Gemeente Loon op Zand

Verklaring van Verantwoordelijkheid

(2020)

Verantwoording van Gemeente Loon op Zand aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van privacy

gemeente Loon op Zand

Datum	:	maart 2021
Auteur	:	Richard van Ineveld Functionaris Gegevensbescherming
Status	:	Concept

Voorwoord

Voor u ligt de Verklaring van Verantwoordelijkheid (VvV) over 2020 van de Gemeente Loon op Zand. In de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei 2018 gehandhaafd wordt, is aan iedere organisatie in Europa een verantwoordingsplicht opgelegd ten aanzien van het omgaan met persoonsgegevens en informatiebeveiliging.

Deze Verklaring van Verantwoordelijkheid informeert u over hoe de Gemeente Loon op Zand omgaat met persoonsgegevens en het beleid dat hierop wordt gevoerd. Het geeft inzicht in de activiteiten die hieromtrent zijn genomen in de afgelopen periode, het aantal beveiligingsincidenten (datalekken), klachten en verzoeken en de ambitie voor 2021.

Inhoudsopgave

1. Inleiding

1.1 Doel Verklaring van Verantwoordelijkheid

In artikel 5 lid 2 AVG is een verantwoordingsplicht opgenomen dat de verantwoordelijke kan aantonen dat de beginselen inzake verwerking van persoonsgegevens worden gevolgd. Concreet betekent dit, dat het College B&W en directie/MT verantwoording aflegt over de realisatie van de doelstellingen en het gevoerde beleid ten aanzien van de belanghebbenden. De organisatie moet transparant zijn in haar handelen en de keuzes die worden gemaakt.

In de Verklaring van Verantwoordelijkheid (VvV) legt de gemeente Loon op Zand verantwoording af aan alle belanghebbenden over de naleving van verplichtingen vanuit wetgeving op het gebied van privacy en informatiebeveiliging. Met de VvV wordt aangegeven hoe de organisatie “in control” is en hoe de verplichtingen vanuit wetgeving worden nageleefd. Dit gebeurt op basis van al hetgeen is gedocumenteerd in de privacy & security administratie. Hiermee wordt een totaalbeeld van ‘accountability’ gegeven.

1.2 Gebruik

Privacy en informatiebeveiliging is een onderdeel van de verantwoordingscyclus van de gemeente Loon op Zand. In het onderstaand overzicht worden de stappen rondom privacy en verantwoording beschreven en welke rollen voor de verschillende personen zijn weggelegd.

De functionaris gegevensbescherming ziet toe op het privacy beleid van de gemeente Loon op Zand, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding en de betreffende audits.

De eigenaren en beheerders van applicaties zorgen voor een aantoonbare effectieve werking van beheer en beveiligingsmaatregelen met betrekking tot deze applicaties, het organiseren van deze maatregelen en de inrichting van de IT processen.

De Chief Information Security Officer (CISO) ziet toe op de maatregelen rondom informatiebeveiliging.

Uiteindelijk wordt een Verklaring van Verantwoordelijkheid (VvV) geschreven door de Functionaris Gegevensbescherming. Dit is een verantwoordingsverklaring en daarmee een aanvulling op de governance paragraaf in het jaarlijkse bestuursverslag. De VvV is bestemd voor stakeholders (belanghebbenden) zoals burgers, medewerkers, leveranciers en andere geïnteresseerden. De controle (op aspecten) van privacy en informatiebeveiliging is onderdeel van de controle op de jaarrekening door de accountant. De accountant kan de uitkomsten van de VvV meenemen in het vaststellen van zijn controleverklaring.

