Privacyverordening

De raad van de gemeente Noardeast-Fryslân,
gelet op artikel 149 Gemeentewet;

Besluit

Vast te stellen de volgende
PRIVACYVERORDENING gemeente NOARDEAST-FRYSLÂN

Artikel 1 Definitie en begripsbepalingen

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

1.2 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 AVG bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde (voorheen: College bescherming persoonsgegevens).

c. Informatieveiligheid omvat de informatiebeveiliging en de gegevensbescherming in het kader van privacy.

d. CISO: Chief Information Security Officer.

e. Dataminimalisatie: alleen de persoonsinformatie die noodzakelijk is voor de uitvoering van wettelijke taken wordt verwerkt.

f. FG: Functionaris Gegevensbescherming, aangewezen door het college van burgemeester en wethouders, als zodanig geregistreerd bij de Autoriteit Persoonsgegevens.

g. MT-er: integraal resultaatsverantwoordelijk manager, verantwoordelijk voor één of meer organisatieonderdelen van de DDFK-organisatie, of daarmee gelijk te stellen functies.

h. Privacy impact assessment (PIA): 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 matigingsacties 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).

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 gegevensbescherming

a. Het college van burgemeester en wethouders benoemt een FG, zoals bepaald in artikel 37 van de AVG, die belast is met toezicht op het privacybeleid van de gemeente.

b. Het college van burgemeester en wethouders, respectievelijk de directie, benoemt een CISO, die belast is met toezicht op het beveiligingsbeleid van de gemeente.

Artikel 4 Beheerder informatieveiligheid

1. Elk organisatieonderdeel, afdeling of team, heeft een contactpersoon – beheerder informatieveiligheid – die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.

2. Tot de taken en verantwoordelijkheden van de beheerder informatieveiligheid behoren in ieder geval:

het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid en het onderliggende informatieveiligheidsplan. Hieronder vallen preventie van informatieveiligheidsincidenten, de detectie van dergelijke incidenten en het geven van adequate respons. De beheerder informatieveiligheid coördineert de toepassing van specifieke wet- en regelgeving. De beheerder informatieveiligheid rapporteert aan de CISO en de FG.

Meer specifiek:

a. het (laten) opstellen van specifiek privacybeleid voor het organisatieonderdeel;

b. ondersteunt bij en wordt geconsulteerd bij de uitvoering van PIA's;

c. onderhoudt en vult het Register van Verwerkingsactiviteiten met alle verwerkingen van persoonsgegevens die binnen het organisatieonderdeel zijn geïnventariseerd;

d. beoordeelt nieuwe of aangepaste verwerkingen voor opname in het Register van Verwerkingsactiviteiten en andere verplichtingen;

e. stelt op en houdt eerste lijns toezicht op het gebruik van privacy protocollen voor verwerkingen die onder de verantwoordelijkheid van het organisatieonderdeel plaatsvinden;

f. consulteert de FG bij de uitvoering van werkzaamheden betreffende de AVG;

g. de informatiebeveiliging van het organisatieonderdeel. Hieronder vallen in ieder geval:

o informatiebeveiligingsbeleid van de DDFK-gemeenten (laten) opnemen en doorvoeren in contracten met bewerkers en leveranciers;

o het melden van datalekken die het organisatieonderdeel aangaan bij de CISO en de FG;

h. consulteert de CISO bij de uitvoering van werkzaamheden betreffende informatiebeveiliging.

Artikel 5 Privacy impact assessment (PIA)

1. Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande bewerkingen, wordt door middel van een 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 bindend advies.

3. De PIA is openbaar ingevolge de Wet Openbaarheid van Bestuur (WOB) nadat de beslissing als bedoeld onder lid 1 is genomen.

Artikel 6 Datalek

1. Geconstateerde datalekken worden terstond gemeld bij de CISO en de FG.

2. De MT-er is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO en FG, zo nodig ondersteunt door vakspecialisten van andere disciplines.

3. De CISO ziet er op toe dat het datalek op adequate wijze wordt gedicht.

4. De FG beoordeelt of het datalek meldingswaardig is zoals bedoeld in de AVG, specifiek de Meldplicht Datalekken.

5. De FG meldt een meldingswaardig datalek binnen 72 uur aan de Autoriteit Persoonsgegevens. De CISO kan hierbij als zijn vervanger optreden.

