GEMEENTE Berg en Dal

GEMEENTEBLAD

Officiële uitgave van de gemeente Berg en Dal

Nr. 498348

27 november 2024

Strategisch Gemeentelijk Informatiebeveiligings- en privacybeleid (IB&P-beleid) 2024-2027

1. Managementsamenvatting

Inleiding
Wij beschikken over veel (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens zijn nodig om onze wettelijke taken goed uit te kunnen voeren.

De gegevens zijn vaak gevoelig. Komen ze in verkeerde handen? Dan kan dat ernstige schade opleveren voor inwoners. Zijn de gegevens niet beschikbaar of kloppen ze niet? Dan kunnen we onze werkzaamheden niet uitvoeren of nemen we verkeerde beslissingen.

Gemeenten zijn steeds vaker het doelwit van hackers en andere criminelen. Gegevens over inwoners leveren veel geld op en kunnen misbruikt worden voor bijvoorbeeld identiteitsfraude.

Gegevens moeten we daarom goed beschermen. In dit strategisch informatiebeveiligings- en privacybeleid beschrijven we welke doelen we ons daarbij hebben gesteld en de manier waarop we dat gaan doen. Het gaat hierbij om de periode 2024 tot 2027 en vervangt het informatie- en privacybeleid over de periode 2019-2023.

Doel
Het is ons doel onze werkzaamheden uit te voeren op “volwassenheidsniveau 3”. Dat betekent dat we alle werkzaamheden uitvoeren volgens een vastgestelde werkwijze. In die werkwijze zijn dan de veiligheids- privacymaatregelen opgenomen, zodat de kans op incidenten beperkt is.

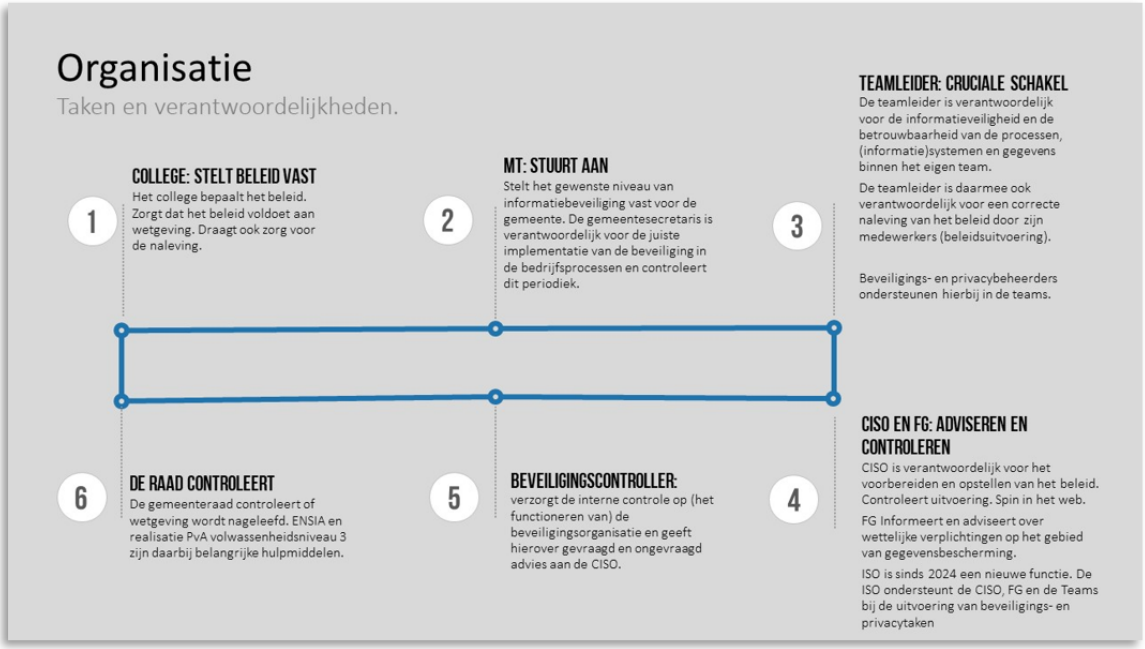
Hiermee borgen we dat:
- Informatie beschikbaar is voor ons werk,
- De informatie actueel en volledig is,
- De informatie vertrouwelijk wordt behandeld en de privacy van inwoners (en eigen medewerkers) geborgd is.

Het nieuwe beleid wordt geconcretiseerd in een jaarlijks (uitvoerings)plan (Informatiebeveiligings- en privacyplan 2024).

