GEMEENTE WESTLAND

GEMEENTEBLAD

Officiële uitgave van de gemeente Westland

Nr. 244778

23 juli

2021

Beleidsregel van het college van burgemeester en wethouders van de gemeente Westland houdende regels omtrent gegevensbescherming

1. Inleiding

De gemeente Westland en al haar medewerkers werken doorlopend met veel gevoelige gegevens. Welke dat zijn hangt veelal af van iemands rol en functie. Het kunnen politiek gevoelige gegevens zijn, financiële gegevens, vertrouwelijke documenten, grondexploitaties en bovenal persoonsgegevens. We zijn en voelen ons daarvoor verantwoordelijk en zijn daarop aanspreekbaar.

Om dit vorm en inhoud te geven is er voorheen beleid op- en vastgesteld. Zo zijn er, los van elkaar, een privacybeleid en een informatie¬beveiligingsbeleid. De basis van het meest recente privacybeleid is de Algemene Verordening Gegevensbescherming (AVG) en de basis voor het huidige informatiebeveiligings¬beleid de destijds geldende Baseline Informatiebeveiliging Gemeenten (BIG). Inmiddels is die baseline vervangen door de Baseline Informatiebeveiliging Overheid (BIO).

Hoewel nog niet overal gebruikelijk, vindt Westland het logisch informatiebeveiliging en privacy niet (meer) los van elkaar te bezien maar als een geïntegreerd geheel. Beide onderdelen gaan immers over zorgvuldig omgaan met gegevens, het op basis van risico¬analyse treffen van passende maatregelen en het voldoen aan kaders. Daardoor is het een logische stap over te gaan naar een Gegevensbeschermingsbeleid waarin vanuit de verschillende aspecten integraal wordt gekeken naar het datagebruik in de organisatie.

2. Van maatregelen naar doelen

De algemene definitie van beleid is: *"het geheel aan opvattingen over te realiseren doelstellingen, tezamen met de in de tijd uitgezette acties en de daarvoor benodigde middelen om deze doelstel-lingen te bereiken".*
De uitwerking van de nu voorliggende opzet richt zich vooral op het eerste deel, het geheel van opvattingen en de te realiseren doelen. Reden hiervoor is dat deze doelen doorlopend aandacht vragen en er waarschijnlijk nooit een moment is aan te wijzen waarin dat is of wordt bereikt. Er bestaat ook geen optimum, omdat op basis van onderkende risico's passende maatregelen worden genomen. In onze dynamische omgeving verandert dit doorlopend, evenzo dat de kaders aan veranderingen onderhevig zijn. Het sturend mechanisme is het principe van plan-do-check-act.

Het samenvoegen van privacy en informatiebeveiliging en dit vervolgens te benaderen als gegevensbescherming is logisch vanwege de raakvlakken en overlappingen die er zijn. Wanneer je het huidig vastgestelde beleid beschouwt, valt allereerst op dat het minder over te realiseren doelen gaat maar juist veel meer over te treffen maatregelen. Ook in het privacybeleid komt dit in zeker mate zo terug. Vervolgens bevatten beide documenten veelal herhalingen van wettelijke verplichtingen of zaken die in de kaders als richting staan aangegeven.

De nu voorliggende nieuwe opzet vormt in die zin een breuk met het verleden. Het accent in dit Gegevensbeschermingsbeleid ligt op wat de organisatie wil bereiken en hoe we daar gaan komen. Dit betekent niet dat we door dit nieuwe beleid heel anders gaan werken. Dit nieuwe beleid legt wel nadrukkelijker vast hoe we de doelen willen halen. Dit komt ook tot uitdrukking in de subtitel: 'Doorlopend: doordacht en doordrongen'. Deze uitgangspunten hebben in dit nieuwe beleid een prominente rol gekregen. De maatregelen die we moeten treffen veranderen niet, we zetten ze alleen voortdurend doordachter in met in ons achterhoofd de te behalen doelen. En het beleid is daar waar nodig aangepast aan actualiteiten en landelijke wijzigingen in bijvoorbeeld wet- en regelgeving.

3. Opzet Gegevensbeschermingsbeleid

Het als organisatie werken volgens een vastgesteld beleid is vooral dan kansrijk als het voldoet aan een aantal vereisten. Deze uitwerking steunt daarbij op de volgende gedachten:

1. Zo min mogelijk regels zodat de bomen in het bos nog worden gezien.
2. Helder wat we willen bereiken
3. Helder hoe we dit willen bereiken
4. Duidelijk wat we van iedereen verwachten

Daar waar in dit beleid "we" staat geschreven, betreft dit de organisatie in brede zin en al haar medewerkers.

