVH-versie-2-3.pdf

- Handelingsprotocol Veilig Thuis 2019
  Vindplaats: https://vng.nl/publicaties/handelingsprotocol-veilig-thuis-2019

- kiezen-en-delen.nl

Door praktijkervaring en gewijzigde regelgeving wijzigt de inhoud of het bestaan van deze documenten. De privacy officer adviseert over de actuele vindplaatsen van de juiste informatie.

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, inclusief de Wet Politiegegevens.
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 een Governance, Risk & Compliance applicatie. 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 Management Systeem. In dit PMS zijn alle verplichtingen vanuit de AVG vertaald naar procedures, maatregelen en acties. Daarmee is dit PMS een belangrijk instrument voor de FG voor haar taak als toezichthouder.
Daarnaast wordt voor het verwerkingenregister ook een speciale applicatie 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 en de Wpg.

Jaarlijks doet de FG verslag van haar bevindingen in het FG jaarverslag. Deze bevindingen hebben het jaarlijkse toezichtsplan dat een nauwe relatie heeft met het jaarplan informatiebeveiliging en privacy.

5.2 Audits

Op dit moment bestaat er nog geen verplichte audit waarmee wordt getoetst of de verwerkingsverantwoordelijk op een voldoende niveau voldoet aan de AVG. Wel zijn in bestaande audits en zelfevaluaties normen opgenomen die direct betrekking hebben op de AVG. Het gaat dan om de Ensia-audit en de DigiD-audit, beide audits toetsen met name het voldoen aan de eisen van informatiebeveiliging. Ook in de zelfevaluatie Reisdocumenten en BRP komen een aantal privacyaspecten aan de orde.
Voor het verwerken van politiegegevens bestaat wel een wettelijke auditplicht. De gemeente verwerkt politiegegevens als de Buitengewoon Opsporingsambtenaren (BOA’s) strafrechtelijke opsporingstaken uitvoeren. Politiegegevens vallen onder de Wet Politiegegevens, deze wet is in belangrijke mate te vergelijken met de AVG, maar kent ook een aantal specifieke regels waaronder dus de auditplicht. Jaarlijks moet een interne audit uitgevoerd worden en om de 4 jaar een externe audit (voor het eerst in 2021). De FG wordt geïnformeerd over de voortgang en de resultaten van deze audits.

5.3 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 over het voorkomen van privacyrisico’s en het verbeteren van de bescherming van persoonsgegevens. De resultaten van de onderzoeken en de adviezen worden vastgelegd.

5.4 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: privacyverklaring 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 haar taak als toezichthouder.

5.5 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. Nieuwe medewerkers (ook tijdelijk inhuur en stagiaires) zijn verplicht de ‘instructie privacy’ door de Privacy Officer te volgen. 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 DPIA waardoor ze concreet aan de slag gaan met privacy.
Aanvullende en nieuwe acties die het privacybewustzijn verbeteren worden geïnitieerd door de Privacy Officer en de FG.

6. Slot

In het Privacybeleid van 2018 schreven we nog dat de bescherming van persoonsgegevens in de jaren daarvoor niet altijd de juiste aandacht had gehad. Nu, bijna 4 jaar verder, staan we er wat dat betreft beter voor. De privacy wet- en regelgeving is geïmplementeerd en er is voortdurende aandacht voor het goed en zorgvuldig omgaan met persoonsgegevens. Dat betekent niet dat we nu klaar zijn en achterover kunnen leunen. De aandacht moet niet verslappen, de privacywereld staat zeker niet stil. Steeds zijn er ontwikkelingen en ook bedreigingen waar we alert op moeten zijn. Een datalek ligt altijd op de loer.
Ook onze organisatie verandert, nieuwe bestuurders en medewerkers dienen zich aan. Het is belangrijk om oud en nieuw steeds bij de les te houden.

Met automatisering is er veel mogelijk ter bescherming van de persoonsgegevens, maar in de praktijk is al vaak gebleken dat automatisering ook een groot risico vormt. Het is nog altijd de mens die beslist over de inzet en het gebruik van automatisering. Om die reden is het goed dat bestuurders en medewerkers zich daarvoor verantwoordelijk weten en voelen.

Het verwerken van persoonsgegevens kent vele vormen en uitingen. In dit privacybeleid zijn een aantal belangrijke onderwerpen t.a.v. het verwerken van persoonsgegevens beschreven. Het privacybeleid is wat dat betreft zeker niet uitputtend en geeft geen antwoord op alle vragen, maar het is wel een belangrijk instrument dat de juiste richting aangeeft voor de dagelijkse privacy praktijk. Periodiek wordt het privacybeleid geëvalueerd en waar nodig aangepast en/of geactualiseerd. Het advies van de FG is daarbij erg belangrijk. Het privacybeleid blijft hierdoor up to date en waarborgt dat de bescherming van persoonsgegevens het uitgangspunt is en blijft bij al ons handelen en al onze dienstverlening.

Bijlage 1

Voorbeeld verwerking in het verwerkingenregister.
(Dubbelklik op de afbeelding voor het volledige document.)

