

Artikel 1 Definitie en begripsbepalingen

1. Deze verordening strekt tot nadere uitwerking van de Algemene Verordening Gegevensbescherming (hierna: de AVG). De in de AVG opgenomen definities zijn onverkort van toepassing.
2. Deze verordening verstaat onder:
 - a. Anonimiseren: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data.
 - b. AP: de Autoriteit Persoonsgegevens, op grond van de uitvoeringswet Algemene verordening gegevensbescherming bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de AVG bepaalde (voorheen: College bescherming persoonsgegevens).
 - c. Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
 - d. CIO: Chief Information Officer, zijnde de concernmanager informatievoorziening en procesmanagement, aangewezen door het college van burgemeester en wethouders.
 - e. CISO: Chief Information Security Officer, zijnde het hoofd informatiebeveiliging, aangewezen door het college van burgemeester en wethouders.
 - f. Dataminimalisatie: alleen de informatie die noodzakelijk is voor de uitvoering van wettelijke taken wordt opgeslagen.
 - g. IRM-er: integraal resultaatsverantwoordelijk manager, verantwoordelijk voor een organisatieonderdeel van de gemeente Hilversum, of daarmee gelijk te stellen functies.
 - h. Data Protection impact assessment (DPIA): een analyse van de gevolgen voor privacy als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.
 - i. Pseudonimiseren: een procedure waarmee identificerende gegevens met behulp van een bepaald algoritme in een dataset worden vervangen door versleutelde gegevens (het pseudoniem).
 - j. Tracking: het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.
 - k. Blockchain: een technologie als een gedistribueerde database die een gestaag groeiende lijst bijhoudt van data-items die gehard zijn tegen manipulatie en vervalsing.

Artikel 2 Verantwoordelijke

De verantwoordelijke voor de verwerking van persoonsgegevens, zoals bedoeld in de AVG, is het college van burgemeester en wethouders, respectievelijk de burgemeester.

Artikel 3 Functionaris voor de gegevensbescherming

Het college van burgemeester en wethouders benoemt een functionaris van de gegevensbescherming, zoals bedoeld in de AVG, die belast is met toezicht op privacy- en beveiligingsbeleid van de gemeente.

Artikel 4 Contactpersoon voor de gegevensbescherming

1. Elk organisatieonderdeel heeft een contactpersoon die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.
2. Tot de taken van de contactpersoon behoren in ieder geval:
 - a. Het onderhouden en aanvullen van de groslijst met alle verwerkingen die binnen het organisatieonderdeel zijn geïnventariseerd.
 - b. Het beoordelen van nieuwe of aangepaste verwerkingen in het licht van de meldplicht en andere verplichtingen.
 - c. Het opstellen van en het houden van toezicht op het gebruik van privacyprotocollen voor verwerkingen die onder verantwoordelijkheid van het organisatieonderdeel plaatsvinden.
 - d. De informatiebeveiliging van het organisatieonderdeel. Hieronder vallen in ieder geval:
 - i. Informatiebeveiligingsbeleid van Hilversum opnemen en doorvoeren in contracten met bewerkers en leveranciers;
 - ii. Alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan.

Artikel 5 Data Protection impact assessment (DPIA)

1. Voordat een beslissing wordt genomen over een nieuw of te wijziging van bestaande bewerkingen, wordt door middel van een DPIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.
2. De functionaris voor de gegevensbescherming geeft over de DPIA een bindend advies.
3. De DPIA wordt openbaar gemaakt nadat de beslissing als bedoeld onder lid 1 is genomen.

Artikel 6 Open Data

1. Hergebruik van gegevens zoals bedoeld in de Wet hergebruik van overheidsgegevens via het aanbieden van open data gebeurt met inachtneming van de AVG en deze verordening
2. Een openbare dataset bevat geen gegevens die herleidbaar zijn naar een persoon.
3. Van open datasets wordt de status van de dataset voor de afnemer weergegeven op de site waarop de open datasets zijn te verkrijgen.

Artikel 7 Big data en tracking

1. Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens gemeente wordt uitgevoerd.
2. Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.
3. Brongegevens die gebruikt worden voor big data toepassingen worden omgezet

- tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is.
4. Indien het noodzakelijk is om van lid 3 af te wijken wordt vooraf toestemming aangevraagd bij de functionaris gegevensbescherming die de aanvraag zal beoordelen in het kader van de wet en doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.
 5. Onderzoek aan de hand van de dataset als bedoeld in lid 3, mag alleen door andere dan de in lid 2 bedoelde geautoriseerde personen worden uitgevoerd.
 6. Alle afspraken met andere partijen over big data en tracking dienen openbaar te worden gemaakt.
 7. Een afspraak met andere partijen over big data en tracking gaat in ieder geval in op:
 - De organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
 - De bewaartermijn;
 - De wijze waarop voldaan wordt aan de meldplicht datalekken, waarbij ieder datalek ook aan de gemeente wordt gemeld;
 - Het verzamel- en verwerkingsdoel;
 - Welke gegevens worden verzameld;
 8. Indien in de openbare ruimte door big data en tracking persoonsgegevens worden verwerkt, dient de persoon die de desbetreffende openbare ruimte betreedt:
 - te worden geïnformeerd over de verwerking van persoonsgegevens zoals bedoeld in de AVG en artikel 17 van deze verordening;
 - toestemming voor de verwerking van persoonsgegevens te hebben gegeven zoals bedoeld in de AVG en artikel 15 van deze verordening.

Artikel 8 Cameratoezicht, Camerabewaking en overige inzet van camera's

1. Camerabewaking kan door particuliere bedrijven worden uitgevoerd onder voorwaarde dat indien er camera's in de openbare ruimte worden gebracht dan wel de camera de openbare ruimte of delen daarvan filmt, er een daartoe strekkend besluit door of namens het college van burgemeester en wethouders is genomen en er een convenant met de verantwoordelijke is afgesloten voorafgaand aan de verwerking.
2. Het convenant zoals bedoeld in het eerste lid gaat in ieder geval in op:
 - De grondslag voor de verwerking van persoonsgegevens;
 - Het verzamel- en verwerkingsdoel;
 - De organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
 - De bewaartermijn;
 - De wijze waarop voldaan wordt aan de meldplicht datalekken.
3. Voor de camera's zoals bedoeld in het eerste lid die voor de inwerkingtredingsdatum van deze verordening zijn opgehangen, geldt dat het convenant zoals bedoeld in het eerste lid binnen drie jaar na de inwerkingtredingsdatum van deze verordening dient te zijn afgesloten.

Artikel 9 Datalekken

1. Geconstateerde en veronderstelde datalekken worden terstond gemeld bij de functionaris voor de gegevensbescherming.
2. De IRM-er is verantwoordelijk voor het dichten van het datalek in samenwerking

met de CISO.

3. De functionaris voor de gegevensbescherming meldt alle datalekken direct aan de Autoriteit Persoonsgegevens.
4. De IRM-er is verantwoordelijk voor de onverwijld melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt. De betrokkene dient daarbij op de hoogte te worden gesteld van de specifieke persoonsgegevens waartoe onbevoegd toegang is verkregen en wat de gevolgen hiervan kunnen zijn.
5. De CISO ziet er samen met de CIO op toe dat het datalek op adequate wijze wordt gedicht.

Artikel 10 Toezicht

1. Voor de uitoefening van zijn toezichthoudende functie beschikt de functionaris voor de gegevensbescherming over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. Ingeval van twijfel of verschil van mening daaromtrent beslist de functionaris voor de gegevensbescherming, de CIO gehoord hebbende.
2. De verantwoordelijke en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken desgevraagd de functionaris voor de gegevensbescherming alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.
3. De functionaris voor de gegevensbescherming heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. De functionaris voor de gegevensbescherming is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.
4. De functionaris voor de gegevensbescherming rapporteert over zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft aanbevelingen over te nemen maatregelen, die een goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen.

Artikel 11 Onderzoek

1. De functionaris voor de gegevensbescherming kan een onderzoek instellen naar de wijze waarop in verband met de verwerking van persoonsgegevens, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd.
2. De functionaris voor de gegevensbescherming kan voor zijn onderzoek gebruik maken van de diensten van derden.
3. De functionaris voor de gegevensbescherming deelt zijn bevindingen aan de Verantwoordelijke mede en geeft zo nodig aanbevelingen.
4. De bevindingen van de functionaris voor de gegevensbescherming alsmede de aanbevelingen zijn naderhand te raadplegen via de website van de gemeente. De functionaris voor de gegevensbescherming kan dit achterwege laten vanwege dringende redenen.

Artikel 12 Openbaar register verwerkingen

De functionaris voor de gegevensbescherming schrijft namens de verantwoordelijke de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register.

Artikel 13 Logboek datalekken

1. De functionaris voor de gegevensbescherming houdt namens de verantwoordelijke een logboek bij waarin datalekken zijn opgenomen.
2. In het logboek worden in ieder geval de volgende gegevens vermeld:
 - a. Het onderwerp van het datalek;
 - b. De datum van het datalek;
 - c. De duur van het datalek;
 - d. de aard van de inbreuk;
 - e. de instanties waar meer informatie over de inbreuk kan worden verkregen;
 - f. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken;
 - g. een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
 - h. de maatregelen die de gemeente heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
 - i. de kennisgeving aan betrokkenen.