4. Relevante wet- en regelgeving

De basis voor dit Gegevensbeschermingsbeleid wordt vooral gevormd door twee belangrijke zaken. De eerste is een wettelijke, de Algemene Verordening Gegevensbescherming (AVG) die sinds 25 mei 2018 van kracht is. De tweede is de Baseline Informatiebeveiliging Overheid (BIO) die sinds 1 januari 2019 van kracht is. Om de lezer een beeld te geven van hoe beide zaken in het dagelijkse werk tot hun recht komen, hierbij een korte samenvatting.

Algemene Verordening Gegevensbescherming

De AVG regelt dat organisaties duidelijk maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data wordt bewaard. Zo moet worden bepaald voor welk doel data wordt gebruikt, op basis van welke grondslag dat plaatsvindt en er wordt niet meer verzameld dan nodig voor het doel. Verder is van belang waar de data wordt opgeslagen en of het met anderen wordt gedeeld. Tot slot regelt de AVG dat onze burgers en klanten rechten hebben om inzage te krijgen in de opgeslagen data, het wijzigen en soms zelfs het verwijderen daarvan. In nagenoeg alle processen die wij als gemeente Westland kennen worden persoonsgegevens gebruikt, dus bijna iedereen heeft hier dagelijks mee te maken.

De Baseline Informatiebeveiliging Overheid (BIO)

De BIO stelt kaders en normen voor de informatieveiligheid. De BIO bevat te nemen maatregelen waarin men keuzes heeft in hoeverre die worden toegepast of niet. In alle gevallen geldt dat er risico's zijn en jij deze in het werk herkent. Daarnaast zijn er verplichte overheidsmaatregelen waarin er feitelijk geen keuze is. Het niet toepassen van zo'n maatregel vraagt een expliciet besluit met toelichting (pas toe of leg uit). Tot slot bevat de BIO meerdere controls aan de hand waarvan kan worden beoordeeld of er juist omgegaan wordt met de risico's en maatregelen.

De BIO bevat meerdere hoofdstukken, een deel daarvan richt zich vooral op technische zaken en een deel op algemene zaken en gedrag. De technische zaken zijn vooral een aandachtpunt voor het taakveld I&A en in mindere mate voor een bepaald proces of toepassing. De andere maatregelen hebben vooral betrekking op alle processen en dagelijkse werkzaamheden. Daarnaast is er een deel dat gaat over de opzet, inrichting en borging van de informatiebeveiliging.

5. Wat is Gegevensbescherming

De gemeente Westland is een informatie-intensieve organisatie met een sterke focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente moeten beschikken over betrouwbare informatie om de klanten optimaal te helpen en te adviseren. Daarnaast moeten burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Om dit meer vorm en inhoud te geven hanteren we in en met ingang van dit beleid onderstaande definities. *(Anders beschreven dan in de kaders maar passend daarbinnen en in begrijpbaardere taal.)*

- Definitie Gegevensbescherming: Bewust en doelgericht ons denken, doen en laten richten op het zorgvuldig bewerken en verwerken van (vertrouwelijke) informatie binnen de geldende wetten, regels en normen.
- Definitie van privacy [1] : Centraal stellen van de belangen van betrokkenen bij het bewerken, verwerken en delen van (bijzondere) persoonsgegevens.
- Definitie van informatiebeveiliging [2] : Het risicobewust treffen, onderhouden en controleren van samenhangende maatregelen met betrekking tot informatieverwerking en informatiesystemen zodat het juiste niveau van beschikbaarheid, integriteit en vertrouwelijkheid is en blijft gewaarborgd.

Medio 2020 heeft door het Coronavirus noodgedwongen het thuiswerken een explosieve groei laten zien. Waar thuiswerken eerst een uitzondering was werd het nu vooral een regel. Dit vraagt van zowel de organisatie als van de medewerkers extra inspanningen om op het gebied van gegevensbescherming de juiste stappen te zetten. Hierbij is het goed ons te realiseren dat het bereiken van onze doelen van gegevensbescherming en het voldoen aan de kaders en richtlijnen veel meer een zaak van bewustwording en bewustzijn is dan het treffen van technische maatregelen. Wat dat laatste betreft, de ICT-basis volstaat zondermeer en daar worden doorlopend verbeteringen doorgevoerd in bestaande voorzieningen en het toevoegen van nieuwe producten. Dit beleid heeft vooral tot doel de bewustwording en het bewustzijn van de organisatie als geheel te versterken.

1) Zie ook https://www.noraonline.nl/wiki/Privacy
2) Zie ook https://www.noraonline.nl/wiki/Informatiebeveiliging

6. Wat willen we bereiken

Het doel wat we met elkaar willen bereiken is dat gegevensbescherming geborgd is, wordt en blijft binnen de organisatie en al haar producten en diensten. Basis daarin is ons besef dat we een verantwoordelijkheid hebben naar onze burgers, onze klanten en onszelf met betrekking tot de gegevensbescherming. Beginsel is dat we ons bewust zijn dat we omgaan met vertrouwelijke data en gevoelige informatie en dat we daarom beschermende maatregelen moeten nemen. Dit om enerzijds de privacy van mensen te bescherming en anderzijds de vertrouwelijkheid, beschikbaarheid en integriteit van de gegevens te garanderen.