Ontwikkelingen
- In het nieuwe beleid zijn de aanbevelingen verwerkt van de regionale rekenkamer. In 2022 heeft de rekenkamer de resultaten gepresenteerd van een onderzoek naar de mate van volwassenheid van onze informatiebeveiliging en privacy.
- Op basis van dat onderzoek heeft de raad het college verzocht een plan van aanpak op te stellen om volwassenheidsniveau 3 te bereiken. Dat plan van aanpak is in september 2023 door de raad vastgesteld. Het plan van aanpak is verwerkt in het nieuwe strategische beleid en het bijbehorende informatiebeveiligings- en privacyplan.
- Naar verwachting treedt eind 2024 nieuwe wetgeving (NIS2/NIB2) in werking die gemeenten verplicht de informatiebeveiliging op orde te hebben. Het houdt concreet in dat gemeenten wettelijk verplicht worden te voldoen aan de BIO. De BIO is een set aan maatregelen voor overheden om informatie goed te beveiligen. De ontwikkelingen rondom NIS2 zijn al in het nieuwe beleid verwerkt.
- We werken zoveel mogelijk volgens de standaards van de Informatiebeveiligingsdienst (IBD)[1].

Taken en verantwoordelijkheden

1) De IBD is onderdeel van de Vereniging van Nederlandse Gemeenten en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.



- **Het college van B en W** is eindverantwoordelijk voor informatiebeveiliging en privacy.
- **Het MT** stelt het beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
- **De teamleiders** zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging en privacybescherming. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Berg en Dal hebben een interne eigenaar die primair verantwoordelijk is voor de bescherming van de gegevens.
- **De Chief Information Security Officer** (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- **De Functionaris voor Gegevensbescherming** (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) voorschrijft.
- **De beveiligingscontroller** verzorgt de interne controle op (het functioneren van) de beveiligingsorganisatie en geeft hierover gevraagd en ongevraagd advies aan de CISO.
- **De gemeenteraad** controleert het college op de naleving van wet- en regelgeving op het gebied van informatiebeveiliging en privacy.

Uitgangspunten

- **We werken risico-gestuurd**: het borgen van veiligheid en privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van veiligheids- en privacyregels en op basis van een risico-inschatting.
- **'Plan, do, check en act'**: informatiebeveiliging en privacybescherming is een continu verbeterproces. Dat betekent dat we steeds beoordelen welke maatregelen nodig zijn, periodiek controleren of deze uitgevoerd worden en ook goed werken. Waar nodig passen we maatregelen of onze werkwijze aan.
- **Iedere medewerker**, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- **Training**: Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures, hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.

2. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2024 tot 2027. Het vervangt het in 2019 vastgestelde Informatiebeveiligingsbeleid 2020-2023 en Privacybeleid.

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau. Een van daarvan is het Beveiligingsplan Suwinet 2024-2027 dat tegelijkertijd met dit strategisch beleidsplan wordt aangeboden.

Met dit 'Strategisch Informatiebeveiligings- en privacybeleid 2024 tot 2027' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) (zie bijlage A) en het VNG Borgingsproduct Algemene Verordening Gegevensbescherming (AVG) versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens (zie bijlage B).

1.1. Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings- en privacy plan (vast te stellen door het managementteam (MT)) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van onder andere teamleiders, de chief information security officer (CISO), de functionaris gegevensbescherming (FG), het dreigingsbeeld Nederlandse gemeenten van de Informatiebeveiligingsdienst (IBD) en de uitkomsten van risicoanalyses (Risico-analyse Informatiebeveiliging en privacy 2023) en gegevensbeschermingsbeoordelingen (DPIA's). Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens op hoofdlijnen hoe de taken en verantwoordelijkheden in de organisatie belegd zijn. Een uitwerking daarvan is te vinden in het document "Informatiebeveiligingsorganisatie 2024-2027".

Samengevat is het nieuwe informatiebeveiligings- en privacybeleid uitgewerkt in de volgende documenten:

- Risico-analyse Informatiebeveiliging en privacy 2023;
- Strategisch Informatiebeveiliging- en privacybeleid 2024-2027;
- Informatiebeveiligingsorganisatie 2024-2027;
- Informatiebeveiligings- en privacyplan 2024;
- Beveilingsplan Suwinet 2024-2027.

