Strategisch Gegevensbescherming- en Informatiebeveiligingsbeleid 2025-2029

gemeente Hilversum

INHOUDSOPGAVE

Leeswijzer

De gemeente geeft door middel van dit beleid een duidelijke richting aan de informatiebeveiliging en gegevensbescherming. Het beleid waarborgt de bescherming van onze informatievoorziening en (persoons)gegevens die we als gemeente beheren. We willen transparant zijn naar onze inwoners en bedrijven over de wijze waarop wij met hun gegevens omgaan. Het beleid biedt het bestuur, het management en de organisatie structuur bij de sturing op en het beheer van gegevensverwerkingen en informatiebeveiliging. In hoofdstuk 4 wordt kort de wettelijke verlichtingen vanuit de Algemene Verordening Gegevensbescherming, de Wet politiegegevens en het normenkader Baseline Informatiebeveiliging Overheid beschreven. De principes en uitgangspunten in de bijlage beschrijven de manier waarop iedereen binnen de gemeente Hilversum werkt aan gegevensbescherming en informatieveiligheid met als doel om onze verantwoordelijkheid als gemeente te bekrachtigen en richting te geven aan de organisatie.

Jaarlijkse review

Het beleid wordt jaarlijks gereviewd. Hierover wordt door het Privacy en Informatieveiligheid Team (PIT) aan de directie gerapporteerd.

GEBRUIKTE AFKORTINGEN

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisregistratie Adressen en Gebouwen
BGT	Basisregistratie Grootschalige Topografie
BIO	Baseline Informatiebeveiliging Overheid
BIV classificatie	Classificatie van mate van beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid
Bpg	Besluit politiegegevens
Bpg-boa	Besluit politiegegevens buitengewoon opsporingsambtenaren
BRO	Basisregistratie Ondergrond
BRP	Basisregistratie persoonsgegevens
Cbw	Cyberbeveiligingswet (Nederlandse implementatie van NIS2)
CER-richtlijn	Critical Entities Resilience Directive (EU versie van de Wwek)
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMT	Concern Management Team
DPIA	Data protection impact assessment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
G&I beleid	Gegevensbescherming- en Informatiebeveiligingsbeleid
IBD	Informatie Beveiligingsdienst
ICT	Informatie- en Communicatietechnologie
ISO	Information Security Officer
NIS2	Network and Information Security Directive 2.0 (Europese “bron” van de Cbw)
PIT	Privacy en Informatiebeveiligingsteam
PNIK	Paspoorten en Nederlandse Identiteitskaarten
PO	Privacy Officer
PUN	Paspoort uitvoeringsregeling Nederland (wet)
SUWI	Structuur uitvoeringsorganisatie werk en inkomen
SUWINET	Gemeenschappelijke elektronische Voorziening Suwi (GeVS, ook wel Suwinet)
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VNG	Vereniging van Nederlandse Gemeenten
WOZ	Waardering Onroerende Zaken
Wpg	Wet Politiegegevens

1 Inleiding

We willen de gegevens die we van Hilversummers beheren optimaal beschermen. Tegelijkertijd willen we veilige en correcte producten en dienstverlening bieden. We voeren wettelijke taken uit; zorgvuldig en naar menselijke maat. Daarbij maken we weloverwogen afwegingen van belangen. We identificeren mogelijke risico's van het gebruik van gegevens van Hilversummers. Zij mogen rekenen op een gemeentelijke organisatie die hun (persoons)gegevens weloverwogen beveiligt en beschermt.

De beveiliging en verwerking van (persoons)gegevens dient hierbij de mens, de belanghebbende, en staat ten dienste aan de taken die we als gemeente uitvoeren. Het beleid is erop gericht om deze belangen naar evenredigheid tegen elkaar af te wegen, terwijl we rekening houden met het algemeen belang dat we als gemeente dienen.

Onze taakuitvoering verandert mee met de samenleving die aan het digitaliseren is. Overal om ons heen worden nieuwe technologieën zoals mobiel internet, slimme camera's en algoritmes gebruikt. Als gemeente kunnen we hierin niet achterblijven. Binnen de gemeente is digitale gegevensuitwisseling met ketenpartners en samenwerkingsverbanden een gegeven. Als gemeente zien we het als onze verplichting om de menselijke maat centraal te stellen.

We zijn ervan overtuigd dat we voorbereid zijn op ontwikkelingen in de samenleving en we de belangen van onze inwoners kunnen behartigen. We vinden het van belang dat we onze informatiehuishouding op orde hebben. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens. Inwoners, bezoekers, ondernemers, medewerkers en (keten)partners (belanghebbenden) mogen erop vertrouwen dat we passende bescherming bieden bij de verwerking van hun (persoon)gegevens.

1.1 Aanleiding

Dit beleid beschrijft het strategisch Gegevensbescherming- en Informatiebeveiligingsbeleid (G&I beleid) voor de jaren 2025-2029 en vervangt het in 2020 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2020-2024' en het 'Privacybeleid 2020-2024'. Daarnaast is in het beleid nu ook de Wet Politiegegevens opgenomen. Beveiliging van gegevens en de bescherming van persoonsgegevens zijn in de uitvoering onlosmakelijk met elkaar verbonden. Daarom is ervoor gekozen om het strategische beleid op het gebied van de bescherming van persoonsgegevens te combineren met het beleid rondom informatiebeveiliging. Hiermee zetten we als de gemeente een volgende stap in bescherming en beveiliging van (persoons)gegevens en gaan voort op de stappen die in de voorgaande jaren gezet zijn. Daarbij stellen we de mens centraal.

1.2 Doel

Dit beleid geeft de kaders voor een zorgvuldige omgang met de gegevens die we als gemeente bij de uitvoering van onze taken verwerken. We zien het als een belangrijke opgave om de bescherming van rechten en vrijheden van personen waarvan we persoonsgegevens verwerken te borgen. Dit zonder te kort te doen aan de noodzaak om de gegevens waar nodig te kunnen gebruiken en delen als deze nodig zijn voor een effectieve dienstverlening, bescherming van de openbare orde en veiligheid of zorgtaken. Een zorgvuldige omgang met (persoons)gegevens, waarbij de menselijke maat centraal staat. Het biedt gegevensbescherming op een manier die de beschikbaarheid, kwaliteit en het stromen van informatie waar nodig bevorderd.