Gemeente Veere

Verwerking overzicht

Algemeen

Naam verwerking	Klachten
Omschrijving	Beknopte omschrijving: Het behandelen van officiële klachten. Volledige omschrijving: Het behandelen van klachten over gedragingen van bestuurders of medewerkers van de gemeente Veere.
Referentie	PROGRAMMA 00 - Juridische kwaliteitszorg - P004007
Referentie nummer	–
Deze verwerking wordt verricht t.b.v. een externe verwerkingsverantwoordelijke	Nee
Hyperlinks & Bijlagen	
Afdeling	
Toon in publiek register	Nee
Controle door privacy functionaris	
Exporteer PDF	–

Verantwoordelijke, Grondslagen en Verwerkingsdoelen

Grondslagen (artikel 6 AVG)	Voldoen aan een wettelijke verplichting
Toelichting grondslagen	Relevante wetgeving/beleidskaders/nota's: Awb, Klachtenregeling gemeente Veere 2021.
Verantwoordelijke	Burgemeester van Veere, College van burgemeester en wethouders, Gemeenteraad van Veere
Verwerkingsdoelen	Behandelen van aanvragen, Wettelijke verplichtingen en/of taken van algemeen belang

Gegevenscategorieën en Bewaartermijnen

Bewaartermijn	Procestermijn + bewaartermijn selectielijst Archiefwet
Bevat bijzondere gegevens	–
Bevat gevoelige gegevens	Ja
Categorieën van persoonsgegevens	Bewijsstukken t.b.v. de aanvraag/melding, Communicatie, Nationaal identificatienummer (BSN), NAW basis
Voorwaarden voor het mogen verwerken van bijzondere persoonsgegevens (artikel 9 AVG)	
Toelichting bij voorwaarden voor verwerken bijzondere persoonsgegevens	–

Categorieën van Betrokkenen, Ontvangers en Externe verstrekkers

Bevat gegevens kwetsbare groep	–
Categorieën van betrokkenen	Adviseur externe organisatie, Belanghebbende, Bestuurders, Exploitant, Gerelateerde, Werknemer gemeente Veere
Aantal betrokkenen	
Wijze van informeren betrokkenen	Aanvraagformulier / aangifte, Brief / e-mail, Niet van toepassing
Categorieën van ontvangers	Behandelend ambtenaar, Commissie bezwaarschriften en klachten, Zeeuwse Ombudsman
Herkomst gegevens	Nee
Externe verstrekkers	Gemachtigde
Toelichting bij externe verstrekkers	–

Verwerkers, Gegevensuitwisselingen

Doorgifte naar derde landen zonder passend beschermingsniveau	–

Gemeente Veere export bestand 27 oktober 2021

Bijlage 2

Model verwerkersovereenkomst

Dit model is opgenomen in Corsa onder nummer 22B.02084

Dit model is gebaseerd op het standaardmodel van de IBD. Dit model wordt regelmatig geüpdatet door de IBD. Het model van de gemeente Veere wordt daar steeds op afgestemd.

Bijlage 3

Model Data Protection Impact Assessment (DPIA)

Hiervoor wordt het model van de IBD gevolgd zoals dat is opgenomen in de applicatie IRPA.

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.

Bijlage 7

Plan van aanpak inzet cameratoezicht op basis van artikel 151c Gemeentewet

Probleem		
1	Is er een openbare orde probleem?	
1a	Beschrijf het probleem en de omvang ervan.	
1b	Zijn er cijfers beschikbaar die het probleem ondersteunen?	
1c	Is het probleem besproken in de 'driehoek'?	
1d	Wat was de uitkomst van dit overleg? (Verslag)	
Andere maatregelen		
2	Zijn er al andere maatregelen getroffen om het probleem aan te pakken?	
2a	Beschrijf de andere maatregelen.	
2b	Wat was het effect/resultaat van deze maatregelen?	
Doel		
3	Wat is het doel van het cameratoezicht?	
3a	Wanneer is dit doel (meetbaar) bereikt?	
3b	Is de inzet van cameratoezicht proportioneel i.r.t. de inbreuk in de persoonlijke levenssfeer?	
3c	Is er een DPIA uitgevoerd? Zo ja, het resultaat bijvoegen.	
3d	Is er contact met de privacy officer?	
Locatie en duur		
4	Op welke locatie(s) wordt het cameratoezicht ingezet?	
4a	Betreft dit uitsluitend een openbare plaats zoals bedoeld in artikel 1 van de Wet openbare manifestaties?	
4b	Voor welke duur wordt het cameratoezicht ingezet?	
4c	Worden vaste of mobiele camera's ingezet?	
4d	Op welke manier wordt in het betreffende gebied het cameratoezicht kenbaar gemaakt.	
Camerabeelden		
5	De politie is verantwoordelijk voor de camerabeelden. Zijn hierover afspraken gemaakt?	
5a	Waar en door wie worden de beelden uitgekeken?	
5b	Wordt er live uitgekeken en door wie?	
5c	Hoelang worden de camerabeelden bewaard?	

5d	Zijn er maatregelen getroffen om de beelden tijdig te verwijderen? Welke maatregelen?		
5e	Zijn er maatregelen getroffen om de camerabeelden voldoende te beveiligen? Welke maatregelen.		
5f	Wie is de beoogde leverancier van de camera's? (Contactgegevens)		
5g	Heeft de leverancier toegang tot de camerabeelden?		
5h	Hoe vindt het datatransport plaats?		
5i	Is er een verwerkersovereenkomst afgesloten met de leverancier?		
Besluit en evaluatie			
6	Is het concept besluit van de burgemeester opgesteld. Zo ja, het besluit bijvoegen.		
6a	Wordt het besluit bekendgemaakt?		
6b	Wordt de gemeenteraad geïnformeerd?		
6c	Wordt er tijdig een besluit genomen om het cameratoezicht te beëindigen?		
6d	Is er een evaluatiemoment vastgelegd?		
6e	Wordt over de evaluatie gerapporteerd?		
Akkoord			
		paraaf	datum
Burgemeester			
Ambtenaar openbare veiligheid			
Coördinator toezicht en handhaving			
Privacy officer			