GEMEENTE BEUNINGEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Beuningen

Nr. 34548

28 januari 2025

Strategisch Informatiebeveiliging- en Privacy Beleid 2025-2028

De raad van de gemeente Beuningen;

gelezen het voorstel van het college van burgemeester en wethouders van 5 november 2024.

B E S L U I T
om het volgende vast te stellen:

Het Strategisch Informatiebeveiliging- en Privacy Beleid 2025 – 2028

Hoofdstuk 1 Managementsamenvatting

Paragraaf 1.1 Inleiding

De gemeente Beuningen werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners (hierna: inwoners). Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde- en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente (persoons)gegevens verwerkt. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze (persoons)gegevens omgaat.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker.
De gemeente Beuningen is zich hiervan bewust en wil door middel van dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna: AVG). 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 2025 tot 2028 en vervangt het verouderde informatie- en privacybeleid.

Paragraaf 1.2 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 2025). Daarnaast wordt het beleid elke drie jaar geëvalueerd. De verdere uitwerking van dit beleid is – waar relevant – vastgelegd in de operationele documenten binnen de gemeenten, zoals concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken en hoe om te gaan met privacyrechten van betrokkenen.

Paragraaf 1.3 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 is de opdracht uitgezet om een plan van aanpak op te stellen om volwassenheidsniveau 3 te bereiken.
Naar verwachting treedt in 2025 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]

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

Paragraaf 1.4 Taken en verantwoordelijkheden
Een uitgebreidere uitwerking van de taken en rollen is in het document informatiebeveiligingsorganisatie te vinden.

1.5 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.

Hoofdstuk 2. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2025 tot 2028. Het vervangt het in 2022 vastgestelde privacybeleid 2022-2025 en het informatiebeveiligingsbeleid 2024-2027.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.
Met dit 'Strategisch Informatiebeveiligings- en privacybeleid 2025 tot 2028' 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).

Paragraaf 2.1 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), Privacy Officer (PO), 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 2025-2028".
Samengevat is het nieuwe informatiebeveiligings- en privacybeleid uitgewerkt in de volgende documenten:
Strategisch Informatiebeveiliging- en privacybeleid 2025-2028;
Informatiebeveiligingsorganisatie 2025-2028;
Informatiebeveiligings- en privacyplan 2025.

Paragraaf 2.2 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 informatieverwerkende 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.

Paragraaf 2.3 Privacy & Gegevensbescherming (AVG/Wpg)
Privacy is de bescherming van de privésfeer, voor de gemeente Beuningen betekent dit voornamelijk het beschermen van de persoonlijke gegevens van haar inwoners en medewerkers. Dit willen we goed regelen in de gemeente Beuningen. 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. De definities van art. 4 AVG hebben in dit beleidsdocument, voor zover het over privacy gaat, dezelfde betekenis. Denk hierbij aan begrippen als: persoonsgegevens, verwerking, verwerker en verwerkingsverantwoordelijke. De uitwerking hiervan is opgenomen in Bijlage C met de begripsbepaling.

Paragraaf 2.4 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.

Paragraaf 2.5 Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy
De gemeente Beuningen 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. De aanpak daarvoor is vastgelegd in het Plan van Aanpak - Informatieveiligheid en privacy naar volwassenheidsniveau 3. Dit plan van aanpak ligt ook ten grondslag aan dit beleid.
Dit niveau sluit aan bij de verplichtingen voor gemeenten in nieuwe wetgeving op het gebied van informatiebeveiliging (NIS2/NIB2. Zie paragraaf 2.2).

Hoofdstuk 3 Strategisch beleid

Paragraaf 3.1 Inleiding

Deze beleidsnota presenteert het strategisch Informatiebeveiligings- en privacy beleid voor de jaren 2025 tot 2028. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen Informatiebeveiligings- en privacyplan 2025.
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.

Paragraaf 3.2 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.