Rechtmatige gegevensverwerking, doelmatige en doeltreffende beheersing van risico's staan centraal. We laten ons leiden door objectieve beoordeling van risico's. Een en ander volgens de toepasselijke wet- en regelgeving en ten dienste aan onze inwoners, bedrijven en bezoekers. We benutten de mogelijkheden van digitalisering, maar niet zonder ook de keerzijden ervan te onderkennen. Met dit beleid bekrachtigen we deze verantwoordelijkheid en stellen de rollen en verantwoordelijkheden vast. Het beleid zorgt dat we als gemeente transparant zijn over de wijze waarop wij het beheer en de sturing op de gegevensverwerking en informatieveiligheid hebben geborgd.

1.3 Onze kernwaarden

Bij de bescherming van (persoons)gegevens en de maatregelen die we treffen op het gebied van de informatiebeveiliging gaan we uit van de kernwaarden van de gemeentelijke organisatie.

Vertrouwen – *we gaan in ons handelen uit van de oprechtheid van onze inwoners en partners. We verwerken (persoons)gegevens op basis van de (wettelijke) taak die we als gemeentelijke organisatie uitvoeren.*

Eenvoud – *we streven in ons handelen naar eenvoud en zorgvuldigheid. We streven bij de bescherming van (persoons)gegevens en informatiebeveiliging naar een optimale balans tussen veiligheid en werkbaarheid.*

Betrokkenheid – *we zijn betrokken bij onze stad, onze inwoners en partners en houden rekening met hun wensen en behoeften We streven naar oplossingen waarbij onze inwoners zoveel als mogelijk regie houden op hun eigen gegevens*.

Professioneel – *we verstaan ons vak, werken effectief samen, spreken elkaar aan en adviseren objectief en integraal. We zijn deskundige met oog voor werkbare- en verantwoorde oplossingen voor de uitvoering van onze gemeentelijke taken en dienstverlening.*

Inclusief – *we behandelen de ander op basis van gelijkwaardigheid en sluiten niemand uit.*
We werken ten dienste van de inwoners, ondernemers, bezoekers, medewerkers en ketenpartners. De gegevensverwerking staat ten dienste aan de mens en ondersteunt de uitvoering van onze gemeentelijke taken en dienstverlening.

Duurzaam – *we streven naar duurzame oplossingen voor onze inwoners, stad en planeet. We zorgen er voor dat we (persoons)gegevens op een slimme, veilige en ethisch verantwoorde wijze inzetten voor het uitvoeren van onze gemeentelijke taken en dienstverlening.*

2 Plaats, scope en randvoorwaarden

Dit beleid is van toepassing op de gehele organisatie (medewerkers, gemeentebestuur en griffie) en is primair gericht aan alle medewerkers die in het kader van hun werkzaamheden gegevens van de gemeente verwerken. Alle medewerkers zijn medeverantwoordelijk voor betrouwbare, transparante en veilige informatieverwerking. Dit beleid betreft een overkoepelend kader waarin de maatregelen op abstract niveau zijn uitgewerkt. In werkplannen, procedures en werkinstructies wordt een verdere uitwerking gegeven aan de wijze waarop de informatiebeveiliging en bescherming van (persoons)gegevens is geborgd.

Met de vaststelling van dit beleid hernieuwt het gemeentebestuur de opdracht tot de naleving van de BIO en de behoorlijke en de zorgvuldige verwerking van (persoons)gegevens. Tevens onderschrijft het gemeentebestuur haar eigen aandeel hierin, dit naar gelang de verantwoordelijkheden naar Europees en Nederlands publiekrecht – of naar de maatstaven van het privaatrecht zoals goed werkgeverschap.

Voor de beleidsvoering betekent dit dat de bestuursorganen zijnde het college, de burgemeester en de gemeenteraad sturing geven en eindverantwoordelijk zijn conform ieders taakstelling. Binnen het college is er een portefeuillehouder privacy, informatiebeveiliging en ICT. Daarnaast blijven burgemeester en wethouders volgens ieders eigen portefeuille verantwoordelijk voor de kwaliteit van gemeentelijke taakuitoefening en rechtsbescherming.

2.1 Plaats

Dit beleid wordt gebruikt om de basis te leggen voor de tactische plannen en daarmee richting te geven aan de verdere invulling van gegevensbescherming en informatiebeveiliging op tactisch- en operationeel niveau.

Dit beleid beschrijft op strategisch niveau het gegevensbescherming- en informatieveiligheidsbeleid. Dit beleid zal, waar nodig, worden uitgewerkt in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het tweejaarlijks op te stellen ‘Gemeentelijk Gegevensbescherming- en Informatieveiligheidsplan’.

Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link wel naar het gegevensbescherming en informatiebeveiligingsbeleid (G&I beleid) gelegd.

2.2 Scope

De scope van het G&I beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld de politie) en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Ook de fysieke toegangsbeveiliging is onderdeel van gegevensbescherming en informatiebeveiliging.

Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.

Dit G&I beleid biedt een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving en normenkaders af zoals uit de AVG, UAVG, Wpg, Bpg, AI Act, Cbw, BRP, PNIK/PUN, DigiD en SUWI (zie lijst met gebruikte afkortingen). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD eisen. Deze zijn in aanvullende beleidsdocumenten uitgewerkt.

Alle procesautomatiseringssystemen die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersystemen en bijvoorbeeld cameratechnologie of verkeersregelinstallaties en gemalen maken ook onderdeel uit van dit beleid.

2.3 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

Borging in alle processen
De gegevensbescherming en informatiebeveiligingseisen maken deel uit van alle gemeentelijke processen en daarnaast is het onderdeel van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd en gecontroleerd.

Creëren van bewustzijn en kennis
De gemeente moet kennis en bewustzijn van gegevensbescherming en informatiebeveiliging binnen de organisatie actief bevorderen en waarborgen.