Concreet vertaalt zich dit in de navolgende strategische doelen van Gegevensbescherming:

- Het managen van de gegevensbescherming.
- Het beschermen van de privacy rechten van burgers en klanten.
- Het adequate beschermen van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang tot systemen en/of informatie.
- Het garanderen van correcte, tijdige en veilige informatievoorzieningen.
- Het waarborgen van veilige informatiesystemen, processen en verwerkingen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Burgers en klanten actief informeren wat er met hun persoonsgegevens gebeurt.
- Het waarborgen van de naleving van dit beleid.

7. Hoe willen we dat bereiken

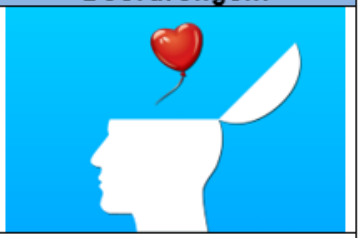
Op basis van bovenstaand uitgangspunt maken we, als het goed is, met elkaar vanzelf de juiste keuzes of zijn we minimaal met elkaar daarover in gesprek. De keuzes maken we daarbij veelal intuïtief omdat we in de basis met elkaar snappen en begrijpen wat rondom gegevensbescherming wel en niet kan. In beginsel werken we daarbij dus niet primair vanuit de kaders en wetten. In het slechtste geval zijn die hooguit uitvoeringsbeperkend voor hoe we de gegevensbescherming willen of kunnen inrichten. Of, zoals iemand het verwoorde: "Een auto rijdt 98% van zijn tijd rechtuit, maar het zou naïef zijn er geen stuur in te plaatsen".

Om bovenstaande meer fundament te geven werken we volgens de slogan:

"Doorlopend: doordacht en doordrongen datagebruik".

8. Doorlopend: doordacht en doordrongen

Om betekenis te geven aan de slogan "Doorlopend: doordacht en doordrongen datagebruik" onderstaand een nadere uitwerking van welke houding en welk gedrag dit van ons vraagt om hieraan te voldoen. Daarbij gaat het ook om de kennis en inzichten die nodig zijn om gegevensbescherming te borgen binnen de organisatie. En minstens zo belangrijk; de intentie waarmee we kijken naar de wijze waarop we de gegevensbescherming kunnen en willen toepassen.

Doorlopend:	Doordacht:	Doordrongen:
		
- Voor, tijdens en achteraf bij het verwerken - Binnen, buiten en thuis - Bewust handelen	- Weloverwogen - In juiste verhouding - Binnen de kaders	- Tot diep in onze wortels - In het hoofd en met het hart - Niet als principe maar als drijfveer

Deze slogan is toepasbaar op bijna alle dagelijkse zaken. Of het nu gaat om de werking van een proces, de aanschaf van een nieuwe toepassing, het testen van een applicatie of het buiten het gebouw werken. Gegevensbescherming is niet iets zoals het ophangen van brandblussers, nee gegevensbescherming moet werken als een rookmelder. Doorlopend actief en paraat om als er iets smeult tijdig aan te slaan.

Het toepassen van de slogan "Doorlopend: doordacht en drongen datagebruik" wint aan waarde door dit te vertalen in voorbeelden waar we geregeld mee in aanraking komen. In de bijlagen is daar een uitwerking over opgenomen.

9. Wat we verwachten

Er is meer nodig dan alleen een slogan om als organisatie voortgang te boeken met de verdere borging van de gegevensbescherming. Aan de wil ontbreekt het in de meeste gevallen niet. Frictie zit er hooguit in de ambities die we als organisatie en politiek hebben om voldoende prioriteit aan gegevensbescherming te kunnen geven. Taakveld Gegevensbescherming neemt vanuit haar rol, in geval er grote risico's blijven bestaan, zonodig haar verantwoordelijkheid door die risico's onder de aandacht te brengen van management en/of bestuur.

De basis voor wat van medewerkers en management wordt verwacht ligt, voor wat betreft het realiseren van de doelen van de gegevensbescherming, opgesloten in het principe van de lerende organisatie. De hoekstenen om dit inhoud geven zijn:

- *De organisatie leert van incidenten en datalekken*
- *Melden van kwetsbaarheden en incidenten wordt beloond*
- *Gegevensbescherming wordt regelmatig in werkoverleggen besproken*
- *We vragen advies en nemen hierin onze verantwoordelijkheid*
- *We willen leren en reserveren daar tijd voor.*

Het taakveld Gegevensbescherming adviseert daarnaast ongevraagd op basis van haar eigen bevindingen. Het taakveld speelt in op actuele ontwikkelingen, verzorgt regelmatig berichten over gegevensbescherming op het intranet en draagt als ambassadeur het nut en de noodzaak van gegevensbescherming uit.