Paragraaf 3.2.1 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 3.2.4.
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 cyberbeveiligingswet heet, zal leiden tot een wettelijke verplichting voor gemeenten om aan de BIO te voldoen, dit wordt verankerd in de nieuwe wetgeving. Op basis van de informatie die op dit moment (september 2024) bekend is, zullen gemeenten als essentiële entiteit aangewezen worden. Dat is de zwaarste categorie.
Vanaf medio 2025 zal naar verwachting de wetgeving 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.

Paragraaf 3.2.2 De AVG & Wpg

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Beuningen 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. Voor strafrechtelijke gegevens geldt de Wet Politiegegevens (Wpg). Indien van toepassing moet de gemeente hiervoor beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten.

Paragraaf 3.2.3 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.

Paragraaf 3.2.4 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.

Paragraaf 3.2.5 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.

Paragraaf 3.2.6 Artificial Intelligence & algoritmes
De mogelijkheden en de toegankelijkheid van Artificial Intelligence (AI) heeft de afgelopen jaren veel ontwikkelingen doorgemaakt. Deze ontwikkelingen hebben ook impact op het informatiebeveiligings- en privacybeleid.
De gemeente beweegt mee met deze ontwikkelingen. De gemeente hecht waarde aan het ethisch en verantwoord omgaan met informatie en gegevens en ook met AI en algoritmes. Hiervoor zijn verschillende ethische richtlijnen opgesteld om het gebruik van AI door de gemeente op een ethische en eenduidige manier te laten verlopen.

Paragraaf 3.2.7 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 Normatiek2 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.

Paragraaf 3.3 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’.

Paragraaf 3.3.1 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), DigiD5 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.
Voorts is dit document, voor zover het over privacy gaat, van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente Beuningen, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Paragraaf 3.3.2 Toepasselijke wettelijke kaders
Verwerkingen van persoonsgegevens zijn gebonden aan wet- en regelgeving. In deze wet- en regelgeving staan bepalingen die aangeven hoe met de bescherming van persoonsgegevens moet worden omgegaan.
De belangrijkste wettelijke kaders staan in:
Archiefwet 1995.
Artikel 8 Europese Verdrag voor de Rechten van de Mens;

Artikelen 10 t/m 13 Grondwet;
De Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG;
De Wet politiegegevens (WPG) en het Besluit politiegegevens;
NIS2/Cyberbeveiligingswet
Wetten gericht op de uitvoering in specifieke sectoren zoals: Wet Maatschappelijke Ondersteuning 2015l
Participatiewet;
Jeugdwet;
Omgevingswet;
Wet open overheid (WOO)
Wet Basis Registratie Personen;
Drank- en Horecawet;
Het wetboek van strafrecht

Paragraaf 3.4 Uitgangspunten
De raad, het bestuur, het managementteam (MT) en teamleiders/proceseigenaren spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. De raad stelt het beleid vast en het bestuur 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.

Paragraaf 3.4.1 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.

Paragraaf 3.4.2 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 Beuningen 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 en beleid kunnen periodiek worden 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.

Paragraaf 3.4.3. 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 manager bedrijfsvoering, 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/proceseigenaren 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.

Hoofdstuk 4. Organisatie, taken, verantwoordelijkheden & verantwoording

Paragraaf 4.1 Organisatie, taken en verantwoordelijkheden
De volgende functies zijn binnen de organisatie belegd:
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 Privacy Officer (PO) heeft een uitvoerende rol en ondersteunt de organisatie bij het privacybeleid . Hierbij is de PO onderdeel van de beleidsvoorbereiding en coördineert, controleert en adviseert op de uitvoering hiervan.

Paragraaf 4.2 Verantwoording
Het bestuur van de gemeente Beuningen legt op verschillende manieren verantwoording af over het gevoerde beleid.
Belangrijke onderwerpen hierbij zijn de verantwoording via:
ENSIA;
WPG-Audit;
Accountantscontrole.