Tweejaarlijkse plannen
Tweejaarlijks wordt een gemeentelijk Gegevensbescherming- en Informatieveiligheidsplan opgesteld onder leiding van de Chief Information Officer (CIO), gebaseerd op dit G&I beleid, de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA), andere audit resultaten, het dreigingsbeeld gemeenten van de IBD, uitkomsten van risicoanalyses, waaronder Data Protection Impact Assessments (DPIA).

Financiële middelen en uitvoeringscapaciteit
Om uitvoering te kunnen geven aan dit strategisch beleid en het G&I (werk)plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3 Governance

Met de toepassing van dit beleid realiseren we het:

- Garanderen van correcte en veilige informatievoorzieningen en systemen.
- Adequaat bescherming van (persoons)gegevens en toepassen van dataminimalisatie.
- Managen van de informatiebeveiliging en het beschermen van (kritieke) bedrijfsprocessen.
- Minimaliseren van risico's van menselijk handelen.
- Voorkomen van ongeautoriseerde toegang tot informatievoorzieningen en systemen.
- Adequaat reageren op incidenten en bewaken van de rechten van betrokkenen.
- Voldoen aan de wettelijke verplichtingen (waaronder de AVG, UAVG, AI act, Cbw, Wpg, Bpg en Bpg-boa).

Om dit te realiseren is het van belang dat verantwoordelijkheden binnen de organisatie helder zijn belegd.

3.1 Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot gegevensbescherming en informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense') waarbij het lijnmanagement verantwoordelijk voor het realiseren van gegevensbescherming en informatiebeveiliging binnen de eigen processen. De tweede lijn, de Information Security Officer (ISO) en de Privacy Officer (PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor, Chief Information Security Officer (CISO) en Functionaris Gegevensbescherming (FG) van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier heeft ook de ENSIA-coördinator een rol.

De betrokkenheid van het bestuur en management is essentieel bij het waarborgen van gegevensbescherming en informatiebeveiliging. Daardoor laat de gemeente zien dat zij deze serieus neemt en het een onderdeel is van de ambitie om gegevens van haar inwoners adequaat te beschermen.

3.2 Gemeenteraad

Met de vaststelling van dit beleid hernieuwt het gemeentebestuur de opdracht tot behoorlijke en zorgvuldige verwerking van (persoons)gegevens en de informatiebeveiliging. Tevens onderschrijft het gemeentebestuur haar eigen aandeel hierin. Voor de beleidsvoering betekent dit dat de bestuursorganen, college, burgemeester en gemeenteraad sturing geven en eindverantwoordelijk zijn conform ieders taakstelling.

De gemeenteraad ziet erop toe dat het college overkoepelend beleid ten aanzien van bescherming van (persoons)gegevens en informatiebeveiliging voor de organisatie vaststelt. Door de gemeenteraad worden voor de uitvoering hiervan de benodigde middelen beschikbaar gesteld. Voorts controleert zij het college bij de uitvoering van deze kaders.

De griffie is ambtelijk verantwoordelijk voor de verwerkingen van de gemeenteraad.

3.3 College van Burgemeester en Wethouders

Het college is integraal verantwoordelijk voor de zorgvuldigheid van de verwerking van gegevens en de informatiebeveiliging binnen de gemeentelijke organisatie. Het college is het aangewezen bestuursorgaan dat de passende gegevensbescherming en informatiebeveiliging waarborgt. Zo is hij verantwoordelijk voor een duidelijk te volgen beleid, doet aan de gemeenteraad voorstellen over in te zetten middelen en stelt specifieke regelingen en procedures vast. Daarnaast controleert het college het management van de organisatieonderdelen op de maatregelen die verband houden met gegevensbescherming en informatiebeveiliging.

Binnen het college is er een portefeuillehouder voor privacy en informatiebeveiliging. Deze legt namens het college (politieke) verantwoording af over de beleidsvoering aan de gemeenteraad. Daarnaast blijven burgemeester en wethouders volgens ieders eigen portefeuille verantwoordelijk voor de kwaliteit van gemeentelijke taakuitoefening en rechtsbescherming. De burgemeester is de verwerkingsverantwoordelijke

voor de verwerkingen die vallen onder de Wet politiegegevens (Wpg). Het college draagt de directie op om dit beleid in nadere richtlijnen en werkinstructies uit te werken.

We leggen via de ENSIA verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen. Deze verantwoording ziet op datakwaliteit en informatieveiligheid van gegevenslevering aan landelijke basisregistraties en over beveiliging van DigiD aansluitingen en Suwinet-inkijk (verticale verantwoording). De ENSIA verantwoording wordt door de directie aan het college aangeboden die daarna rapporteert aan de raad over de datakwaliteit en informatieveiligheid en beveiliging van de DigiD aansluitingen en Suwinet-inkijk (horizontale verantwoording).
De FG rapporteert aan het college door middel van zijn jaarverslag. Het college informeert de raad daarover. Het college verantwoordt zich over gegevensbescherming en informatiebeveiliging via het Jaarverslag aan de raad.

3.4 Directie

Aansturing

De directie geeft uitvoering aan het beleid. Binnen het directieteam is deze taak belegd bij de CIO. De directie zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging en bescherming de (persoons)gegevens of andere informatie die onder hen berust. De directie zorgt daarnaast ook dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin gegevensbescherming en informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

- De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.
- De directie draagt zorg voor het uitwerken van het tactische informatiebeveiligings- en privacy werkplan en laat zich hierin bijstaan door de CISO, ISO, FG en PO van de gemeente.
- De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp gegevensbescherming en informatiebeveiliging wordt in de gemeente gezien als een integraal onderdeel van risicomanagement.
- De directie stelt proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG door middel van de deelname van de FG aan het CIO.
- Bij uitbesteding of mandatering van taken en verantwoordelijkheden naar een externe dienstverlener of uitvoeringsorganisatie zorgt de directie voor borging van gegevensbescherming – en informatiebeveiligingseisen die moeten gelden voor de uitbesteedde taak. Zij zorgt er ook voor dat er door de organisatie gerapporteerd wordt over deze aspecten.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over gegevensbescherming en informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Daarbij krijgt de directie jaarlijks rapportages van de CISO en de FG.