6. De MT-er is, indien nodig, verantwoordelijk voor de onverwijlde melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt.

Artikel 7 Toezicht

1. Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden zoals in de AVG omschreven.

2. De verantwoordelijke en 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 de goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen conform artikel 4 lid 2 AVG.

Artikel 8 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 Verantwoordelijke mede en geeft zo nodig aanbevelingen.

Artikel 9 Register van Verwerkingsactiviteiten

De FG houdt namens de Verantwoordelijke toezicht op het tijdig, juist en volledig muteren van verwerkingen van persoonsgegevens in het Register van Verwerkingsactiviteiten conform de eisen van de AVG. Hiermee wordt de transparantie van het verwerken van persoonsgegevens geborgd.

Artikel 10 Logboek datalekken

1. De FG houdt namens de Verantwoordelijke een logboek bij waarin datalekken zijn opgenomen.

2. In het logboek worden in ieder geval de volgende gegevens vermeld:

o het onderwerp van het datalek;

o de datum van het datalek;

o de duur van het datalek;

o de aard van de inbreuk;

o de instanties waar meer informatie over de inbreuk kan worden verkregen;

o de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;

o een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;

o de maatregelen die de gemeente daadwerkelijk heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;

o de kennisgeving aan betrokkenen, indien nodig.

Artikel 11 Rechten betrokkene

1. De taken zoals omschreven in hoofdstuk 3 AVG, ‘Rechten van de betrokkene’, worden onder verantwoordelijkheid van de leidinggevende door het betreffende organisatieonderdeel uitgevoerd.

2. Bij uitoefening van deze taken wordt de FG geconsulteerd.

Artikel 12 Inwerkingtreding

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

Artikel 13 Citeertitel

Deze verordening wordt aangehaald als: Privacyverordening gemeente Noardeast-Fryslân.

Aldus besloten door de raad van de gemeente Noardeast-Fryslân in zijn openbare vergadering d.d. .3 december 2020

Aldus besloten door de raad van de gemeente Noardeast-Fryslân in zijn openbare vergadering

d.d. 3 december 2020.

De raad voornoemd,

de adjunct-griffier,

Signed By: Toren, Tineke <t.toren@noardeast-fryslan.nl>
16/12/2020 12:04:39 CET
ID: 70176a6f-b44d-48dc-93af-dc3380beee54
Auth: Scribble

mw. T. Toren

de voorzitter,

Signed By: Kramer, Johannes <j.kramer@noardeast-fryslan.nl>
16/12/2020 13:22:46 CET
ID: 70176a6f-b44d-48dc-93af-dc3380beee54
Auth: Scribble

mr. J.G. Kramer

Toelichting

Artikel 1 Definitie en begripsbepalingen

Behoeft, uitgezonderd pseudonimiseren, geen nadere toelichting. Pseudonimiseren is noodzakelijk indien datasets vergeleken moeten worden. Dit kan bijvoorbeeld gedaan worden binnen het sociaal domein. De gemeente wil de zorg die wordt geboden door de instellingen controleren door gericht onderzoek waarbij vaak meerdere datasets worden gebruikt.

Artikel 2 Verantwoordelijke

Het college van burgemeester en wethouders dan wel de burgemeester zijn, ieder vanuit hun eigen bevoegdheid, te allen tijde Verantwoordelijke voor de verwerkingen en bewerkingen die door of namens de gemeente worden uitgevoerd.