10. Borging compliant werken

Een vraag die kan opkomen is: Hoe borgen we het voldoen aan de wettelijke eisen, kaders en normen wanneer we de gegevensbescherming intuïtief inrichten?

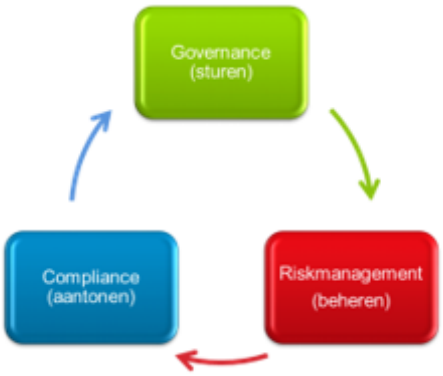
Wanneer een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving wordt dit aangeduid met de term compliance. Het volledig kennis hebben van de geldende wet- en regelgeving lijkt in die zin haaks te staan op intuïtief inrichten van de gegevensbescherming. Het is echter niet reëel van het lijnmanagement en de medewerkers te verwachten dat zij alle kennis in huis hebben. Wat wel verwacht mag worden is dat er een minimaal basisniveau aanwezig is en wordt toegepast bij het lijnmanagement en de medewerkers. Als handreiking en gedachtensteun is er een drietal factsheets met de basisinformatie als bijlagen bijgevoegd. De inhoud daarvan wordt bijvoorbeeld ook gebruikt om nieuwe medewerkers te infomeren over Gegevensbescherming.

Het taakveld Gegevensbescherming bezit in ieder geval de noodzakelijke specifieke kennis van de gegevensbescherming. Via de weg van gevraagde en ongevraagde adviezen wordt deze kennis aan de organisatie ter beschikking gesteld. De borging van compliant werken vindt daarbij ook plaats middels de producten die het taakveld Gegevensbescherming aanbiedt. Een deel daarvan is verplicht bij nieuwe of gewijzigde processen en bij aanschaf of inzet van toepassingen. In een producten- en diensten catalogus (PDC) voor het deel van Taakveld Gegevensbescherming is het aanbod nader uitgewerkt (zie bijlage).

11. Borging accountability

Het intern organiseren dat we in voldoende mate voldoen aan de wetten en kaders is niet voldoende. Niet voor ons zelf maar ook niet voor het bestuur, de politiek en partijen buiten. Verder hebben we sowieso te maken met het verplicht afleggen van verantwoording, bijvoorbeeld in geval van ENSIA[3]. Dit proces wordt accountability genoemd. Het steunt op een drietal onderdelen zoals in de foto hiernaast aangegeven.

3) ENSIA= Eenduidige Normatiek Single Information Audit. Betreft het verantwoordingsproces over informatieveiligheid bij gemeenten door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.



Basis vormt het risico gericht benaderen van processen, toepassingen en situaties. Het risico gericht werken kwam hiervoor al ter sprake en het belang is duidelijk. Om verantwoording af te kunnen leggen is het belangrijk om risico's die worden onderkend goed vast te leggen en aan een lijnverantwoordelijke te koppelen. Daarbij te beschrijven met welke maatregelen de risico's kunnen of zullen worden weggenomen, verminderd of afgewenteld. Tot nu toe ontbreekt dit vastleggen nog vaak en hebben verantwoordelijken onvoldoende inzicht welke zaken nog dienen te worden opgepakt. Daarvoor zijn er tools, deels op basis van instrumenten vanuit het VNG/IBD aangeboden, die de organisatie daarbij helpt. (Zie het productenboek Gegevensbescherming).

Vanuit het belang van accountability heeft het taakveld Gegevensbescherming ook een rol. Dit komt terug in de driejaarlijkse GAP-analyse[4]. Die wordt gemaakt op zowel het gebied van informatiebeveiliging als rondom de privacy. Verder houdt het taakveld de normenkaders actueel, is er coördinatie op het traject ENSIA en voert het taakveld zelfstandig onderzoeken en audits uit. Doel van dit alles is om, zoals de kaders stellen, "Aantoonbaar in control" te zijn.

12. Verantwoordelijkheden en rollen

De basis van de verantwoordelijkheden ligt opgesloten in het model van de Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, FG, Privacy officer en security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. Deze werkwijze is volledig in lijn met de BIO en de AVG. Die stellen namelijk dat de primaire verantwoordelijkheid om binnen de wettelijke en verplichte kaders de gegevensbescherming in te richten bij het lijnmanagement ligt. Vanuit die verantwoordelijkheid ligt daar het initiatief voor het borgen van gegevensbescherming binnen zijn of haar team. De lijnmanager wordt daarin ondersteund en geholpen door tools die Taakveld Gegevensbescherming maakt om dit verantwoord mogelijk te maken. Daarnaast is het taakveld gegevensbescherming beschikbaar voor advies en ondersteunen zij bij het toepassen van deze tools en implementatie van maatregelen.