1.2. Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie:

- **Beschikbaarheid (of continuïteit)**: het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- **Integriteit**: het waarborgen van de correctheid (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking oftewel het in overeenstemming zijn van informatie met de werkelijkheid;
- **Vertrouwelijkheid**: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3. Privacy & Gegevensbescherming (AVG/Wpg)

Privacy is de bescherming van de privésfeer. Dit is niet alleen het beschermen van persoonlijke gegevens. Maar ook het recht om met rust gelaten te worden. Het betekent dat de gemeente zich niet mengt in het persoonlijke leven van haar inwoners als dit niet nodig is. Dit willen we goed regelen in de gemeente Berg en Dal. Ook wanneer we taken uitvoeren samen met (maatschappelijke) partners in de regio. Zowel in onze digitale als niet-digitale dienstverlening. Privacy is bovendien een grondrecht en wordt beschermd door wetten en regelgeving in veel landen over de hele wereld. In de Europese Unie is de AVG een belangrijk juridisch kader voor gegevensbescherming en privacy.

Persoonsgegevens zijn alle gegevens die herleidbaar zijn naar een (natuurlijk) persoon. Bijvoorbeeld naam, adres, geboortedatum of BSN Dit kan van een inwoner zijn, maar ook iemand anders die contact heeft met de gemeente Berg en Dal. De persoon over wie de gegevens gaan, noemen we de betrokkene.

Het verwerken van persoonsgegevens is elke handeling met persoonsgegevens. Zoals verzamelen, bewaren, raadplegen, wijzigen, vernietigen of delen van persoonsgegevens. De gemeente Berg en Dal houdt een register bij van alle verwerkingen van persoonsgegevens.

Privacy is ook het recht en de mogelijkheid van inwoners om controle te hebben over zijn of haar persoonlijke informatie en gegevens, en om te kunnen zien welke informatie met anderen wordt gedeeld. Inwoners kunnen hiervoor gebruik maken van het Inzagerecht

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk. Daarbij verwerken we niet meer gegevens dan nodig is.

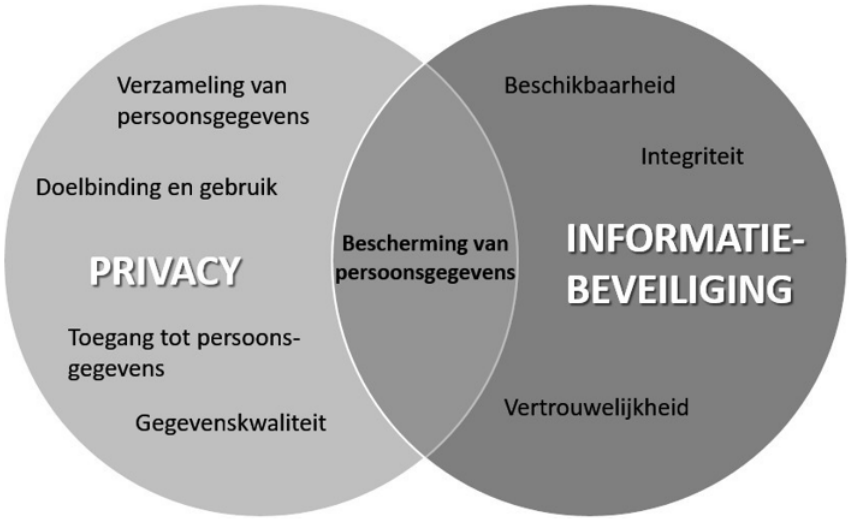
Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4. Relatie tussen privacy en informatiebeveiliging
Privacy en informatiebeveiliging hangen nauw met elkaar samen. Het zijn twee verschillende begrippen, maar wel met een gemeenschappelijk raakvlak. Privacy gaat over het vertrouwelijk omgaan met persoonlijke gegevens; een goede beveiliging maakt daarvan hoort daar bij. Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle (gevoelige) informatie.

Om onze dienstverlening vorm te kunnen geven, verwerkt de gemeente persoonsgegevens. Zoals bij de uitgifte van een paspoort, het bieden van een uitkering of de aanvraag van een vergunning. Inwoners moeten er dan op kunnen vertrouwen dat hun persoonsgegevens veilig zijn bij ons. Het privacybeleid ondersteunt dan ook op de uitgangspunten die verwoord zijn in het Informatiebeveiligingsbeleid.

Zowel informatiebeveiliging als privacy vragen om een risico-gedreven aanpak. Dit betekent dat we onderzoeken welke risico's er zijn als we werken met gegevens. Als het nodig is, neemt de gemeente maatregelen om deze risico's te weg te nemen of zoveel mogelijk te verkleinen.