2. Mededeling Gemeentesecretaris

Privacy kan goed lastig zijn en in de weg zitten. Als je een pandemie onder controle wilt krijgen en de bewegingen van individuen wilt monitoren. Of een vaccinatiebewijs wilt inzetten als instrument om gecontroleerd weer ruimte te geven aan activiteiten. Of als je misbruik van een collectieve voorziening wil tegengaan door bestanden te koppelen. Of als je met het doel transparant te zijn besluiten van het college actief openbaar wilt maken met de onderliggende documenten en je dan eerst deze moet screenen op persoonsgegevens.
Privacybescherming is in het algemeen ook geen issue, waarvoor je gemeentesecretaris of beleidsmedewerker maatschappelijke zorg of vergunningverlener wilt worden. Je wilt dan in beeld komen met inhoudelijke voorstellen.
Maar…. Het besef is in een gering aantal jaren sterk gegroeid dat we privacybescherming juist wel hoog op onze aandachtspuntenlijst moeten zetten. Negatief benaderd, omdat je er ongelooflijk veel gedoe mee krijgt als je dit aspect niet op orde hebt en door een fout van de gemeente privacygegevens onvoldoende blijken te zijn beschermd. Maar vooral en op de eerste plaats omdat privacybescherming een essentieel rechtsstatelijk uitgangspunt is. Een zeer beschermingswaardige verworvenheid. Of, zoals Noam Chomsky het vanuit een ander perspectief zegt: “Het is gevaarlijk, wanneer mensen bereid zijn hun privacy op te geven.”. Wij krijgen als overheid heel veel gegevens van burgers en dat geeft ons de dure plicht om daar uiterst zorgvuldig, proportioneel en met grote aandacht voor bescherming van de privacy van deze burgers mee om te gaan. Daar kan de burger van Loon op Zand op rekenen.

Ad de Kroon maart 2021
Interim Gemeentesecretaris

3. Mededeling Functionaris Gegevensbescherming

Afgelopen jaar kenmerkte zich natuurlijk door het corona virus, ook op privacy gebied. We zijn met zijn allen thuis gaan werken waardoor de veilige omgeving waar we normaal onze werkzaamheden uitvoeren niet vanzelfsprekend meer is. Hierdoor zijn de risico's toegenomen, medewerkers vergaderen vanuit thuis met het risico dat huisgenoten kennis kunnen nemen van hetgeen besproken wordt. Microsoft Teams hebben we bewust gekozen als vergadertool omdat deze op dat moment het veiligste was. Verder hebben we maatregelen getroffen om het werken in de thuisomgeving zo veilig mogelijk te maken.

Als Functionaris Gegevensbescherming heb ik in 2020 veel vragen gekregen uit de organisatie omtrent privacy hetgeen betekent dat het onderwerp leeft. In het komend jaar zullen we deze bewustwording verder uit moeten breiden waarbij met name het melden van datalekken aandacht zal krijgen.

Doordat we als gemeente veel samenwerken met andere gemeentes hebben we vorig jaar de samenwerking met de FG's van omliggende gemeentes verder uitgebreid. Op regelmatige basis treffen de FG's van de verschillende gemeenten in de regio elkaar. Zo is er een regulier overleg met Heusden, Loon op Zand, Waalwijk en Baanbrekers. Is er een overleg 'AVG-coalitie' met de FG's van gemeenten en (zorg)partijen rond het Zorg- en Veiligheidshuis en andere samenstellingen. Hierdoor hebben we al een aantal regionale project van advies kunnen voorzien en stelt het ons in staat om gelijke tred te houden op privacy gebeid met collega gemeentes.

Richard van Ineveld — maart 2021
Functionaris Gegevensbescherming

4. Privacy en gegevensbescherming

3.1 Afhandeling datalekken

Eventuele datalekken zijn onderzocht door de Functionaris Gegevensbescherming. De gemeente Loon op Zand streeft een open cultuur na waarin datalekken laagdrempelig gemeld worden. Het onderzoek van de datalekken is er primair op gericht om ervan te leren.

Datalekken worden volgens een vastgestelde procedure afgehandeld. Wanneer iemand een mogelijk datalek vaststelt wordt hier direct melding van gemaakt bij de Functionaris Gegevensbescherming, de FG neemt de melding in behandeling en bepaalt of de melding binnen de reikwijdte van de meldplicht datalekken valt. Daarna zal de FG de impact van het datalek bepalen en wanneer deze beperkt is zal de FG het incident afhandelen. Als echter het datalek een grotere impact blijkt te hebben wordt er een crisisteam samengesteld om de afhandeling te verzorgen.

