

Privacybeleid van de gemeente Elburg 2024

Het college van burgemeester en wethouders van de gemeente Elburg;

overwegende dat,

het gewenst is om een beleidsregels vast te stellen omtrent

- de eenduidige en transparante wijze waarop binnen gemeente Elburg wordt omgegaan met persoonsgegevens omdat binnen gemeente Elburg veel wordt gewerkt met persoonsgegevens.

gelet op:

de artikelen 4:81, eerste lid, 4:83 en 1:3, vierde lid, van de Algemene wet bestuursrecht; en artikel 24, tweede lid jo. artikel 4, zevende lid van de Algemene Verordening Gegevensbescherming; en

artikel 32 Algemene Verordening Gegevensbescherming jo. iso-control 18.1.4 van de Baseline Informatiebeveiliging Overheid

b e s l u i t vast te stellen de volgende beleidsregels: Privacybeleid van de gemeente Elburg 2024

Algemeen

Inleiding

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren van. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Elburg is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Begripsbepaling

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

Visie

De komende jaren zet de gemeente als betrouwbare dienstverlenende organisatie in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers (met name haar inwoners) en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

Kernwaarden

Wij denken mee

Bij het gebruik van persoonsgegevens wordt uitgegaan van de mogelijkheden, rekening houdend met kaders die gelden vanuit wet- en regelgeving.

Wij zijn betrokken en professioneel

Privacyfunctionarissen worden vroegtijdig betrokken bij het vormgeven van verwerkingen en de wijze waarop gebruik gemaakt wordt van persoonsgegevens. Het beperken van de inbreuk op de rechten van burgers (met name de inwoners van de gemeente) en bedrijven geldt als uitgangspunt.

Wij benutten de kracht in de samenleving

De gemeente vraagt in voorkomend geval de belanghebbenden naar hun mening over voorgenomen verwerkingen van persoonsgegevens, overeenkomstig artikel 35, negende lid, van de Algemene Verordening Gegevensbescherming.

Wij zijn klantgericht

De verwerking van persoonsgegevens moet ten dienste van de betrokkene staan.

Wij zijn betrouwbaar

De gemeente verwerkt persoonsgegevens op een aantoonbare wijze conform wet- en regelgeving. Daarbij wordt rekening gehouden met de risico's voor en belangen van de belanghebbende.

Doel

Met dit Privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit Privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domein specifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde Privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke Privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit Privacybeleid worden opgevolgd en actief worden uitgedragen.

Reikwijdte

Over wie gaan de persoonsgegevens

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Organisatie(s) en verwerkingen

Dit Privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Principes voor de verwerking van persoonsgegevens

Algemeen

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (publiekrechtelijke taak of een wettelijke verplichting).

Welbepaalde doeleinden

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra

waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design

De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacyvriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

Samenwerking

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het Privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit Privacybeleid.

Transparantie

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website van de gemeente Elburg. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingenregister

De gemeente beschikt over een verwerkingenregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevensbescherming effect beoordeling (GEB)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevensbescherming effect beoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd). Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt de gemeente de Privacy Baseline van het Centrum voor Informatiebeveiliging en Privacy (CIP) als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. De privacy baseline is een normenkader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente.

Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Rollen en verantwoordelijkheden

Algemeen

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy Officer en de CISO.

Responsible/ Feitelijk verantwoordelijk/ Ambtelijk verantwoordelijk

1. Gemeentesecretaris en domeinmanagers; en
2. De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken

Accountable/ Eindverantwoordelijk/ Bestuurlijk verantwoordelijke

1. Het college van B&W

Consulted/ Adviserend

1. Privacy Officer; en
2. CISO; en
3. Functionaris Gegevensbescherming

Informerend/ Geïnformeerd

1. Gemeenteraad; en
2. Functionaris Gegevensbescherming; en
3. Belanghebbende(n)/Betrokkene(n)

College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

1. Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
2. Stelt het privacybeleid vast;
3. Geeft sturing aan Privacybeleidsvoering en legt rekenschap af over Privacybeleidsvoering aan de FG;
4. Evalueert de toepassing en werking van het Privacybeleid op basis van de rapportage van de FG;
5. Bevordert duurzame privacycultuur.

Gemeentesecretaris en domeinmanagers

De gemeentesecretaris en de domeinmanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de domeinen, alsmede voor de uitvoering van het Privacybeleid.

De gemeentesecretaris en de domeinmanagers hebben de volgende rollen en verantwoordelijkheden:

1. Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen domein;
2. Verantwoordelijk voor implementatie en uitvoering van het Privacybeleid binnen het eigen domein;
3. Informeert de FG op welke manier het eigen domein compliant is aan de privacywetgeving;
4. Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen het eigen domein;
5. Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op het eigen domein;
6. Verantwoordelijk voor autorisaties en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
7. Aansturen van de Privacy Officers, voor zover benoemd binnen het eigen domein;
8. Bevordert duurzame privacy cultuur;

9. Betreft PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezicht-houdende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

1. Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
2. Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
3. Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
4. Draagt Privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
5. Adviseert verwerkingsverantwoordelijken bij privacy klachten en verzoeken van betrokkenen (ombudsfunctie);
6. Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
7. Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
8. Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
9. Doet verslag aan het College van B&W.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het Privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

1. Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het Privacybeleid;
2. Opstellen Privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
3. Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het Privacybeleid;
4. Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
5. Beheert het centrale verwerkingenregister;
6. Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevensbescherming effect beoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
7. Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
8. Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
9. Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
10. Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
11. Ontwikkelt de bewustmakingsprogramma's- en privacy trainingen voor medewerkers, en organiseert deze;
12. Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
13. Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Andere rollen en verantwoordelijkheden

Juridische Zaken: Ondersteunen van Privacy Officer ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.

CISO: De CISO definieert het informatieveiligheidsbeleid, gebaseerd op een risicomanagementbenadering en rekening houdend met het informatieveiligheidsdreigingsbeeld, trends en de organisatiebehoefte. De CISO adviseert de domeinmanagers bij de uitwerking van het informatiebeveiligingsbeleid in plannen voor hun medewerkers. De gemeente Elburg volgt het door de VNG en de IBD11 voorgestelde functieprofiel van de concern CISO.

De CISO adviseert op het proces bij het afhandelen van ernstige beveiligingsincidenten. Dit betreft ook het betrekken van de PO en/of FG bij het crisisteam.

Communicatie: In gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)

Audit/ Concern Control: Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.

Informatiemanagement: Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze/ in welk systeem verwerkt kan/ moet worden).

Privacy ambassadeurs/contactpersonen: De Privacy Contactpersoon is het eerste aanspreekpunt binnen het domein waar de Privacy Contactpersoon werkzaam is en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het Privacybeleid.

Intrekking oude beleidsregels

Het Privacybeleid gemeente Elburg, geldend sinds 2 oktober 2019, wordt ingetrokken met ingang van de datum waarop deze beleidsregel[s] in werking treden.

Inwerkingtreding en citeertitel

1. Deze beleidsregels treden in werking op 20 augustus 2024.
2. Deze beleidsregels worden aangehaald als: Privacybeleid van de gemeente Elburg 2024.
3. Deze beleidsregels worden eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is kan het college van burgemeester en wethouders besluiten tot een tussentijdse herziening.

Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Elburg in de vergadering van 20 augustus 2024.

de burgemeester de secretaris

J.N. Rozendaal A. v.d. Maat-Bosma