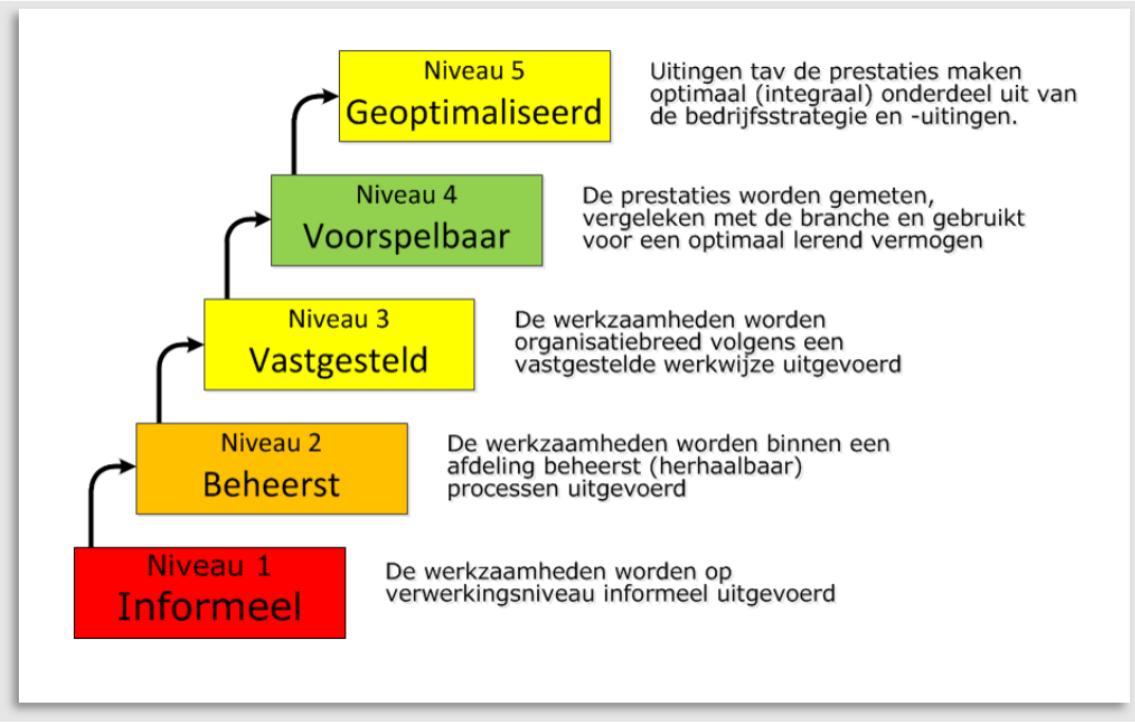
De afbeelding hieronder geeft de samenhang tussen informatiebeveiliging en privacy weer.



1.5. Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy

De gemeente Berg en Dal wil een betrouwbare partner zijn voor onze inwoners, bedrijven en ketenpartners. Informatie van inwoners, ondernemers, medewerkers en andere betrokkenen wordt veilig, vertrouwelijk en zorgvuldig behandeld. Privacy wordt te allen tijde beschermd.

Er zijn vijf niveaus van professionalisering te onderscheiden in de manier waarop informatiebeveiliging en privacy geborgd worden:



Het is onze ambitie onze werkzaamheden uit te voeren op “volwassenheidsniveau 3” volgens het CIP-model. Dat betekent dat alle werkzaamheden worden uitgevoerd volgens een vastgestelde werkwijze worden uitgevoerd.

De ambitie sluit aan bij de conclusies en aanbevelingen van het regionale rekenkameronderzoek over onze informatiebeveiliging en privacybescherming. In juli 2022 is daarvan het eindrapport “Weten wat je moet weten” gepubliceerd.

Het onderzoek van de rekenkamer heeft duidelijk gemaakt dat een professionalisering van de informatiebeveiliging en privacybescherming noodzakelijk is, wil onze gemeente de veiligheid van gegevens van inwoners en bedrijven in voldoende mate kunnen borgen. Niveau 3 wordt algemeen gezien als het minimale niveau waarop een gemeente moet zitten.

Naar aanleiding van het rapport van de rekenkamer heeft de raad het college verzocht een plan op te stellen om de volwassenheid van het huidige niveau 1,5 naar niveau 3 te brengen. Het College heeft de ambitie overgenomen om naar niveau 3 te groeien. De aanpak daarvoor is vastgelegd in het Plan van Aanpak - Informatieveiligheid en privacy naar volwassenheidsniveau 3. De raad heeft dit voorstel aangenomen in september 2023.

Het volwassenheidsniveau 3 dient eind 2025 behaald te zijn.

Naar verwachting sluit dit niveau ook goed aan bij de verplichtingen voor gemeenten in nieuwe wetgeving op het gebied van informatiebeveiliging (NIS2/NIB2. Zie paragraaf 2.2).

2. Strategisch beleid

2.1. Inleiding

Deze beleidsnota presenteert het strategisch Informatiebeveiligings- en privacy beleid voor de jaren 2024 tot 2027. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen Informatiebeveiligings- en privacyplan 2024.

Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2. Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het beleid zijn de volgende:
- Baseline informatiebeveiliging overheid (BIO) en de NIS2;
- Algemene Verordening Gegevensbescherming (AVG);
- De Wet Politiegegevens (Wpg);
- De 10 principes voor informatiebeveiliging;
- Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten;
- Informatie uit incidenten, inbreuken op de beveiliging en datalekken;
- Artificial Intelligence (AI) en algoritmes.

2.2.1. De BIO en de NIS2
De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Het is ook een manier om prioriteiten te stellen zodat de aandacht uitgaat naar die onderwerpen waar de risico's het grootst zijn. Zie ook 2.2.5.

Overheden hebben met elkaar afgesproken dat zij de BIO implementeren in de eigen organisatie. Naar verwachting zal binnen korte tijd er ook een direct wettelijke verplichting komen. De Europese richtlijn Network and Information Systems Directive 2 (NIS2), die in Nederland Netwerk- en informatiebeveiligingsrichtlijn (NIB2) heet, zal leiden tot een wettelijke verplichting voor gemeenten om aan de BIO te voldoen (wordt verankerd in de Wbni). Op basis van de informatie die op dit moment (januari 2024) bekend is, zullen gemeenten als essentiële entiteit aangewezen worden. Dat is de zwaarste categorie.

Vanaf eind 2024 zal de wetgeving waarschijnlijk in werking treden. Gemeenten en samenwerkingsverbanden van gemeenten zullen dan:
- *Aan de BIO moeten voldoen;*
- *Incidenten moeten melden bij de IBD;*
- *Bestuurders moeten trainen op gebied van informatiebeveiliging;*
- *Te maken krijgen met toezicht voor- en achteraf.*

Met het strategisch beleid en de uitwerking ervan zullen we voldoen aan de verplichtingen, zoals nu bekend.

2.2.2. De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Berg en Dal is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de AVG.

2.2.3. De Wpg
De gemeente heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de Wet Politiegegevens (Wpg). Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risicoinschatting, registratie en logging, meldplicht en documentatieplicht.

2.2.4. De 10 principes voor informatiebeveiliging
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn in Bijlage B opgenomen.

2.2.5. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten en risico-analyse
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

We hebben daarom een risicoanalyse uitgevoerd op basis van dit dreigingsbeeld. Deze is als een afzonderlijk document beschikbaar. De uitkomsten zijn gebruikt bij het opstellen van het informatiebeveiligings- en privacyplan.

2.2.6. Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd, het ISMS. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3. Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.

Binnen gemeenten wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook teams die zich met PA bezig houden[3]. Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR)[4]. In de komende planperiode zullen wij uitzoeken in hoeverre al gebruik wordt gemaakt van PA.

2.4. Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.

Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacybeleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven ‘Gemeentelijk Informatiebeveiligings- en privacyplan’.

2.5. Scope informatiebeveiliging en privacy

De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), Wpg, (Basisregistratie personen) BRP, wet- en regelgeving Reisdocumenten (PNIK/PUN), DigiD[5] en Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.

2) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.
3) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
4) https://www.cert-wm.nl/csir
5) DigiD is een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren, een soort digitaal paspoort voor overheidsinstanties.

2.6. Uitgangspunten

Het bestuur, het managementteam (MT) en teamleiders spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het bestuur stelt het beleid vast en draagt zorg voor de naleving ervan. Het MT maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy) risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het MT dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het IB&P beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1. Strategische doelen

De strategische doelen van het IB&P beleid zijn:

- Het managen van de informatiebeveiliging;
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens;
- Het toepassen van dataminimalisatie;
- Het minimaliseren van risico's van menselijk gedrag;
- Het voorkomen van ongeautoriseerde toegang;
- Het garanderen van correcte en veilige informatievoorzieningen;
- Het beheersen van de toegang tot informatiesystemen;
- Het waarborgen van veilige informatiesystemen;
- Het adequaat reageren op incidenten;
- Het beschermen van (kritieke) bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen;
- Het waarborgen van de naleving van dit beleid.