Paragraaf 4.2.1 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.

Paragraaf 4.2.2 Accountantscontrole
Informatiebeveiliging en privacy maakt deel uit van de jaarlijkse controle van de jaarrekening door de accountant.

Hoofdstuk 5. Vaststelling

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

Aldus besloten in de openbare vergadering van de raad, gehouden op 17 december 2024
De griffier, Esther Jonkman
De voorzitter, Daphne Bergman

Bijlage 1 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 2 De10 principes voor informatiebeveiliging / 6 beginselen van de AVG

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.
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.
Rechtmatigheid, behoorlijkheid en transparantie
Rechtmatige grondslag
Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. De gemeente Beuningen heeft inzichtelijk welke persoonsgegevens zij bijhoudt, waar ze vandaan komen en met wie ze worden gedeeld. De gemeente Beuningen houdt een verwerkingsregister bij waarin dit beginsel is uitgewerkt.
Behoorlijkheid
De gegevensverwerking moet behoorlijk zijn. De Gemeente Beuningen geeft hier invulling aan met behulp van het onderstaande:
Privacy by Default en Privacy by Design
De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacyvriendelijk mogelijk.
ii. Data protection impact assessment (DPIA)/ Effectenbeoordeling
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van een verwerking van persoonsgegevens. De gemeente voert in dat geval een

(Pre-)DPIA. Als daaruit blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen.
iii. Samenwerking(en)
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten. Hiervoor wordt zoveel mogelijk gebruik gemaakt van de modelovereenkomst van VNG-realisatie.
gg. Samenwerkingsverbanden
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids-)organisaties om een taak van algemeen belang uit te voeren.
In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.
Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Transparantie heeft ook beperkingen wanneer er sprake is van legitieme uitzonderingen. Dit kan zijn in situaties die betrekking hebben op de openbare orde en veiligheid. De gemeente kan, met inachtneming van de wet- en regelgeving, een voorbehoud maken op het transparantiebeginsel.
Rechten van betrokkenen
Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt.
Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.
Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.
Verwerkingsregister (art. 30 AVG)
De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt
Het verwerkingsregister van de gemeente Beuningen is een levend document, deze wordt doorlopend up-to-date gehouden met de nieuwste verwerkingen van persoonsgegevens. Het verwerkingsregister wordt online gepubliceerd. De laatste versie van het verwerkingsregister van de gemeente Beuningen is te vinden op de gemeentelijke website.
Doelbinding
De gemeente Beuningen verzamelt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen.
Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). Zo heeft de gemeente altijd inzichtelijk voor welk doel zij persoonsgegevens verwerkt.
Subsidiariteit: bij de verwerking van persoonsgegevens wordt erop toegezien dat een inbreuk op de persoonlijke levenssfeer van de betrokkenen zoveel als mogelijk wordt beperkt. Er wordt altijd nagegaan of het doel ook met minder ingrijpende middelen kan worden bereikt.
Proportionaliteit: de inbreuk op de belangen van betrokkenen mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.
Dataminimalisatie
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.
Juistheid

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

Opslagbeperking

De gemeente Beuningen moet persoonsgegevens verwijderen zodra die niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Derhalve mag de gemeente gegevens slechts voor een bepaalde tijd bewaren.
De gemeente stelt de bewaartermijnen van een verwerking vast aan de hand van wettelijke bepalingen en selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk.
De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Vertrouwelijkheid en integriteit

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

Bijlage 3: Begripsbepaling

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;
Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
Betrokkene: Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.
Verwerkingsregister: Het verwerken van persoonsgegevens is elke handeling met persoonsgegevens. Zoals verzamelen, bewaren, raadplegen, wijzigen, vernietigen of delen van persoonsgegevens. De gemeente Beuningen houdt een register bij van alle verwerkingen van persoonsgegevens.
Privacyrechten : Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt.
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.
Minimale gegevensverwerking: 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.
Verantwoording: 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 vasn 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.