In de bijlage is er een uitwerking van de rollen en verantwoordelijkheden van alle direct en indirect betrokkenen. Ten opzichte van het huidige beleid wijzigt deze overigens niet.

Vanwege de meervoudige rol die Taakveld Gegevensbescherming heeft, nog kort een toelichting. Enerzijds is er een adviserende rol met betrekking tot gegevensbescherming en maatregelen die genomen kunnen worden. Anderzijds bewaakt Taakveld Gegevensbescherming de kwaliteit van de gegevensbescherming op hoofdlijnen en houdt zij vinger aan de pols of we voldoende compliant zijn. Daarbij heeft de Functionaris Gegevensbescherming (FG) een wettelijke taak als toezichthouder wat betreft privacy en de AVG. De Chief Information Security Officer (CISO) is een verplichte overheidsmaatregel vanuit de BIO om vanuit een onafhankelijke positie als interne toezichthouder de kwaliteit van de informatiebeveiliging te bewaken.

Jaarlijks maakt Taakveld Gegevensbescherming een plan waarin accenten voor het dan komende jaar worden benoemd. Dit jaarplan wordt door het DT vastgesteld. Belangrijke input voor het jaarplan zijn daarbij: het dreigingsbeeld dat de IBD jaarlijks uitbrengt; uitkomsten ENSIA; wettelijke veranderingen; ontwikkelingen op het gebied van gegevensbescherming; GAP-analyse IB en privacy; signalen vanuit de organisatie en tot slot de analyses en bevindingen vanuit incidenten.

4) GAP-analyse is het weergeven van het verschil tussen de huidige en de gewenste situatie.

13. Samenwerking met ketenpartners

Als overheid wisselen we steeds vaker en steeds meer digitale gegevens uit met ketenpartners of met samenwerkingsverbanden. Er bestaan en ontstaan steeds meer vormen en redenen waarbij met andere partijen informatie wordt gedeeld. Ketenpartners krijgen toegang tot een deel van onze eigen informatie en gemeente Westland krijgt toegang tot informatie van andere partijen. Op technisch vlak geldt daarbij dat wij als gemeente vertrouwen moeten (kunnen) hebben op de ICT-voorzieningen van derden voor opslag van informatie of voor de uitvoering van bedrijfsprocessen.

Het is daarom noodzakelijk dat de gegevensbeschermings-risico's die samenhangen met ketens worden geïdentificeerd, dat noodzakelijke maatregelen worden toepast en wordt vastgesteld wie de verwerkingsverantwoordelijke is. Uiteraard gebeurt dit voordat er toegang wordt verleend aan een ketenpartner of voordat er wordt aangesloten op een voorziening van een ketenpartner. Dit betekent dat risico's en noodzakelijke maatregelen aantoonbaar mee worden gewogen in keuzes van samenwerking en bij het aangaan van contracten. Vastgesteld wordt daarnaast wie toegang heeft tot welke gegevens om het doel van de samenwerking te realiseren. In geval van verwerking van persoonsgegevens wordt er de landelijke door VNG vastgesteld verwerkersovereenkomst afgesloten. Afspraken over Gegevensbescherming worden in een overeenkomst vastgelegd. Daarnaast stelt de lijnverantwoordelijke bij voorkeur minimaal jaarlijks vast of aan de voorwaarden van gegevensbescherming wordt voldaan.

14. Tot slot

Met het hiervoor beschreven Gegevensbeschermingsbeleid zetten we een belangrijke stap de toekomst in. Het doet recht aan de integrale verantwoordelijkheid van de lijnmanagers, biedt voorwaarden voor het bestuur om hun verantwoordelijkheid te kunnen dragen en biedt de raad een basis om haar toezichthoudende taak uit te kunnen voeren. Daarnaast zet het de medewerkers van het taakveld Gegevensbescherming in een goede positie als ondersteuner en adviseur van management en medewerkers.

De opzet van dit beleid is, anders dan voorheen, gericht op wat we willen bereiken: een goede borging van de gegevensbescherming in de producten en diensten. Het geeft handen en voeten aan hoe we dat willen bereiken en volgens welke meetlat "Doorlopend: doordacht en doordrongen datagebruik". Belangrijk daarbij is vast te stellen dat we als organisatie moeten blijven voldoen aan de kaders die gelden. Dit beleid kan dan ook niet los worden gezien van de AVG, de BIO, de bestuurlijke aanvulling op de BIO vanuit de VNG met de 10 bestuurlijke principes, de ISO 27001/27002 en de standaarden waar we aan moeten voldoen.