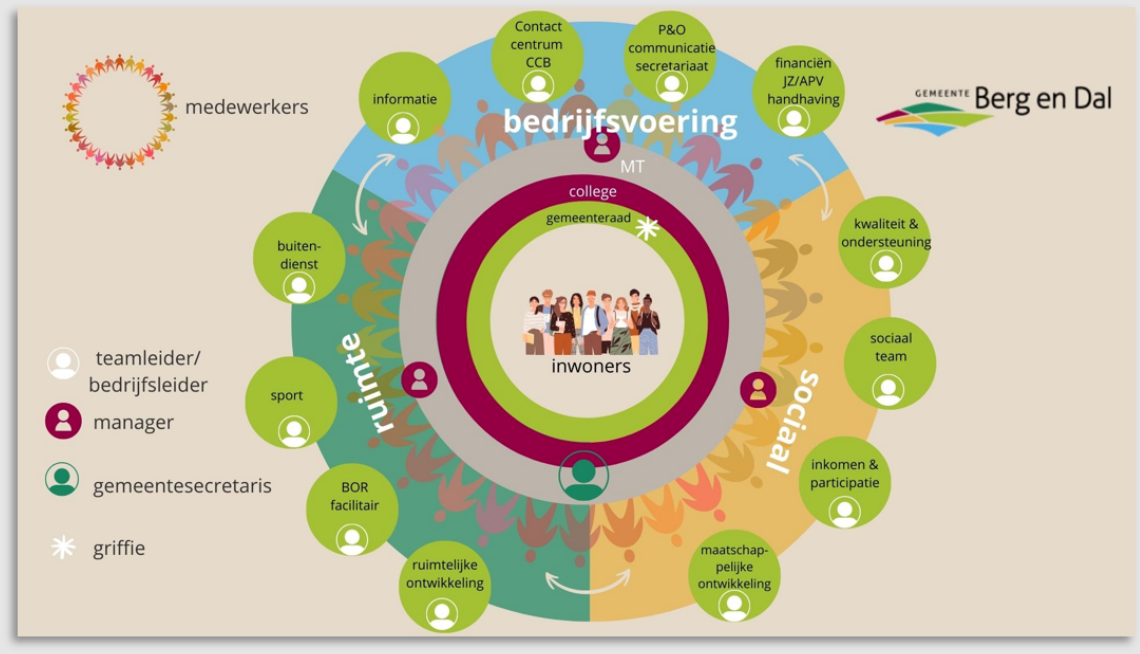
2.6.2. Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Berg en Dal hebben een interne eigenaar die de vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare informatievoorziening en privacybescherming. In het IB&P plan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.3. IB&P governance

De organisatiestructuur van de gemeente ziet er per november 2023 als volgt uit:



Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch IB&P-beleid vast.
- De gemeenteraad heeft een controlerende rol. De raad dient de naleving van de wet- en regelgeving op het gebied van informatiebeveiliging en privacy toetsen.
- Het MT stelt jaarlijks het Informatiebeveiligings- en privacyplan vast.
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming (ISMS)[6].
- Het MT is verantwoordelijk voor het vragen om informatie bij de teamleiders en ziet erop toe dat de teamleiders adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken. De CISO brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG en de WPG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- Het MT en de teamleiders stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de FG. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en/of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teamleiders zijn verantwoordelijk voor de borging van de AVG dan wel de Wpg binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De teamleiders zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.

6) NB: veel van deze documenten zijn tot stand gekomen in het zaaksysteem en zullen daar ook in opgeslagen blijven.

- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamleiders voeren dataclassificaties informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG uit om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de teamleider en de medewerker.

2.6.4. Randvoorwaarden

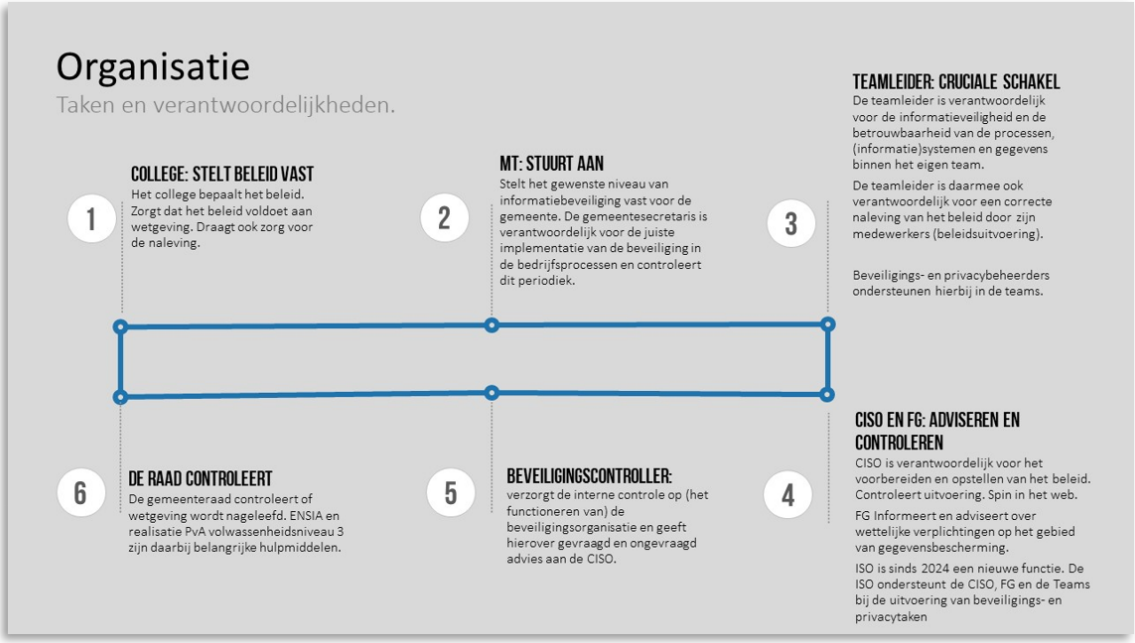
Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan opgesteld onder leiding van de Teamleider Informatie, gebaseerd op:
  - Dit IB&P-beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten zoals de WPG-audit;
  - het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risico-analyses en DPIA's;
  - De door de teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P- plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken, verantwoordelijkheden & verantwoording

