

Verordening van de gemeenteraad van de gemeente Harderwijk houdende regels omtrent privacy Privacy verordening Harderwijk 2018

De raad van de gemeente Harderwijk;

gezien het voorstel van burgemeester en wethouders van 22 mei 2018, nummer 18.00249;

gelet op de Algemene verordening gegevensbescherming (EU 2016 / 679);

b e s l u i t:

vast te stellen de volgende

Privacy verordening Harderwijk 2018

Artikel 1 Definitie en begripsbepalingen

Deze verordening strekt tot nadere uitwerking van de Algemene Verordening Gegevensbescherming (hierna: de Wet). De in de Wet opgenomen definities en overige normen zijn onverkort van toepassing. Deze verordening verstaat onder:

Op basis van artikel 4 AVG

- *Persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- *Verwerking*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- *Bestand*: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
- *Verwerkingsverantwoordelijke*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- *Verwerker*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- *Ontvanger*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt;
- *Pseudonimisering*: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Aanvullend

- *De betrokkene*: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt;
- *Domein*: een organisatieonderdeel van de gemeente Harderwijk;
- *Domeindirecteur*: integraal resultaatsverantwoordelijk manager, verantwoordelijk voor een domein;
- *MIZ*: de gemeenschappelijke regeling Meerinzicht die uitvoerder is voor een deel van de bedrijfsvoering van de gemeente Harderwijk en waar uit dien hoofde ook gegevensverwerking plaatsvindt;
- *CISO*: Chief Information Security Officer, verantwoordelijk voor informatiebeveiliging, in dienst bij MIZ;



- *FG*: Functionaris Gegevensbescherming, de door het college van B&W aangestelde functionaris, die namens het college toezicht op de verwerking van persoonsgegevens en als zodanig is aangemeld bij de AP;
- *AP*: de Autoriteit Persoonsgegevens, op grond van de Wet bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde;
- *Gegevensbeschermingseffectbeoordeling*: met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit wordt ook wel een Privacy Impact Assessment (PIA) of een Data Protection Impact Assessment (DPIA) genoemd;
- *BIG*: Baseline Informatiebeveiliging Gemeenten; de set van afspraken tussen gemeenten ten aanzien van het niveau van informatiebeveiliging;
- *Big data*: we spreken over Big data als het gaat om minimaal twee van de drie factoren: (1) een grote hoeveelheid van data/gegevens die (2) in principe ongestructureerd worden opgeslagen en (3) snel binnenkomen en/of kunnen worden opgevraagd;
- *Anonimiseren*: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel kunnen worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data.

Artikel 2. Reikwijdte van de verordening

Deze verordening is van toepassing op alle verwerkingen van persoonsgegevens die binnen de gemeente en indien mogelijk op basis van verwerkingsovereenkomsten ook binnen de ketenpartners als MIZ, ODNV, VNOG etc. plaatsvinden en die vallen onder de werkingssfeer van de wet.

Artikel 3. Algemene beginselen

1. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
2. Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.
3. Persoonsgegevens worden slechts verwerkt indien daarvoor op grond van artikel 6 van de wet een rechtmatige grondslag aanwezig is.
4. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
5. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.
6. Persoonsgegevens worden slechts verwerkt voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
7. De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden behoudens het bepaalde in de wet. Hetzelfde geldt voor strafrechtelijke gegevens of daarmee verband houdende veiligheidsmaatregelen.

Artikel 4 Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens, zoals bedoeld in de Wet, is het college van burgemeester en wethouders, respectievelijk de burgemeester. De domeindirecteuren zijn gemandateerd verantwoordelijk voor de verwerking van persoonsgegevens binnen hun domein.

Artikel 5 Geheimhoudingsplicht.

De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de verwerkingsverantwoordelijke, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking gehouden is.

Artikel 6 Beveiliging

1. De verantwoordelijke zorgt voor een passende beveiliging van persoonsgegevens door middel van het hebben, onderhouden en naleven van een gemeentebreed informatiebeveiligingsbeleid conform de BIG. Deze maatregelen garanderen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich mee brengen. De verantwoordelijke ziet toe op de naleving van die maatregelen.
2. In het informatiebeveiligingsbeleid is vastgelegd:
 - a. wie bestuurlijk en op directieniveau eindverantwoordelijk is voor gemeentebrede informatiebeveiliging, waaronder de beveiliging van persoonsgegevens;



- b. dat een functioneel overleg (zoals opgenomen in paragraaf 2.3 Informatiebeveiligingsbeleid gemeente Harderwijk) verantwoordelijk is voor advisering over gemeentebrede informatiebeveiliging;
 - c. hoe de informatiebeveiligingsorganisatie verder is ingevuld;
 - d. hoe de planning en control van de gemeentebrede informatiebeveiliging is geregeld.
3. De FG maakt onderdeel uit van de onder lid 2b. genoemde functioneel overleg.
 4. De verwerking door een verwerker wordt geregeld in een schriftelijke overeenkomst of een andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt.

Artikel 7 Rechten betrokkene

Een betrokkene kan een verzoek over verwerking van zijn persoonsgegevens aan de gemeente doen. Dit verzoek kan betreffen: informatie over, inzage in, correctie van, overdracht van, verzet tegen, vergeten worden en bezwaar tegen, de verwerking of wijze van verwerking van zijn/haar persoonsgegevens.