Met het vaststellen van dit beleid komen de volgende beleidsdocumenten te vervallen:
- Privacybeleid gemeente Westland (Corsa 18-0108256)
- Kadernota privacybeleid (Corsa 18-0077745)
  Gemeentebreed Informatiebeveiligingsbeleid 2018-2021 (Corsa 18-0251091)

Het "oude" beleid bevat op onderdelen uitwerkingen van maatregelen. Omdat dit niet wordt opgenomen in dit nieuwe beleid ontstaat er met het vervallen van bovenstaande beleidsdocumenten er formeel een vacuüm op die onderdelen. (Bijvoorbeeld de wijze waarop de dataclassificatie plaatsvindt.) In 2021 stelt het taakveld Gegevensbescherming voor die onderdelen een procedure beschrijving op en voegt die toe aan de kennisbank op intranet. Tot die tijd werken we nog op basis van de werkwijze zoals die in het oude beleid zijn beschreven. Het is overigens niet reel te verwachten dat deze werkwijze tot een probleem zou kunnen of gaat leiden.

Bijlage
- Normenkader Gegevensbescherming
- Voorbeelden “Doorlopend: doordacht en doordrongen datagebruik”
- Uitwerking verantwoordelijkheden en rollen betrokkenen
- Factsheet Gegevensbescherming
- Factsheet Privacy/AVG
- Factsheet Informatiebeveiliging
- Productenboek Gegevensbescherming

Normenkader Gegevensbescherming

Een beleid gericht op de doelen die we willen bereiken blijft afhankelijk van de kaders die er gelden en vingerend zijn. Onderstaand een weergave daarvan. Jaarlijks wordt het normenkader door de audit coördinator gegevensbescherming geactualiseerd. Deze opsomming gaat uit van het kader dat geldt na vaststelling van het nu voorliggende Gegevensbeschermingsbeleid 2021-2023.

Omschrijving	Doel	Bas	Datum vastgesteld
Normen, standaarden, wet- en regelgeving, etc. Gegevensbescherming			
BIO versie 1.04	Kaderstelling	IB	1-1-2020
Algemene Verordening Gegevensbescherming (AVG)	Wetgeving	Privacy	25-5-2018
Uitvoeringswet AVG (UAVG)	Wetgeving	Privacy	25-5-2018
Criteria Borging AVG	Kaderstelling	Privacy	nvt
Forum standaardisatie	Kaderstelling	IB	nvt
GIBIT	Kaderstelling	IB	nvt
Verantwoordingsrichtlijn GeVS (Suwinet)	Kaderstelling	IB	nvt
Normenkader DigiD audit versie 2.0	Kaderstelling	IB	26-5-2020
Wet basisregistratie personen (BRP)	Wetgeving	IB	nvt
Paspoortuitvoeringsregeling nederland (PUN)	Wetgeving	IB	nvt
Wet basisregistraties adressen en gebouwen (BAG)	Wetgeving	IB	nvt
Kwaliteit en toezichtkader BAG 2019 versie 1.0	Kaderstelling	IB	1-7-2019
Wet basisregistratie grootschalige topografie (BGT)	Wetgeving	IB	nvt
Wet basisregistratie ondergrond (BRO)	Wetgeving	IB	nvt
Normenkader veilige email (NTA7516)	Kaderstelling	Privacy	mei-19
Beleid, procedures, templates etc. Westland specifiek Gegevensbescherming			
Informatiebeveiligingsbeleid	Kaderstelling	IB	11-12-2018
Beheer van Bedrijfsmiddelen versie 12-10-18 14-09 DEF 7	Procedure	IB	
Personele beveiliging versie 12-10-18 14-10 DEF 8	Procedure	IB	
Fysieke beveiliging en beveiliging van de omgeving versie 12-10-18 14-10 DEF 9	Procedure	IB	
Beheer van communicatie en bedieningsprocessen versie 12-10-18 14-11 DEF 10	Procedure	IB	
Toegangsbeveiliging 12-10-18 14-11 DEF 11	Procedure	IB	
Verwerving ontwikkeling en onderhoud van informatiesystemen 12-10-18 14-12 DEF 12	Procedure	IB	
Beheer van informatiebeveiligingsincidenten 12-10-18 14-12 DEF 13	Procedure	IB	
Bedrijfscontinuiteitsbeheer 12-10-18 14-13 DEF 14	Procedure	IB	
Naleving 12-10-18 14-13 DEF 15	Procedure	IB	
Cloudbeleid versie 1.3	Kaderstelling	IB	18-12-2019
ICT aansluitvoorwaarden versie 4.7	Kaderstelling	IB	20-9-2019
Beveiligingsplan Suwinet incl. privacyreglement versie 4.0	Kaderstelling	IB	11-12-2018
Kadernota Uitgangspunten Privacybeleid	Kaderstelling	Privacy	12-6-2018
Privacybeleid	Kaderstelling	Privacy	24-4-2018
Privacyverklaring	Externe verantwoording	AVG	mei-18
Privacyreglement en gedragslijnen	Kaderstelling	Privacy	7-8-2018
Privacyreglement BRP	Kaderstelling	Privacy	16-6-2014
Aanwijzingsbesluit FG	Externe verantwoording	AVG	29-10-2019
Regeling FG	Kaderstelling	AVG	7-8-2018
Verwerkingsregister - openbaar	Externe verantwoording	AVG	mei-18
Verwerkingsregister - intern	Werkdocument	AVG	nvt
Standaard verwerkersovereenkomst 2.2	Organisatie	Privacy	9-4-2020
Uitvoeringsaanpassing PIA - PIA-tool IBD	Organisatie	Privacy	25-4-2019
Uitvoeringsprotocol datalekken versie 1.1	Protocol	Privacy	6-6-2018
Uitvoeringsprocedure Rechten van betrokkenen versie 1.4	Procedure	Privacy	24-5-2019