3.1. Organisatie, taken, verantwoordelijkheden



- **Het college van B en W** is eindverantwoordelijk voor informatiebeveiliging en privacy.

- **Het MT** stelt het beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
- **De teamleiders** zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging en privacybescherming. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Berg en Dal hebben een interne eigenaar die primair verantwoordelijk is voor de bescherming van de gegevens.
- **De Chief Information Security Officer** (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- **De Functionaris voor Gegevensbescherming** (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG en de Wpg voorschrijft.
- **De beveiligingscontroller** verzorgt de interne controle op (het functioneren van) de beveiligingsorganisatie en geeft hierover gevraagd en ongevraagd advies aan de CISO.
- **De gemeenteraad** controleert het college op de naleving van wet- en regelgeving op het gebied van informatiebeveiliging en privacy.

Een uitwerking hiervan is te vinden in het document Informatiebeveiligingsorganisatie 2024-2027.

3.2. Verantwoording

Het bestuur van de gemeente Berg en Dal legt op verschillende manieren verantwoording af over het gevoerde beleid.

Belangrijke onderwerpen hierbij zijn de verantwoording via:
- ENSIA;
- Wpg-audit, en
- Accountantscontrole.

ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Zowel aan de raad als aan stelselhouders voor DIGID en bijvoorbeeld SUWI.

De verantwoording over de informatiebeveiliging en privacybescherming komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging en privacy. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG.

Wpg

De wet Politiegegevens (Wpg) stelt de kaders voor het omgegaan met politiegegevens. Hoewel het merendeel van de persoonsgegevens die binnen de gemeente worden verwerkt onder de AVG valt, werken we ook met politiegegevens. Hierop is de Wpg van toepassing. De naleving van de verplichtingen uit de Wpg door de gemeente moet periodiek geaudit worden door een externe auditor. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegevens (AP).

Accountantscontrole

Informatiebeveiliging en privacy maakt deel uit van de jaarlijkse controle van de jaarrekening door de accountant.

4. Vaststelling

Dit Strategisch Gemeentelijk Informatiebeveiligings- en privacy beleid laat zien dat de gemeente Berg en Dal informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op: 19 maart 2024 door het college van Gemeente Berg en Dal

Edwin van der Velde
Gemeentesecretaris

Mark Slinkman
Burgemeester

Bijlage A: Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid.

Eén normenkader
Het gebruik van één normenkader voor de gehele overheid biedt een aantal voordelen:
- Het versterken van de informatieveiligheid door betere afstemming binnen ketens van overheden en andere partijen;
- Administratieve lastenverlichting bij overheid en bedrijven, zowel afnemers als leveranciers, door uniforme beveiligingsnormen bij de overheid;
- Aansluiting bij internationale regelgeving en standaarden;
- Vermindering van onderhoudskosten.

Implementatie BIO
De BIO is in december 2018 vastgesteld door de Ministerraad voor de Rijksoverheid. Daarvoor was door de gemeenten, waterschappen en provincie reeds besloten tot invoering van de BIO. De overheidslagen zijn per 1-1-2019 gestart met de implementatie van de BIO. Iedere overheidslaag heeft daarvoor zelf een implementatiepad opgesteld. De minister van BZK heeft bepaald dat in het digitale verkeer met het Rijk de BIO wordt gehanteerd.