Artikel 3 Functionaris voor de gegevensbescherming

De gemeente heeft een functionaris voor de gegevensbescherming (FG) benoemd die verantwoordelijk is voor het toezicht op privacy en de borging er van. De FG staat als zodanig geregistreerd bij de Autoriteit Persoonsgegevens. Hij kan het college van burgemeester en wethouders en de burgemeester gevraagd en ongevraagd advies geven over privacyaangelegenheden.
De FG heeft verregaande bevoegdheden op grond van de AVG. In artikel 38 lid 3 AVG wordt zijn onafhankelijke rol benadrukt; “De functionaris kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Hij ondervindt geen nadeel van de uitoefening van zijn taak. De verantwoordelijke stelt de functionaris in de gelegenheid zijn taak naar behoren te vervullen.”
Hoewel de FG een eigen rol kent, treedt hij in overleg met de CISO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.
Tot de taken van de FG behoren in ieder geval:
1. Toezicht op de verwerking van persoonsgegevens door de gemeente Noardeast-Fryslân.
2. Gevraagd en ongevraagd signaleren, adviseren en informeren over zaken aangaande de AVG, deze verordening en overige onderwerpen die de privacy betreffen.
3. Toezicht houden op het gemeentelijk privacy-veiligheidsbeleid door middel van advisering en controles.
4. Toezicht houden op de inventarisatie van de verwerkingsprocessen en het beheer daarvan in het Register van Verwerkingsactiviteiten.
5. Is verantwoordelijk voor meldingsplicht in geval van datalekken en het beheren van het logbook inzake datalekken.
6. Aanspreekpunt en contactpersoon aangaande privacy, zowel intern als extern, in het bijzonder voor de Autoriteit Persoonsgegevens.

Artikel 4 Beheerder Informatieveiligheid

De beheerder informatieveiligheid is een medewerker die werkzaam is binnen de gemeente onder verantwoordelijkheid van de MT-er van een organisatieonderdeel. Hij/Zij is verantwoordelijk voor borging van de privacy en informatiebeveiliging bij het betreffende organisatieonderdeel. De beheerders informatieveiligheid hebben regelmatig overleg met de CISO en de FG en dragen bij aan een eenduidige uitvoering van het informatiebeveiligings- en privacybeleid door de organisatie.

Artikel 5 Privacy Impact Assessment (PIA)

Voordat wordt besloten om met een verwerking van persoonsgegevens te beginnen of te wijzigen, wordt door het organisatieonderdeel een privacy impact assessment (PIA) uitgevoerd. Uitgangspunt bij een PIA is dat afhankelijk van de verwerking passende waarborgen worden ingebouwd (privacy by design). Bij iedere verwerking van persoonsgegevens wordt dataminimalisatie toegepast. Daarnaast worden binnen die minimale dataset – waar mogelijk – de persoonsgegevens eerst geanonimiseerd en worden de overige persoonsgegevens gepseudonimiseerd. Deze keuzes worden onderbouwd voorgelegd aan de FG, die mede beslist over de inhoud van de PIA.
De PIA legt in de eerste plaats de risico's bloot van projecten waarbinnen wordt gewerkt met persoonsgegevens, en het draagt bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden die worden gegeven in de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe groot deze kans is en op welke gebieden dit speelt. De PIA doet dit door op een gestructureerde wijze:
o De mogelijke (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokkene personen en organisaties in kaart te brengen;
o De risico's voor de betrokken personen en organisaties zoveel mogelijk te lokaliseren. Op basis van de uitkomsten van de PIA kan de gemeente gericht acties ondernemen om deze risico's te verminderen. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project. De PIA is openbaar met inachtneming van de Wet openbaarheid van bestuur.
In ieder geval worden de volgende gegevens van verwerkingen openbaar:
1. de reden om de persoonsgegevens te bewaren;
2. bewaartermijnen en een motivering waarom voor die bewaartermijn gekozen is met zo mogelijk een verwijzing naar het wettelijk kader;
3. mogelijke uitzonderingen op de gekozen bewaartermijn met uiteenzetting van de voorwaarden waaronder langer bewaard kan worden;
4. een verwijzing naar de persoon bij wie een betrokkene een verzoek kan indienen als hij inzage wil hebben in verwerkingen die hem aangaan;
Er zal gebruik worden gemaakt van de PIA die door de Informatie Beveiligings Dienst (IBD) wordt aanbevolen. De IBD is onderdeel van VNG-realisatie.
De FG ziet toe op het proces en geeft een bindend advies over de PIA.