Zie voor nadere informatie Corsa 18-0222648.

Voorbeelden Doorlopend: doordacht en doordrongen datagebruik

Doorlopend:
- Bij het inrichten van een nieuw proces
- Bij veranderingen in een proces
- In het dagelijks handelen
- In het verantwoorden hoe je met gegevensbescherming omgaat.

Doordacht en doordrongen:
- Bij datagebruik
  - Waarom heb je iets nodig (**AVG: doelbinding en rechtmatigheid**)
  - Wat heb je nodig (**AVG: dataminimalisatie**)

- Bij dataverwerking
  - Binnen welke context (**binnen of buiten; kunnen meekijken op scherm**)
  - Met wie deel je informatie en wat betreft het (**alleen binnen netwerk; geen usb**)
  -

- Bij processen
  - Niet meer dan nodig (**need to know versus nice to know**)
  - Zijn het persoonsgegevens (**betreft het bijzondere persoonsgegevens?**)
  - Wat doen we er mee (**met wie delen we het wel of juist niet**)
  - Hoe lang bewaren (**niet onnodig lang bewaren maar ook niet voortijdig vernietigen**)
  - Wie heeft er toegang toe en wanneer (**toegang tot gebouwen, systemen en data**)

- Bij toepassingen
  - Waar slaan we data op (**alleen vanuit gemeente gefaciliteerd**)
  - Wie kunnen er bij (**rechten en rollen**)
  -

- Bij apparaten
  - Hoe beveilig je een toestel (**2-factor**)
  - Voldoet het aan de normen (**virusscanner; vertrouwd Wifi-netwerk**)
  -

- Bij de infrastructuur
  - Past het in de gewenste structuur (**architectuur**)
  - Is de beveiliging op orde (**laatste patches en updates**)
  - Zijn er koppelingen met andere netwerken (**juiste certificaten en technisch veilig**)