Bij uitbesteding of mandatering van taken en verantwoordelijkheden naar een externe dienstverlener of uitvoeringsorganisatie zorgt de directie ervoor dat er door de organisatie gerapporteerd wordt over gegevensbescherming en informatiebeveiliging. Daarbij worden afspraken gemaakt over de jaarlijkse verantwoording op het gebied van gegevensbescherming en informatiebeveiliging door middel van een rapportage, bijvoorbeeld een zogenaamd Third Party Memorandum van een onafhankelijke auditor of een FG verslag.

3.5 Lijnmanagers

Uitvoering (eerste lijn)

Gegevensbescherming en informatiebeveiliging valt onder de verantwoordelijkheden van alle managers. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. We werken er naar toe dat alle processen, systemen, applicaties altijd één eigenaar hebben; er moet dus altijd iemand (eind)verantwoordelijk zijn. Proceseigenaren voeren in feitelijke zin de regie over de uitvoering van taken binnen hun teams. Dit is nadrukkelijk afgesproken in het Concern Management Team (CMT).

Processen juist inrichten waarbij de risico's beheerd worden

Het betrekken van het Privacy en Informatiebeveiligingsteam (PIT) bij nieuwe of gewijzigde processen zorgt ervoor dat er tijdig advies gegeven kan worden over beheersmaatregelen die de gegevensbescherming optimaliseert. Daarbij is het de verantwoordelijkheid van de lijnmanager om procedures en werkinstructies in lijn met het vastgestelde beleid beschikbaar te stellen aan (nieuwe) medewerkers. Daarbij voldoen de processen aan geldende wet- en regelgeving. Het is binnen processen van belang om vroegtijdig de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld te signaleren. Het behoort tot de taken van de lijnmanagers om DPIA's uit te voeren, door hiertoe opdracht te geven en zorg te dragen voor het voldoen aan de kwaliteitseisen uit de DPIA.

Controleren van (werk)processen

Het erop toezien dat de controles op het verwerken van persoonsgegevens regelmatig worden uitgevoerd, Waarbij nadrukkelijk aandacht is voor risico's die inwoners lopen wanneer gegevens in een proces verwerkt worden. Bovendien zijn zij verantwoordelijk voor de jaarlijkse controle op de autorisaties om vast te stellen dat alleen geautoriseerde medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.

Sturen op (werk)processen

Het toezien op het hebben van minimale basiskennis van medewerkers op het gebied van de privacywetgeving en toepassing hiervan in het dagelijks werk. Het toezien op de training van medewerkers in het gebruik van beveiligingsprocedures. Bespreking van beveiligingsincidenten en datalekken en de consequenties die dit moet hebben voor beleid en maatregelen. Verantwoordelijk voor het nemen van (beheers)maatregelen die de continuïteit van het proces borgen.

Rapporteren over (werk)processen

Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal een keer per jaar het onderwerp gegevensbescherming en informatiebeveiliging te bespreken in een planning en control overleg met de afdelingsmanager en businesscontroller, waarbij het PIT kan adviseren.

Verantwoordelijkheid bij overdracht van taken of diensten aan dienstverlener of uitvoeringsorganisatie

Daar waar taken of diensten zijn uitbesteed aan externe leveranciers of uitvoeringsorganisaties, waarborgen de proceseigenaren aan de hand van dienstverleningsafspraken optimale condities op het gebied van gegevensbescherming en informatiebeveiliging.

Verantwoordelijkheid bij overdracht van taken naar een dienstverlener via een gemeenschappelijke regeling

Bij deelname in een gemeenschappelijke regeling en andere samenwerkingsverbanden voorzien proceseigenaren de gemeentebestuurders die de gemeente vertegenwoordigen van sturingsinformatie, zodat deze op hun beurt in staat zijn om de belangen en risico's op een juiste wijze te kunnen beheersen. Managers beheren en voeren regie over ketensamenwerkingen.

3.6 Interne adviseurs PIT

Ondersteuning (tweede lijn)

Om de kwaliteit en de voortgang van de het beleid te waarborgen, is er tweede lijn-ondersteuning. Proceseigenaren zijn en blijven zelf verantwoordelijk. Maar daarvoor kunnen zij rekenen op tweede lijn-versterking. Deze wordt geboden door professionals op het gebied van informatiemanagement, communicatie, juridische zaken, audit, inkoop, risicomanagement, informatiebeveiliging en ICT. Het kernteam voor gegevensbescherming en informatieveiligheid wordt gevormd door het Privacy- en Informatiebeveiligingsteam (PIT).

Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. De adviseurs van het PIT verzorgen een bewustwordingsprogramma om medewerkers kennis en informatie bij te brengen over gegevensbescherming en informatieveiligheid.

Vastgestelde beleidsstukken (bijv. vastgesteld beleid, beveiligingsplannen, standaarden en richtlijnen) worden centraal beheerd en intern gepubliceerd zodat alle medewerkers zich kunnen informeren over de geldende afspraken rondom informatiebeveiliging en privacybescherming.

De ENSIA coördinator is een rol van de security officer binnen het team en heeft als taak om de jaarlijkse ENSIA verantwoording over datakwaliteit van de basisregistraties en informatiebeveiliging van de DigiD en Suwinet-inkijk aansluiting van de gemeentelijke organisatie aan de stelselhouders en de raad te coördineren. Het goed doorlopen van deze verantwoordingscyclus is essentieel voor continuering van de dienstverlening aan de belanghebbenden.

Het PIT rapporteert vier keer per jaar aan de CIO. De leden van het CMT ontvangen twee keer per jaar de rapportage van de interne adviseurs van het PIT, met daarin de voortgang op de onderwerpen uit de tactische jaarplannen, actuele ontwikkelingen en informatie met betrekking tot gegevensbescherming en informatiebeveiliging, informatie over datalekken en informatiebeveiligings-incidenten en de opvolging daarvan. Het PIT reviewt jaarlijks het Strategisch Gegevensbescherming- en Informatiebeveiligingsbeleid 2025-2029 en rapporteert daarover aan het CIO.

De ENSIA rapportage wordt door de CISO/ENSIA coördinator via het bestuurlijke besluitvormingsproces via de wethouder aan de raad aangeboden.