BIO en de 'pas-toe-of-leg-uitlijst'
Informatiebeveiligingsstandaarden ISO 27001 en ISO 27002 zijn geplaatst op de 'pas toe of leg uit'-lijst) van het Forum Standaardisatie. Op de die lijst wordt de verhouding tussen de ISO-standaard 27001 en 27002 met de BIO uitgelegd. De BIO is gebaseerd op de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017. Op specifieke controls geeft de BIO een nadere invulling in de vorm van overheidsmaatregelen. De overheid heeft zich verplicht de BIO te implementeren.

De tekst van de BIO is hier te downloaden.

Bijlage B: De 10 principes voor informatiebeveiliging / 6 beginselen van de AVG

1. De 10 principes voor informatiebeveiliging
Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren, zowel binnen de eigen organisatie, maar ook daarbuiten. Als professionele organisatie past hierbij dat de gemeente ook de beveiliging van informatie adequaat organiseert. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien.

Bij de uitwisseling moet de gemeente te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid heeft om de gegevens van de inwoners onder alle omstandigheden te beschermen.

Bestuurlijke aanvulling op de normen en regels
De principes gaan over waarden die de bestuurders en afdelingsmanagers zichzelf opleggen. Deze waarden zijn verbonden aan de waarden van de organisatie. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie.
Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Toelichting:

1. Bestuurders bevorderen een veilige cultuur
Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als de organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunnen we adequaat reageren op dreigingen en samenhangende risico's.

2. Informatiebeveiliging is van iedereen
Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen de organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3. Informatiebeveiliging is risicomanagement
Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten. Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak afdelingsmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Afdelingsmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4. Risicomanagement is onderdeel van de besluitvorming
Risicomanagement is onderdeel van alle besluiten en risicomanagement is 'chefsache'. U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw afdelingsmanagers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6. Informatiebeveiliging is een proces
Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier. Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7. Informatiebeveiliging kost geld
Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.
Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8. Onzekerheid dient te worden ingecalculeerd
De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden.
Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt. Verbetering komt voort uit leren en ervaring.

9. Risicobeheer wordt voortdurend verbeterd door leren en ervaring
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed de informatiehuishouding ook beveiligd is, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10. Het bestuur controleert en evalueert
Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp.

Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

11. De 6 beginselen van de AVG
De Algemene verordening gegevensbescherming (AVG) kent 6 basisprincipes, in de AVG 'beginselen' genoemd. Die staan in artikel 5 van de AVG. Elke organisatie die persoonsgegevens verwerkt, moet zich hieraan houden. En dit kunnen aantonen. Dat is de verantwoordingsplicht.

De 6 AVG-beginselen zijn:
1. rechtmatigheid, behoorlijkheid en transparantie;
2. doelbinding;
3. dataminimalisatie;
4. juistheid;
5. opslagbeperking;
6. vertrouwelijkheid en integriteit.

1. Rechtmatigheid, behoorlijkheid en transparantie
Organisaties mogen persoonsgegevens alleen verwerken in overeenstemming met de wet. Dan is de verwerking rechtmatig. Een verwerking die niet aan de AVG voldoet, is dus onrechtmatig.
Voor betrokkenen moet het behoorlijk en transparant zijn hoe en waarom hun persoonsgegevens verwerkt worden. Zij moeten in ieder geval op de hoogte zijn van de identiteit van de organisatie die hun

persoonsgegevens verwerkt. Ook moet het doel van de gegevensverwerking duidelijk zijn en moet er een geldige grondslag voor zijn.

2. Doelbinding
Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven.
Het doel waarvoor een organisatie persoonsgegevens gaat verwerken, moet verenigbaar zijn met het doel waarvoor deze gegevens zijn verzameld. Oftewel: de organisatie mag de gegevens niet ineens voor een heel ander doel gebruiken.

3. Dataminimalisatie
Als organisaties persoonsgegevens verwerken, moeten ze daarbij uitgaan van het principe ‘zo min mogelijk’. Dat houdt bijvoorbeeld in dat de verwerking van de gegevens moet passen bij het doel. En dat de organisatie niet meer gegevens mag verwerken dan noodzakelijk is om het doel te bereiken.

4. Juistheid
De verwerkingsverantwoordelijke moet ervoor zorgen dat de gegevens juist zijn. En de gegevens actualiseren als dat nodig is.
Mensen kunnen ook aan organisaties vragen hun persoonsgegevens aan te passen als die niet kloppen. Dat is het recht op rectificatie.

5. Opslagbeperking
Organisaties moeten persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Organisaties mogen gegevens dus maar een bepaalde tijd bewaren.

6. Vertrouwelijkheid en integriteit
De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere persoonsgegevens, zoals over iemands gezondheid, gelden extra strenge regels.