Verantwoordelijkheden en rollen betrokkenen

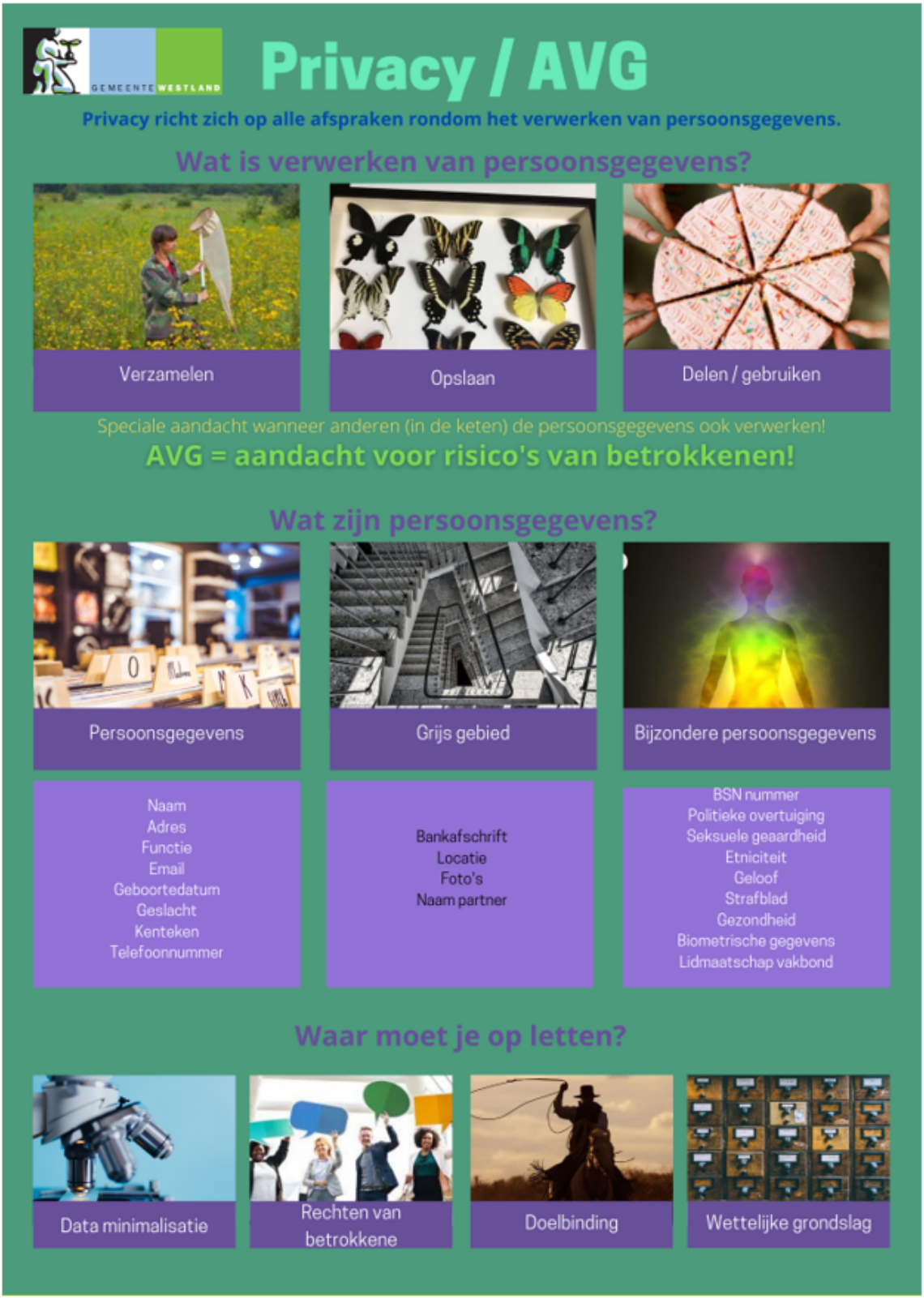
Cluster-directeur	• Voert regie en houdt toezicht op zijn processen inzake Gegevenbescherming • Aantoonbaar compliant aan wetten en kaders • Dataclassificatie van systemen • Risicoafweging en treffen maatregelen • Medewerkers meenemen in hun verantwoordelijkheid
Teammanager / proces eigenaren / procesverantwoordelijke	• Operationele verantwoordelijkheid voor systemen en processen • Voert regie en houdt toezicht op zijn processen inzake gegevensbescherming • Stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesysteem vast. • Het treffen van maatregelen op basis van risicomanagement • Zorgen voor Bewustwording onder personeel • Beheersen van en rapporteren over incidenten
Procesverantwoordelijke / proces eigenaren	• Verantwoordelijke voor implementatie juiste beveiligingsniveau • Opstellen plan van aanpak • Rapporteert aan CISO over beveiligingsincidenten • Regelen van toegang tot gegevens nodig voor hun taak voor medewerkers
Medewerkers	• Verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen • Werken volgens en binnen richtlijnen, kaders en gedragsregels

Functionaris Gegevens-bescherming	• Intern toezichthouder verwerking persoonsgegevens • Verantwoordelijk voor het toezicht op de naleving van de privacywetten en –regels • Adviseren over allerlei privacy gerelateerde zaken • Verantwoordelijk voor het afhandelen van vragen en klachten
CISO / security manager (strategisch)	• Verantwoordelijk voor het implementeren van, adviseren over en toezicht houden op het informatiebeveiligingsbeleid • Coördineert formuleren IB beleid • Risicoanalyse en GAP-analyse en coördinatie prioritering maatregelen • Bevorderen bewustzijn • Contactpersoon IBD/CERT
ISO / security officer (tactisch / operationeel)	• Adviseren bij projecten • Managen van risico's • Opstellen informatiebeveiligingsplan met betrekking tot het cluster • Controle op uitvoering beveiligingsplan
Privacy officer	• Verantwoordelijk voor het vormgeven en bewaken van het privacybeleid. • Adviserende rol voor de clusters • Ondersteunen bij melden van datalekken

Raad	• Controle en toetsing op werking beleid
College	• Eindverantwoordelijke • Politiek verantwoordelijk voor een passend niveau gegevensbescherming
Gemeente-secretaris	• Gemandateerde door college voor bevoegdheden op gebied Gegevenbescherming • Verantwoordelijk voor uitvoering van organisatiebrede vraagstukken te aanzien van gegevensbescherming • Verantwoordelijk voor de inrichting en werking van beveiligingsorganisatie
DT	• Vaststellen gewenste niveau van gegevensbescherming

Factsheet Gegevensbescherming

Factsheet privacy/AVG



Factsheet Informatiebeveiliging

Productenboek Gegevensbescherming

Zie Corsa 20-0221989

GEMEENTE WESTLAND

Auteur(s)	M.G. Vieselman, R.P.J. Ritsema, M.T. van Rijn
Datum	augustus 2020
Versie	1.0
Status	Definitief

ALG HS 0017

20-0221989

Pagina 1 van 21