Bij de afhandeling worden de richtlijnen van de toezichthouder gevolgd en wanneer noodzakelijk wordt melding gedaan bij de Autoriteit Persoonsgegevens. Tevens kan het voorkomen dat de betrokken personen die “geraakt” zijn door het datalek worden geïnformeerd.

In 2020 zijn er in totaal 14 interne meldingen geweest en heeft de gemeente in vier gevallen het incident gemeld bij de Autoriteit Persoonsgegevens. In twee gevallen hebben we tevens de betrokkenen geïnformeerd.

Menselijke oorzaak		13
Technische oorzaak		1
Gemeld door leverancier		2
TOTAAL		14

3.2 Klachten en verzoeken

Met de komst van de Algemene Verordening Gegevensbescherming zijn de rechten van burgers en andere betrokkenen sterk uitgebreid. Iedereen heeft het recht op informatie en men kan een verzoek tot inzage doen. Als er persoonsgegevens van iemand worden verwerkt heeft deze het recht te weten welke gegevens dit zijn, waarvoor de gemeente deze gegevens precies gebruikt en met wie deze gegevens eventueel worden gedeeld. Bij het indienen van een inzageverzoek hoeft men geen reden op te geven. Verder moet het mogelijk zijn om een klacht in te dienen over de verwerking van (bepaalde) persoonsgegevens. Dit kan bij de gemeente maar men kan ook een klacht indienen bij de Autoriteit Persoonsgegevens.

Het is ons niet bekend of er bij de Autoriteit Persoonsgegevens klachten zijn ingediend over de gemeente Loon op Zand. In een dergelijk geval verloopt de communicatie tussen de AP en de gemeente via de Functionaris Gegevensbescherming.

Verzoeken in 2020

Informatieverzoeken		0
Inzageverzoeken		2
Verzoek tot rectificatie		0
Verzoek tot wissing		1
Bezwaar/beperking		0
Klacht		1
TOTAAL		4

3.3 Privacy tickets

Regelmatig zijn er in de organisatie vragen over privacy en wil men een advies over het omgaan met de AVG. Medewerkers van de gemeente Loon op Zand kunnen in een dergelijk geval een mail sturen aan de Functionaris Gegevensbescherming voor advies. Deze aanvragen worden vastgelegd in de privacy administratie. In 2020 heeft de Functionaris Gegevensbescherming in totaal 71 vragen gekregen. Deze vragen varieerden van het beoordelen van een verwerkersovereenkomst tot vragen of bepaalde gegevens uitgewisseld mochten worden.

3.4 DPIA

Vanuit de AVG is er de verplichting om voor verwerkingen die een verhoogd risico vormen voor de betrokkene of de organisatie een Data Protection Impact Assessment (DPIA) uit te voeren. Bij een DPIA worden de risico's in kaart gebracht en worden maatregelen gedefinieerd om deze risico's weg te nemen.

Voor het uitvoeren van dergelijke DPIA's maakt de gemeente gebruik van een standaard handreiking en bijbehorende vragenlijst. Het proces van het uitvoeren van een DPIA kent de volgende stappen:

Een DPIA kent een aantal belangrijke doelen. Het belangrijkste doel is:

1. Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste privacy risico's.

Daarnaast kunnen nog de volgende doelen worden onderscheiden:

2. Het verminderen van de gevolgen van toezicht en handhaving
3. Het verbeteren van de kwaliteit van gegevens.
4. Het verbeteren van de dienstverlening.
5. Het verbeteren van de besluitvorming.
6. Het verhogen van het privacy bewustzijn binnen de organisatie.
7. Het verbeteren van de haalbaarheid van het project.
8. Het verstevigen van het vertrouwen van de klanten, werknemers of burgers in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd.
9. Het verbeteren van de communicatie over privacy en de bescherming van persoonsgegevens.
10. Inzicht in, of ontdekken van, schaduw registraties waar mogelijk verplicht gebruik gemaakt van basisregistraties van toepassing hoort te zijn.