3.7 FG, CISO, Concerncontroller, Businesscontroller

Controle, verantwoording en audits (derde lijn)

Uitvoering en toezicht op het beleid is een verantwoordelijkheid van het bestuur van de gemeente Hilversum. De bestuurders en directeuren van de gemeente Hilversum zullen werken volgens de tien principes voor informatiebeveiliging en de principes voor het verwerken van persoonsgegevens, zoals beschreven in de Bijlage.

Zij geven sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorlichting en het vragen om informatie. De CISO en de FG rapporteren en adviseren (gevraagd en ongevraagd) over gegevensbescherming en informatieveiligheid aan de directie en het college.

De FG ontvangt van de directie en afdelingsmanagers proactief informatie over de bescherming van persoonsgegevens en deelt hierop zijn bevindingen met de adviseurs van het PIT.

De Concerncontroller en de Businesscontroller zijn er tijdens de P&C-gesprekken verantwoordelijk voor dat er aandacht is voor informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en/of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.

Rapporteren via het jaarverslag aan de raad

De verantwoording over de gegevensbescherming en informatiebeveiliging komt in de bedrijfsvoering paragraaf van het gemeentelijk jaarverslag tot uitdrukking.

Rapporteren via de ENSIA verantwoordingssystematiek aan de raad
De audit in het kader van de ENSIA-verantwoording wordt door de CISO en ENSIA coördinator gebruikt om de stukken voor het college te voorzien van een onafhankelijk oordeel. In de ENSIA collegeverklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de gestelde eisen/normen.

Rapporteren via het FG jaarverslag aan het college
De verantwoording over de gegevensbescherming komt in het onafhankelijke FG-jaarverslag tot uitdrukking. Daarmee informeert de FG het college over de stand van zaken voor de gemeente Hilversum.

Rapporteren over informatiebeveiliging aan de CIO
De jaarlijkse verantwoording over de informatiebeveiliging door de CISO toont in hoeverre de organisatie stappen heeft gemaakt in het verbeteren van de beveiliging. De CIO ontvangt deze rapportage.

Rapporteren over uitgevoerde audits
De Concerncontroller actualiseert in samenspraak met de CISO jaarlijks de auditplannen op het gebied van informatieverwerking, en rapporteert aan de directie over de uitgevoerde audits. De CISO en de FG op de hoogte gesteld worden van de bevindingen.

4 Wettelijke eisen

De basis voor dit strategisch beleid is de NEN-ISO 27.001 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO), de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en het VNG Borgingsproduct AVG versie 3.0. We hanteren de meest recent vastgestelde versie van de Baseline Informatiebeveiliging Overheid.

De verwerking van (persoons)gegevens door buitengewoon opsporingsambtenaren (boa's) vallen onder omstandigheden onder de Wpg, het Besluit Politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren ('Bpg boa') en de Regeling periodieke audit politiegegevens. Hoewel deze wet- en regelgeving deels overlap kent met de AVG, zijn er een aantal verschillen.

In de Bijlage beschrijven we de principes die we hanteren. Deze zijn gebaseerd op de beginselen uit de AVG voor het verwerken van persoonsgegevens en op de geldende principes voor informatiebeveiliging, de BIO.

4.1 Gegevensbescherming en AVG

De gemeente werkt met (persoons)gegevens van belanghebbenden. Deze gegevens gebruiken we voor het goed kunnen uitvoeren van onze taken. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed uit te voeren is de verwerking van persoonsgegevens noodzakelijk. Bij de omgang met (persoons)gegevens hebben we een grote verantwoordelijkheid. De juiste bescherming van (persoons)gegevens is hierbij een essentieel maar ook complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, inzet van nieuwe technologie, en de veranderende wet- en regelgeving.

Uitgangspunt van wet- en regelgeving is echter dat de verwerking van (persoons)gegevens ten dienste staat van de mens. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen. Andere grondrechten zijn bijvoorbeeld het recht op menselijke waardigheid, veiligheid, onderwijs, participatie, net zoals het recht op bescherming van het privéleven. Anders gezegd; verwerking van (persoons)gegevens moet ten dienste staan van ons welzijn volgens de publieke waarden. Tegelijkertijd prevaleert iemands individuele belang niet noodzakelijk, maar kunnen belangen van anderen zwaarder wegen – vooral als deze belangen bij wet of gemeentelijke verordening zijn aangemerkt als zijnde van algemeen belang.

Het gaat om de balans. Daar waar de gemeente publiekrechtelijk of privaatrechtelijk een legitieme rol heeft en dat gepaard gaat met verwerking van (persoons)gegevens, is dat toegestaan. Risico's vloeien voort uit de kans dat we door niet, of door het gebrekkig verwerken van informatie over mensen (persoonsgegevens) hen sociale, psychische of financiële schade of misschien wel schade voor de gezondheid of gevaren voor de persoonlijke veiligheid aandoen.

We maken gebruik van een risicoanalyse (Data Protection Impact Assessment; DPIA) om inzicht te krijgen in de risico's bij een verwerking. Met de DPIA classificeren we gemeentelijke activiteiten en de bijbehorende informatieverwerking en schatten hierbij de risico's voor betrokkenen en/of de organisatie in en nemen waar nodig passende maatregelen om de risico's te mitigeren. Door middel van realistische scenario's kunnen risico's worden onderkend waarin inwoners of andere doelgroepen gedupeerd raken door digitalisering. Hoe hoger de risicoscore, hoe meer aandacht en prioritering nodig is, en hoe robuuster de maatregelen. Daarnaast registreren we alle datalekken, die we zo goed mogelijk oplossen en ervan leren om zo ook herhaling te voorkomen.

4.2 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatiehuishouding aantoonbaar te waarborgen. Van groot belang daarbij is dat de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de (persoons)gegevens, bedrijfsprocessen en (informatie)systemen geborgd wordt.

De normen uit het normenkader van de NEN-ISO 27.001 en het daarop gebaseerde normenkader van de Baseline Informatiebeveiliging Overheid (BIO) krijgt een wettelijke status in de vorm van de Cyberbeveiligingswet (Cbw). Het omvat ook de Europese eisen die voortvloeien uit de Network and Information Security Directive 2.0 (NIS2).