Artikel 8 Klachten

Klachten met betrekking tot de wijze waarop de gemeente met persoonsgegevens om gaat kunnen worden ingediend bij de Functionaris voor Gegevensbescherming.

Artikel 9. Functionaris voor de gegevensbescherming (FG)

1. Het college van burgemeester en wethouders benoemt een FG die belast is met het toezicht op het privacy- en informatiebeveiligingsbeleid van de gemeente. Tot de taken van de FG behoren op grond van artikel 39 AVG:
 - a. de verantwoordelijke informeren en adviseren over hun verplichtingen uit hoofde van de wet;
 - b. toezien op de naleving van privacywetgeving en van het privacybeleid;
 - c. desgevraagd adviseren over de PIA en toezien op de uitvoering daarvan;
 - d. Samenwerken met de AP
 - e. optreden als contactpunt voor de AP
2. Aanvullende taken van de FG in het kader van deze verordening:
 - a. aanspreekpunt voor alle zaken de bescherming van de persoonlijke levenssfeer betreffende;
 - b. toezien op het onderhouden en aanvullen van het register met alle verwerkingen die binnen de te onderscheiden domeinen zijn geïnventariseerd.

Artikel 10. Contactpersoon Privacy

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

Artikel 11 Het register van verwerkingen

1. De verantwoordelijke houdt een register van verwerkingen van persoonsgegevens bij, waarop deze verordening van toepassing is.
2. Bij die inschrijving worden in ieder geval de volgende gegevens vermeld:
 - a. de naam en contactgegevens van de verwerkingsverantwoordelijke en indien van toepassing, de gezamenlijke verwerkingsverantwoordelijke;
 - b. de doelen van de verwerking;
 - c. een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
 - d. een beschrijving van de ontvangers van de persoonsgegevens;



- e. een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
 - f. de termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
 - g. een algemene beschrijving van de beveiligingsmaatregelen.
3. Het college van burgemeester en wethouders besluit tot doorhaling van een verwerking in het register van verwerkingen indien de verwerking wordt opgeheven.

Artikel 12 Gegevensbeschermingseffectbeoordeling

1. Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande verwerkingen als bedoeld in artikel 35 van de AVG, wordt door middel van een Gegevensbeschermingseffectbeoordeling (of Privacy Impact Assessment, hierna PIA) aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.
2. De FG geeft over de PIA een advies aan de verantwoordelijke.

Artikel 13 Open data

1. De gemeente kan hergebruik van gegevens, zoals bedoeld in de Wet hergebruik van overheidsgegevens, aanbieden 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 (beschikbaar, in onderzoek, niet beschikbaar, gepland) van de dataset voor de afnemer weergegeven op de site waarop de open datasets zijn te verkrijgen.

Artikel 14 Big data & Tracking

1. Gegevens in big data 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 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 worden.
5. Onderzoek aan de hand van de dataset als bedoeld in lid 3, mag alleen door anderen dan de in lid 2 bedoelde geautoriseerde personen worden uitgevoerd.
6. Tracking wordt door de gemeente niet toegepast.

Artikel 15 Cameratoezicht, camerabewaking en overige inzet van camera's

1. Cameratoezicht in de openbare ruimte of waarbij de openbare ruimte geheel of gedeeltelijk in beeld wordt gebracht ten behoeve van de openbare orde of veiligheid vindt alleen door of namens de gemeente plaats, na een daartoe strekkend besluit van de burgemeester.
2. Bij inzet van camera's voor andere gemeentelijke doeleinden adviseert de FG voorafgaand aan deze inzet.

Artikel 16 Datalek

1. Geconstateerde datalekken worden terstond gemeld bij de CISO.
2. De domeindirecteur is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO.
3. De domeindirecteur beoordeelt of het datalek meldingswaardig is, als bedoeld in de Wet en laat zich daarbij adviseren door de FG.
4. De FG meldt een meldingswaardig datalek direct aan de Autoriteit Persoonsgegevens.
5. De domeindirecteur is verantwoordelijk voor de onverwijld melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt.

Artikel 17 Logboek datalekken

1. De CISO houdt namens de verantwoordelijke een logboek bij waarin beveiligingsincidenten zijn opgenomen.
2. Indien het beveiligingsincident persoonsgegevens betreft wordt in ieder geval in het logboek 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. 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 en in de toekomst te voorkomen;
- i. De kennisgeving aan betrokkenen.

Artikel 18 Toezicht

1. Voor de uitoefening van zijn toezichhoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn.
2. De personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken desgevraagd de FG alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.
3. De FG heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.
4. De FG 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 19 Onderzoek

1. De FG 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 FG kan voor zijn onderzoek gebruik maken van de diensten van derden.
3. De FG deelt zijn bevindingen aan de verwerkingsverantwoordelijke mede en geeft zo nodig aanbevelingen.

Artikel 20 Inwerkingtreding

Deze verordening treedt in werking met ingang van de dag na de datum van haar bekendmaking en vervangt de "Verordening op de verwerking van persoonsgegevens Harderwijk", die hiermee wordt ingetrokken.

Artikel 21 Citeertitel

Deze verordening wordt aangehaald als: 'Privacy verordening Harderwijk 2018'.

*Aldus vastgesteld door de raad van de gemeente
Harderwijk in zijn openbare vergadering van
12 juli 2018,*

*de heer H.J. van Schaik
voorzitter*

*de heer H.R. Lanning
raadsgriffier*