Artikel 6. Datalek

Op 1 januari 2016 is de Wet bescherming persoonsgegevens gewijzigd als gevolg van de Wet meldplicht datalekken en uitbreiding van de bestuurlijke boetebevoegdheid van de Autoriteit Persoonsgegevens (hierna te noemen AP). Het vervolg hierop is per 25 mei 2016 opgenomen in de Algemene Verordening Gegevensbescherming.
Belangrijk gevolg hiervan is dat organisaties verplicht zijn om een inbreuk op de beveiliging te melden, wanneer het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. De melding moet aan de AP worden gedaan. In sommige gevallen moeten de betrokkenen op de hoogte worden gebracht wiens persoonsgegevens zijn gelekt, namelijk als de inbreuk ongunstige gevolgen voor betrokkenen met zich mee brengt. Indien de regels niet of onvoldoende worden nageleefd kan de AP een forse boete opleggen.
Zowel private als publieke organisaties worden verplicht om inbreuken in de beveiliging die leiden tot verlies, misbruik of diefstal, te melden bij de AP, indien het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. Melding dient binnen 72 uur plaats te vinden.

Melden mag ook later maar dan moet gemotiveerd worden waarom de melding is uitgesteld. Daarnaast moet ook degene wiens persoonsgegevens het betreft een melding krijgen, wanneer er (waarschijnlijk) sprake zal zijn van ongunstige gevolgen voor zijn of haar privacy.

Wat is een datalek?
Er is sprake van een datalek als het gaat om een beveiligingslek waarbij persoonsgegevens in handen vallen van derden die geen toegang tot die persoonsgegevens zouden mogen hebben. Persoonsgegevens zijn alle gegevens die direct of indirect naar personen zijn te herleiden. Een datalek is het gevolg van een beveiligingsprobleem of een gebruikersfout. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen.
Illegaal verkregen bedrijfsgegevens over een productieproces of marktstrategie betreffen kostbare informatie, maar vallen niet onder de gangbare definitie van datalek.

Wanneer is er sprake van inbreuk op de beveiliging?
Een inbreuk op de beveiliging hoeft niet te betekenen dat de beveiliging is tekort geschoten. Denkbaar is dat de beveiliging op zich van voldoende niveau is, maar dat de beveiligingsmaatregelen worden omzeild. In de toelichting bij de meldplicht datalekken wordt als voorbeeld genoemd: een hack van een ICT-systeem dat persoonsgegevens bevat en de diefstal van een laptop of mobiele telefoon uit een afgesloten kluisje. Daarnaast kan de inbreuk op de beveiliging het gevolg zijn van een tekortschietende beveiliging. Dat is bijvoorbeeld het geval als bepaalde bestanden niet goed beveiligd zijn geweest of als er menselijke fouten zijn gemaakt.
Als voorbeelden kunnen worden genoemd: het slordig omgaan met wachtwoorden, papieren dossiers die (deels) als oud papier worden aangeboden, het kwijtraken van apparaten of gegevensdragers met privacygevoelige informatie, een USB-stick, laptop, tablet, telefoon. Ook het onversleuteld elektronisch uitwisselen van privacygevoelige informatie valt hieronder, bijvoorbeeld via e-mail of andere onbeveiligde verbindingen.
Op de hierboven genoemde situaties is de meldplicht van toepassing. Uitsluitend wanneer de getroffen voorzieningen niet specifiek bedoeld zijn voor de beveiliging van persoonsgegevens hoeft geen melding te worden gedaan.
De gemeente verwerkt veel persoonsgegevens van inwoners om haar taken uit te kunnen oefenen. Inwoners hebben recht op bescherming van hun persoonsgegevens. Daarom is de gemeente verplicht om persoonsgegevens goed te beveiligen. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.
Ook voor partijen die in opdracht van de gemeente persoonsgegevens verwerken (verwerkers) brengt de wetgeving indirect verplichting met zich mee. Denk bijvoorbeeld aan leveranciers van ICT systemen. Hier dienen schriftelijke afspraken over te zijn gemaakt, zodat bij een eventueel datalek de gemeente onmiddellijk wordt ingelicht door de dienstverlener teneinde te bepalen of er daadwerkelijk een datalekmelding moet worden gedaan. De leverancier zal de gemeente dan per ommegaande moeten waarschuwen als zij een inbreuk vaststelt.
De Autoriteit Persoonsgevens kan bij nalatigheid om aan haar te melden een boete opleggen als genoemd in artikel 83 van de AVG.
NB: deze boete staat los van de boete die geldt voor het datalekken zelf. Afhankelijk van de aard en omvang van het datalek kan de AP hiervoor ook een boete opleggen als genoemd in artikel 83 van de AVG.