Informatiebeveiliging geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus van informatiesystemen ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het bestuur, medewerkers, burgers, gasten, bezoekers en externe relaties.

4.3 Wet politiegegevens (Wpg)

De Wpg geldt sinds 2008 al voor de politie, de marechaussee, de rijksrecherche en bijzondere opsporingsteams zoals de FIOD. Sinds 2019 is de boa aan dat lijstje toegevoegd door middel van het Besluit politiegegevens boa. In algemene zin is de Wpg van toepassing op iedere verwerking van een politiegegevens, dat wil zeggen een persoonsgegeven die wordt verwerkt in het kader van de uitvoering van de politietaak. Dit kunnen ook ondersteunende taken zijn bij de uitvoering van opsporingstaken.

De gemeente heeft boa's in dienst. Samen met de politie en andere organisaties zijn zij verantwoordelijk voor de veiligheid en leefbaarheid. Omdat boa's en ondersteunende collega's in het kader van hun politietaak persoonsgegevens verwerken, is op hen in bepaalde gevallen de Wpg van toepassing.

Bij de verwerking van (persoons)gegevens ten behoeve van de opsporingstaak van opsporingsambtenaren (boa's) is het Bpg, verder uitgewerkt in het BPG boa van toepassing. In de praktijk zijn boa's werkzaam binnen een eigen domein, en hebben zij – in tegenstelling tot een algemeen opsporingsambtenaar van de politie – een opsporingsbevoegdheid voor één of meer specifieke wetten en wetsartikelen.

Binnen de gemeente is het toepassingsgebied van de Wpg daarom beperkt tot werkzaamheden van boa's die via het Bpg gebonden zijn aan specifieke wetgeving. In de praktijk zijn boa's werkzaam binnen een eigen domein, en hebben zij – in tegenstelling tot een algemeen opsporingsambtenaar van de politie – een opsporingsbevoegdheid voor één of meer specifieke wetten en wetsartikelen. De boa's ontlenen hun bevoegdheden aan het domein waarbinnen zij werkzaam en beëdigd zijn.
De wet maakt onderscheid in de domeinen:

1 Openbare Ruimte: aanpak van overlast, verloedering of veiligheid voor zover dit laatste niet ziet op de openbare orde. Het gaat daarbij om overtredingen die de leefbaarheid aantasten en niet zien op de openbare orde.
2 Milieu, welzijn en infrastructuur: natuur en milieu, arbeidsinspectie, voedsel- en warencontroles, dierenwelzijn, openbare gezondheid, fysieke leefomgeving (zoals gebouwen, parken, schone lucht, rivieren, bossen) en infrastructuur.
3 Onderwijs: handhaving leerplichtwet en andere wet- en regelgeving die daarmee te maken heeft.
4 Openbaar vervoer: strafbare feiten opsporen binnen het domein openbaar vervoer.
5 Werk, Inkomen en Zorg: strafrechtelijke handhaving op het gebied van werk, inkomen, belastingen en sociale zaken.
6 Generieke Opsporing: restcategorie boa's met meestal algemene opsporingsbevoegdheid.

Werkzaamheden van boa's worden onderverdeeld in drie categorieën van opsporingstaken, te weten:

- Uitvoering van dagelijkse politietaken (artikel 8 Wpg);
- Onderzoek in verband met handhaving van de rechtsorde in een specifiek geval (artikel 9 Wpg); en/of
- Ondersteunende taken (artikel 13 Wpg).

Het Wpg-regime is van toepassing op deze opsporingstaken. Binnen de gemeente Hilversum zijn alleen boa’s werkzaam binnen Domein I: Openbare Ruimte. Zij voeren enkel opsporingstaken uit die vallen onder de artikel-8 verwerkingen. De feitelijke werkgever van de boa's zijn verwerkingsverantwoordelijke voor de verwerking van de Wpg.

De boa's hebben naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken. Zij krijgen dan bij het verwerken van gegevens te maken zowel met de AVG te maken als met de Wpg. Wanneer gegevens worden verwerkt moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg.

Wpg Auditverplichting

Interne audit

Sinds 2019 vindt ten minste jaarlijks een interne audit plaats. Deze audit heeft betrekking op één dan wel een aantal onderdelen van de wet en heeft tot doel om op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. In de interne audit betrekken we ten minste de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien, maar ook de werking daarvan.

Externe audit

Met ingang van 2021 zijn we verplicht tot het uitvoeren van een externe audit over de verwerking onder het regime van de Wpg. De controle heeft betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures. Resultaten van eerdere interne audits worden betrokken bij de externe audit. Externe audits worden uitgevoerd door een derde partij. Een afschrift van de controleresultaten verstrekken we aan de AP. Tekortkomingen worden opgenomen in een verbeterrapport. Binnen een jaar na de oorspronkelijke auditresultaten vindt daarop een hercontrole plaats. De hercontrole geldt alleen voor die onderdelen van de Wpg waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens, uiterlijk 1 jaar na uitvoering van de audit, verstrekt aan de AP.

Bijlage I - Principes en uitgangspunten

Deze bijlage beschrijft de algemene principes en uitgangspunten die we als gemeente hanteren. De betrokkenheid van het bestuur en management is essentieel bij het waarborgen van gegevensbescherming en informatiebeveiliging. Daardoor laat de gemeente zien dat zij dit serieus neemt en het een onderdeel is van de ambitie om gegevens van haar inwoners adequaat te beschermen.

Het gehele gemeentelijke management speelt een rol bij de uitvoering van dit G&I beleid. Managers dragen verantwoordelijkheid om een inschatting te maken van het belang van een informatievoorziening en zij beoordelen of er risico's zijn waarvoor (beheers)maatregelen nodig zijn. Daarbij kan zij zich laten adviseren door het PIT.

Het uitgangspunt is dat gegevensbescherming en informatiebeveiliging optimaal ingericht zijn, zodat we de gegevens van inwoners, ondernemers, bezoekers, medewerkers en (keten)partners rechtmatig en veilig verwerken. Het management volgt dit beleid op, draagt het uit in de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Dit beleid is van toepassing op de gehele organisatie, processen, objecten, organisatieonderdelen, informatiesystemen, procesautomatisering en (persoons)gegevens en het is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

Principes voor de verwerking van persoonsgegevens

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.