Artikel 14 Rechten betrokkene

1. De taken zoals omschreven in artikel 15 van de AVG en volgende worden centraal uitgevoerd onder verantwoordelijkheid van de CIO
2. Bij uitvoering van de taken wordt de functionaris van de gegevensbescherming betrokken
3. Een betrokkene kan een verzoek zoals bedoeld in artikel 15 van de AVG ook via andere gangbare publieksdienstverleningkanalen van de gemeente Hilversum doen. Dit verzoek is geldig ongeacht het middel waarmee het wordt gedaan.

Artikel 15 Toestemming

1. De gemeente vraagt toestemming waar nodig. Indien beroep kan worden gedaan op een andere wettelijke grondslag zoals omschreven in artikel 6(1) van de AVG, verdient dat de voorkeur.
2. Indien voor de verwerking van persoonsgegevens toestemming aan de betrokkene wordt gevraagd, dient de toestemming te voldoen aan de volgende voorwaarden:
 - a. De betrokkene verkeert niet onder druk van omstandigheden om toestemming te verlenen;
 - b. De toestemming dient een specifiek doel;
 - c. De betrokkene is duidelijk geïnformeerd en daarbij wordt voldaan aan de voorwaarden zoals bedoeld in AVG en artikel 17 van deze verordening.
3. Bij gebruik van toestemming als grondslag voor de verwerking dient de betrokkene vooraf aan de verwerking en expliciet toestemming te hebben gegeven voor de verwerking van de persoonsgegevens.
4. In het geval dat er door de betrokkene toestemming voor het verwerken van persoonsgegevens is verleend, kan de betrokkene ten alle tijden die toestemming intrekken.
5. Indien er geen toestemming is verleend of de toestemming is ingetrokken dan wel er geen andere grondslag voor de verwerking is, worden de persoonsgegevens niet verwerkt.

Artikel 16 Geheimhoudingsplicht

Indien een persoon die uit hoofde van ambt, beroep of wettelijke voorschrift dan wel krachtens een overeenkomst tot geheimhouding is verplicht, voor de verwerking van de persoonsgegevens waarop een geheimhoudingsplicht rust, zijn geheimhoudingsplicht dient te doorbreken, moet gelden dat:

- er een grondslag voor verwerking van persoonsgegevens als bedoeld in artikel 6 van de AVG is;
- er grond is voor de doorbreking van de geheimhoudingsplicht, waaronder begrepen maar niet beperkt tot:
 - a. een wettelijke verplichting tot verstrekken van persoonsgegevens;
 - b. een conflict van plichten;
 - c. toestemming van de betrokkene.

Artikel 17 Informatieverstrekking

1. De betrokkene dient bij de verwerking van zijn persoonsgegevens in alle gevallen te worden geïnformeerd, tenzij dit onmogelijk blijkt.
2. De informatie zoals bedoeld in lid 1 van dit artikel gaat ten minste in op:
 - Het doel van de verwerking;
 - De rechten van de betrokkene.
3. De informatie zoals bedoeld in lid 1 is specifiek bedoeld voor de betrokkene. De betrokkene kan niet worden aangesproken als onderdeel van het algemene publiek.
4. In afwijking van lid 3 van dit artikel kan de betrokkene worden aangesproken als onderdeel van het algemeen publiek al er persoonsgegevens worden verwerkt zoals omschreven in artikel 7 van deze verordening.
5. Indien met derden persoonsgegevens worden uitgewisseld, dient de betrokkene te worden geïnformeerd over:
 - aan welke partijen de persoonsgegevens worden opgevraagd dan wel verstrekt;
 - welke persoonsgegevens worden uitgewisseld.

Artikel 18 Derden

1. In gevallen van samenwerking met externe partijen, waarbij sprake is van verwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar de gegevensuitwisseling aan moet voldoen.
2. De afspraken zoals bedoeld in lid 1 gaan in ieder geval in op:
 - De organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
 - De bewaartermijn;
 - De wijze waarop voldaan wordt aan de meldplicht datalekken;
 - Rechten betrokkene;

Artikel 19 Blockchain

De gemeente gebruikt geen Blockchain technologie bij de verwerking van persoonsgegevens.

Artikel 20 Inwerkingtreding

Deze verordening treedt in werking met ingang van de dag na datum van haar bekendmaking.

Artikel 21 citeertitel

Deze verordening wordt aangehaald als: Privacy verordening gemeente Hilversum.

Aldus besloten in de openbare vergadering van (**datum**) van de gemeenteraad van Hilversum,

De griffier,

De voorzitter,

P.M.H. van Ruitenbeek

P.I. Broertjes