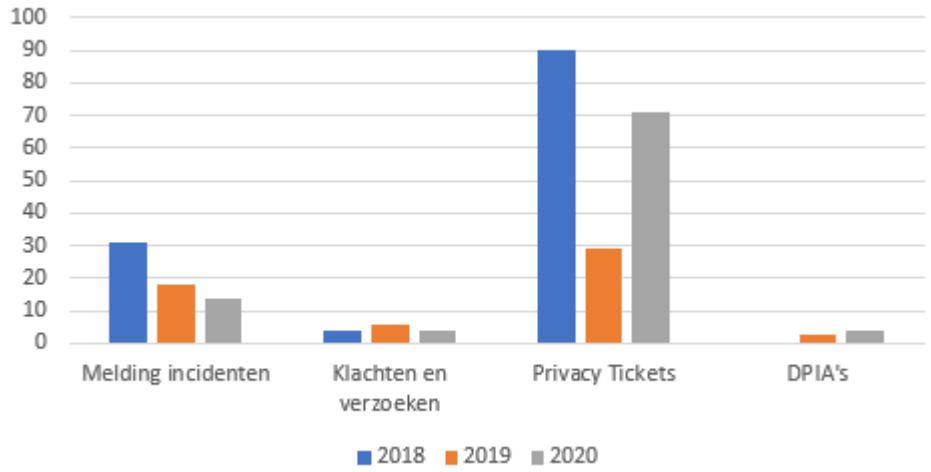
Uitgevoerde DPIA's 2020

In 2020 hebben we in de gemeente Loon op Zand de volgende DPIA's uitgevoerd:

- Postverwerking
- iBabs
- Xential
- Zaakgericht werken

3.5 Samenvattend beeld

Vergelijking 2018-2020



Conclusie

In de vergelijking is te zien dat privacy aandacht heeft van de organisatie. Dit concluderen we aan de hand van het aantal tickets dat in 2020 is behandeld. Echter zien we ook dat met name het aantal meldingen van incidenten achterblijft. Verzoeken van inwoners blijft stabiel en zijn er enkele per jaar. Het aantal DPIA's zal het komende jaar sterk gaan toenemen.

Aanbevelingen

Op basis van voorgaande worden de volgende aanbevelingen gedaan:

- Organiseer bewustwording ten aanzien van datalekken
- Betrek de FG tijdig (dus vooraf) bij alle aangelegenheden ten aanzien van persoonsgegevens
- Meld alle incidenten tijdig bij de FG/CISO
- Nodig de FG regelmatig uit voor advies en/of overleg
- Zorg ervoor dat de noodzakelijke documentatie omtrent verwerkingen up-to-date blijft
- Implementeer een plan voor de borging van de AVG

5. Ambitie voor 2021

Vanuit de cijfers en aanbevelingen kunnen we de volgende ambitie voor het komend jaar definiëren.

Het verbeteren van processen rondom het verwerken van persoonsgegevens blijft een continue proces. De medewerkers van de gemeente zijn cruciaal als het gaat om het beschermen van persoonsgegevens, bewustwording en bewustzijn is hierbij natuurlijk evident. In het komend jaar zal een van de speerpunten zijn om een plan te implementeren om het bewustzijn van de medewerkers continue te onderhouden en daar waar mogelijk te verbeteren.

Er zal een handboek datalekken worden ontwikkeld om meer duidelijkheid omtrent incidenten te verschaffen aan medewerkers waardoor datalekken beter kunnen worden afgehandeld.

Verder dienen we Privacy en Informatiebeveiliging verder in de organisatie te verankeren, hiervoor zal een plan worden gemaakt om de borging van de AVG middels een management cyclus naar een hoger volwassenheidsniveau te brengen.