Persoonsgegevens worden rechtmatig, behoorlijk en transparant verwerkt

We verwerken uitsluitend persoonsgegevens om te voorzien in een legitieme informatiebehoefte. Zonder die informatie gaat iets fout in de gemeentelijke dienstverlening, taakuitoefening of bedrijfsvoering. 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 wettelijke verplichting of een publiekrechtelijke taak.

Doelbinding

We verwerken persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder specifiek 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 we alleen die persoonsgegevens verwerken die noodzakelijk zijn om het doel te bereiken. We zien af van 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 doelen aan elkaar verwant moeten zijn, zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. We

voeren 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 en leggen deze overweging vast.

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 kiest de gemeente 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 kiezen we voor die mogelijkheid.

Juiste en actuele gegevens
We zorgen ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij worden verwerkt. We nemen redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd
We stellen de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en selectielijsten. Gemeenten hebben op grond van de Archiefwet 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, stellen we de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens worden dan niet langer worden bewaard dan noodzakelijk. We bewaren gegevens alleen langer indien deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon Is uitgesloten. Voor de Wpg hanteren we de bewaartermijnen zoals genoemd in artikel 8 van de Wpg.

Integriteit en vertrouwelijkheid
We nemen passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. We beveiligen de gegevens tegen ongeautoriseerd gebruik, vernietiging, verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design
We houden 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’ genoemd. We dragen 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 privacy-vriendelijk mogelijk.

Toegang tot gegevens
Uitsluitend geautoriseerde gebruikers zijn bevoegd tot het verwerken van (persoons)gegevens 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. Het beheer van bevoegdheden wordt bovendien periodiek gecontroleerd. We hanteren 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.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies, verwijdering 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 (AP) en soms bij de getroffen betrokkenen. We volgen hierin de richtlijnen van de toezichthouder. We registreren datalekken, zetten de bevindingen om in verbeterpunten en zien toe op de opvolging hiervan.

Samenwerking
Soms schakelen we derden in om (persoons)gegevens in opdracht te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan wet- en regelgeving op het gebied van bescherming van persoonsgegevens en aan het beleid van de gemeente. We maken met deze derden contractuele afspraken over de omgang met persoonsgegevens en de informatiebeveiliging.

Samenwerkingsverbanden
We werken ook samen met andere (overheids)organisaties om onze taken van algemeen belang uit te voeren. Om deze reden delen wie ook informatie met deze organisaties waar dat nodig is of ontvangen we juist informatie van anderen. In die gevallen kan sprake zijn van een of meerdere verwerkersverantwoordelijken. We maken met deze organisaties afspraken over de wijze waarop

persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat minstens gelijk is aan dat van de gemeente.

Doorgifte buiten de Europese Economische Ruimte
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte of internationale organisaties geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving.

Transparantie
We informeren de betrokkenen tijdig op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat we persoonsgegevens verwerken en op welke wijze en voor welke doeleinden we dit doen. De betrokkene wordt op heldere en duidelijke wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijken we af van deze informatieplicht.

Rechten van betrokkenen
Iedereen heeft het recht om te weten welke persoonsgegevens de gemeente over hem/haar verwerkt. 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 het recht op overdraagbaarheid.

Geschillenbeslechting
Indien de betrokkene van mening is dat we op een onjuiste wijze met zijn of haar (persoons)gegevens omgaan, kan hij of zij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op onze website. De betrokkene heeft ook het recht een klacht in te dienen bij de AP, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording
De AP houdt toezicht op de naleving van wet- en regelgeving op het gebied van bescherming van persoonsgegevens in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de FG. De FG ziet erop toe dat de AVG intern wordt nageleefd. 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 van zijn werkzaamheden, bevindingen en aanbevelingen.

Verwerkingsregister
We hebben een verwerkingsregister, waarin de verwerkingen van persoonsgegevens (AVG en Wpg) zijn opgenomen en inzichtelijke zijn gemaakt. De Wpg-specifieke verwerkingen maken onderdeel uit van het verwerkingsregister. Wpg-specifieke verwerkingen wijken niet wezenlijk af van de AVG-verwerkingen in het verwerkingsregister. Wel zijn de Wpg-verwerkingen uitgebreider gedocumenteerd, omdat de gemeente Hilversum op grond van artikel 32 Wpg en 6:4 Bpg aanvullende informatie vastlegt.

Risicoanalyse
Als uit de risicoanalyse (DPIA) blijkt dat inderdaad hoge risico's zijn verbonden aan de verwerking nemen we maatregelen om deze risico's te mitigeren. Als het niet lukt om voldoende maatregelen te nemen om dit risico te beperken moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

We streven ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control zijn betekent in dit verband dat we weten 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 maken we gebruik van het borgingsproduct van de VNG/IBD als het beoordelingskader voor een zelfevaluatie en het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct 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
Slechts het hebben van beleid en het doorvoeren van maatregelen is niet voldoende om risico's op het terrein van de verwerking van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat de kennis van risico's wordt verhoogd en waarmee het zorgvuldig verwerken van persoonsgegevens wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, onder andere via instructies en trainingen. Dit gebeurt passend binnen de context van en bij het domein waarbinnen deze worden verwerkt.

Aanvullende normen Wpg
Het normenkader van de Wpg is grotendeels gelijk aan dat van de AVG.
Op hoofdlijnen geldt aanvullend nog het volgende:

- Er is een scheiding tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er wordt onderscheid gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Er is documentatie vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de AP.
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

De principes van informatiebeveiliging

De tien principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader van de Baseline Informatiebeveiliging Overheid (BIO) en gaan over de waarden die de bestuurder zichzelf oplegt. Deze principes zijn:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van de bestuurders bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor belanghebbenden. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Uitgangspunten voor de inrichting van informatiebeveiliging

De belangrijkste uitgangspunten van het beleid zijn:

Baseline Informatiebeveiliging Overheid (BIO)
We richten onze informatiebeveiliging in conform de meest actuele versie van de BIO. Deze bestaat uit een baseline met verschillende niveaus van beveiligen. De maatregelen worden op basis van ‘best practices’ bij (lokale) overheden genomen. Voor de ondersteuning maken we gebruik van de diensten en ondersteuningsproducten van de VNG/IBD.