Wie meldt een datalek?
Iedereen kan aan de gemeente een datalek melden. Zowel interne medewerkers als andere personen die een mogelijk datalek constateren kunnen een melding doen via de gebruikelijke dienstverleningskanalen

zoals e-mail, telefoon etc. Voor medewerkers is daarnaast nog een laagdrempelig meldingssysteem (Topdesk) ingeregeld. De FG is degene die meldt bij de AP, waarbij de CISO als zijn vervanger kan optreden.

Meldingsplicht of niet
Niet elk datalek moet bij de AP worden gemeld. Nodeloze meldingen moeten worden voorkomen. Er dient aan bepaalde criteria te worden voldaan. De FG zal, zonodig in overleg met de CISO / Kernteam informatieveiligheid, bepalen of een melding aan de AP noodzakelijk is aan de hand van criteria die door de AP zijn vastgesteld.
De FG houdt een overzicht bij van de datalekken. Dit overzicht wordt, vanuit archief technisch oogpunt, permanent bewaard. De meldingsdossiers (meldingsformulier en andere relevante stukken) over de datalekken worden gedurende zeven jaar na het vervallen van het belang bewaard.

Artikel 7 Toezicht

De FG is belast met het toezicht op alle privacyaspecten binnen de gemeente Noardeast-Fryslân. Hij beoordeelt zelfstandig of de gemeente voldoet aan de AVG en deze verordening. Zijn bevoegdheden zijn verstrekkend, hij kan in het uiterste geval een beslissing overrulen. Dit zal alleen het geval zijn als duidelijk is dat de Autoriteit Persoonsgevens ook niet kan instemmen met de betreffende beslissing op privacy gebied.
De FG zal bij een privacy issue altijd eerst via “de lijn” proberen de situatie op te lossen. Vervolgens zal de MT-er worden gevraagd de beslissing aan te passen en ten slotte zal waar nodig interventie plaatsvinden via de directie of het college.

Artikel 8 Onderzoek

De FG kan een onderzoek instellen naar (schendingen van) privacyaspecten door de gemeente Noardeast-Fryslân. Hij kan hiervoor derden inschakelen die vertrouwelijk met de persoonsgegevenskwestie om kunnen gaan, zoals bijvoorbeeld een accountant die vanuit zijn professie een geheimhoudingsplicht kent. Het onderzoek en mogelijke aanbevelingen kunnen openbaar worden gemaakt. Er kunnen dringende redenen zijn om openbaarmaking vooralsnog achterwege te laten, zoals bijvoorbeeld in het geval het college eerst verregaande maatregelen moet treffen om een mogelijke privacyschending te voorkomen.

Artikel 9 Openbaar Register van Verwerkingsactiviteiten

Alle nieuwe dan wel gewijzigde verwerkingen (werkprocessen) waarin persoonsgegevens worden verwerkt, worden ingevolge artikel 30 AVG opgenomen in het Register van Verwerkingsactiviteiten. De FG houdt toezicht op dit Register.

Artikel 10 Logboek datalekken

De FG houdt een logboek bij van datalekken en stemt dit af met de CISO. Het logboek is openbaar. De FG houdt bij opname in het register rekening met de belangen die bij openbaarmaking zijn gemoeid. Gegevens worden geminimaliseerd en geanonimiseerd. Verder kunnen er bijvoorbeeld redenen zijn om openbaarmaking aan te houden, zoals bijvoorbeeld bij een ernstig datalek dat eerst moet worden gedicht.

Artikel 11 Rechten betrokkene

Betrokkenen kunnen de gemeente verzoeken om inzage te geven in de verwerkingen van hun persoonsgegevens. Dit kan zowel schriftelijk, digitaal als in persoon via de door de gemeente ingerichte dienstverleningskanalen waarbij alle redelijke maatregelen worden genomen om de identiteit te controleren van een betrokkene die om inzage verzoekt.