Cybersecurity Implementatie Richtlijn (CSIR)
Binnen de gemeente wordt naast ICT ook Operationele Technologie ingezet. Met Operationele Technologie worden systemen bedoeld voor de besturing van apparaten voor middel van procesautomatisering. Dit beleid is ook voor de bescherming van procesautomatisering en betreft dan ook beleidsafdelingen die zich met procesautomatisering bezighouden. Voor deze bescherming maken we gebruik van de CSIR.

Forum Standaardisatie
Bij de aanschaf, aanpassing en doorontwikkeling van oplossingen met een informatiecomponent conformeren we ons aan de aanbevelingen van het Forum standaardisatie.

De gemeente Hilversum wil goede beveiliging voor haar websites en e-mail. Daarom conformeren we ons aan de overheidsbrede interbestuurlijke afspraken waarbij bepaalde open standaarden bij de aanschaf van nieuwe ICT-systemen/-diensten (of de doorontwikkeling van bestaande) verplicht moeten worden toegepast.

De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement
Alle informatiebronnen- en systemen die gebruikt worden door de gemeente Hilversum hebben een interne eigenaar. Deze eigenaar bepaalt de noodzakelijke mate van beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid (de z.g. BIV classificatie) van de gegevens in de bron of het systeem. Deze eigenaar bepaalt ook de waarde van de informatie die de bron of het systeem bevat. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.

Verankering in de organisatie
Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het G&I beleid vormt samen met het G&I (werk)plan het fundament voor een betrouwbare informatievoorziening en privacybescherming. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.

Informatiebeveiliging (en gegevensbescherming) is een continu verbeterproces.
De stappen 'Plan, do, check en act' vormen samen het managementsysteem van gegevensbescherming en informatiebeveiliging. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de eisen, zoals gesteld in dit beleid.

Regels en verantwoordelijkheden voor het G&I beleid dienen te worden vastgelegd.
Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Risico gestuurde aanpak
Het borgen van gegevensbescherming in de uitvoering van gemeentelijke processen vindt risico gestuurd plaats. De managers in de organisatie maken afwegingen ter naleving van gegevensbeschermingsregels en op basis van een risico-inschatting.

Er is een formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties ingericht.
Managers moeten personeel (alle soorten) aan- en afmelden via een procedure. Daarnaast moeten er periodieke controles plaatsvinden. De toegang tot (vak)applicaties kennen een aparte autorisatieprocedure en we streven ernaar dat deze altijd samenhangt met het account van de gemeente Hilversum.

Het borgen van toegangsbeveiliging
Voor logische toegangsbeveiliging wordt het vier ogen principe toegepast bij het inrichting autorisatiematrixen. De verantwoordelijke voor de applicatie beoordeelt periodiek de uitgegeven toegangsrechten en beoordeelt nieuwe aanvragen.

Medewerkers loggen in op gemeentelijke systemen door middel van een beveiligde inlogprocedure (met Multi Factor Authenticatie), waarbij gebruikers verantwoordelijk zijn voor het beschermen van hun authenticatie-informatie.

Communicatiebeveiliging
Ter bescherming van vertrouwelijkheid, integriteit (juistheid) en betrouwbaarheid van informatie maken we gebruik van cryptografie of andere beheersmaatregelen om deze te beschermen. Dit geldt voor alle systemen die door de gemeentelijke organisatie gebruikt worden. Bij het inrichten van cryptografische beheersmaatregelen passen we de "Pas toe of leg uit lijst" van het Forum Standaardisatie en aanbevelingen van het NCSC toe.

Er worden regels, procedures of overeenkomsten voor informatieoverdracht ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.

Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
Bij het goede beheer van de leveranciersrelaties hoort dat we de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.

DigiD aansluitingen
We maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van SaaS-diensten die door leveranciers worden geleverd. Het eigenaarschap van de DigiD webapplicaties is belegd in de lijnorganisatie en de Teammanager van Interne Dienstverlening – team Business IT Ondersteuning. Zij zijn verantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen. Per DigiD-aansluiting is een functioneel beheerder aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier. Het auditdossier wordt jaarlijks aan de externe auditor beschikbaar gesteld, inclusief de servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, t.a.v. DNSSEC) en de beoordeelde releases (C.08). We conformeren ons daarbij aan de eisen uit de meest recent vastgestelde en gepubliceerde normen van Logius ICT beveiligingsassessment DigiD.

Tweemaal per jaar wordt door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn en hierover wordt verslag (autorisatiematrix) gedaan richting de procesverantwoordelijke.

Er vindt een jaarlijkse toetsing van dit normenstelsel plaats in het kader van de ENSIA door een externe auditor en de CISO waarbij over de resultaten van deze toetsing horizontale (van college aan de raad) en verticale (naar Logius) verantwoording plaatsvindt.

Bijlage II - Gebruikte documentatie

- Template “Voorbeeld IB&P beleid” van Vereniging van Nederlandse Gemeenten Informatiebeveiligingsdienst (IBD), licentie onder: CC BY-NC-SA 4.0. (9 juni 2023)
- Privacybeleid 2020-2024
- Strategisch Informatiebeveiligingsbeleid 2020-2024
- Bijlage bij Strategisch Informatiebeveiligingsbeleid (B.01 norm)
- Baseline Informatiebeveiliging Overheid (BIO) GAP analyse rapportage 2023
- Mens centraal digitaal document - S. Katus, PMPartners
- Forum voor standaardisatie informatiebeveiliging standaarden
- NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)
- Three Lines Model – Institute of Internal Auditors (IIA)
- VNG Borgingsproduct AVG versie 3.0
- Beginselen uit de AVG voor het verwerken van persoonsgegevens
- De 10 bestuurlijke principes voor informatiebeveiliging van de VNG
- https://www.bio-overheid.nl/
- VNG rapport uitvoeringsanalyse regelgeving informatiebeveiliging Digital Decade
- CMT besluit over processenlandschap en processenlijst is genomen op 20-07-2022