GEMEENTE BREDA

GEMEENTEBLAD

Officiële uitgave van de gemeente Breda

Nr. 524232

16 december 2024

Strategisch beleid voor Gegevensbescherming 2024 -2027

Bekendmaking
Burgemeester en wethouders van Breda maken bekend dat zij op 19 november 2024 het Strategisch beleid voor Gegevensbescherming 2024 – 2027 hebben vastgesteld.

Inwerkingtreding
Het beleid wordt van kracht met ingang van de dag na deze bekendmaking.

Rechtsmiddelen
Tegen het besluit tot vaststelling van het beleid is geen bezwaar of beroep mogelijk.

Strategisch beleid voor Gegevensbescherming 2024 -2027

1. Inleiding

Doel en Doelgroep
Het doel van dit strategische beleid is het beschrijven van de organisatie en het proces voor de borging en beheersing van gegevensbescherming. Het legt daarmee een basis voor:

1. De waarborging van de bescherming van de persoonlijke levenssfeer van burgers, medewerkers en andere betrokkenen, vallende binnen het werkveld van de gemeente.
2. Een doel gebonden, veilige informatievoorziening en gegevensverwerking.
3. Een betrouwbare informatievoorziening.

De gemeente Breda moet in control zijn op haar gegevensbescherming. Daarom legt zij primair verantwoording af aan de interne toezichthouder, de Functionaris Gegevensbescherming (FG) en de Gemeenteraad. Extern aan haar samenwerkingspartners, de Autoriteit Persoonsgegevens en aan het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (hierna: BZK) in het kader van de ENSIA-verantwoording.

Reikwijdte van het beleid
Het strategisch gegevensbeschermingsbeleid richt zich primair op bestuur en management, de privacy-, data- en informatiebeveiligingsorganisatie en leidinggevenden. Het is van toepassing op alle medewerkers, inhuur, bezoekers en externe relaties. Het is ook van toepassing op iedereen binnen de Gemeente die met of namens andere gemeentes verantwoordelijk is voor de uitvoering van het gemeentelijke beleid.

Kortom: iedereen die intern dan wel samen met anderen op enige manier te maken heeft met (aspecten van) het stelsel van beveiligingsmaatregelen t.a.v. webapplicaties en/of de infrastructuren voor de netwerksegmenten met webapplicaties in het algemeen, en DigiD en andere authenticatie- en identificatiediensten in het bijzonder.

Het strategisch beleid vormt de basis voor de tactische beleidsplannen en geeft daarmee richting aan de verdere invulling van gegevensbescherming op tactisch en operationeel niveau. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifiek beleid, aanvullend op dit strategisch beleid. In het volgende hoofdstuk wordt de kern van het strategisch beleid uiteengezet.

2. Gegevensbescherming

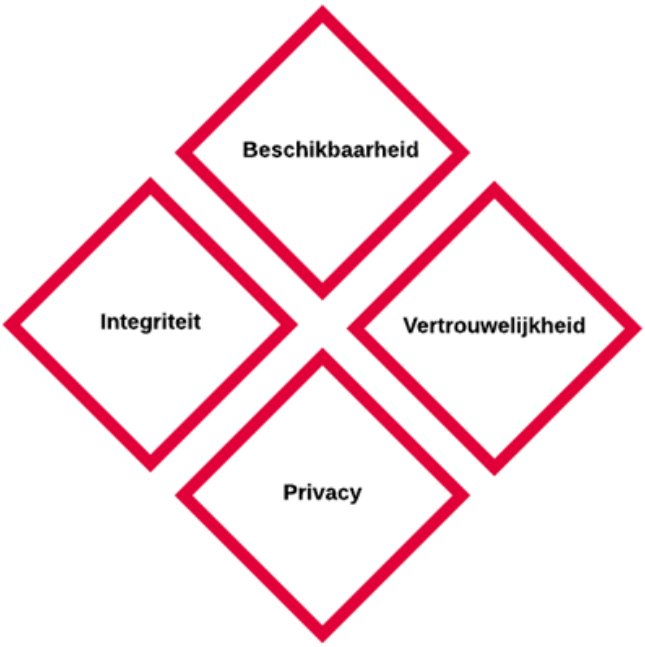
De gemeente Breda sluit aan bij het kader van de Informatiebeveiligingsdienst (IBD) en definieert het veilig omgaan met gegevens als: Het proces van het beschermen van gegevens, informatie en gerelateerde componenten (zoals processen, geautomatiseerde informatiesystemen, personen en papieren documenten) tegen onbedoelde of vooropgezette inbreuken op:

Beschikbaarheid: De mate waarin gegevens en gegevensverwerkingen op de juiste momenten beschikbaar zijn voor gebruikers.

Integriteit: De mate waarin de juistheid en volledigheid van gegevens is gewaarborgd.

Vertrouwelijkheid: De mate waarin gegevens alleen toegankelijk zijn voor degenen die hiervoor gerechtigd zijn.

Privacy: De mate waarin personen invloed hebben op de manier waarop de gemeente met hun gegevens omgaat. De mate waarin ze het recht hebben hun persoonlijke levenssfeer te beschermen.



Het treffen van gegevensbeschermingsmaatregelen moet voorkomen dat de gegevensverwerking wordt verstoord of dat gegevens beschadigd raken. De keuze welke maatregelen nodig zijn, is afhankelijk van de zwaarte van de eisen die worden gesteld aan de beveiliging van een proces of een informatiesysteem. Maatregelen worden daarom bepaald op basis van een risicomanagementproces.

Visie en missie gegevensbescherming

Visie op gegevensbescherming

De gemeente Breda verwerkt persoonsgegevens en informatie van de inwoners van Breda en omliggende gemeenten en van medewerkers.

Het gaat hier om basisgegevens zoals namen, adressen, telefoonnummers maar ook om bijvoorbeeld gezondheidsgegevens die in het kader van dienstverlening of taken van de gemeente noodzakelijk zijn. Met al deze gegevens moet op een zorgvuldige en veilige manier worden gewerkt, zodat deze niet voor andere doeleinden worden gebruikt of door derden misbruikt kunnen worden.

De gemeente zet zich continu in om gegevens en informatie zo goed mogelijk te beschermen. Door gebruik te maken van internationaal geaccepteerde informatiebeveiligingsnormen en actief de eisen uit de privacyregelgeving toe te passen, geeft de gemeente Breda haar inwoners, bedrijven en samenwerkingspartners de zekerheid dat ze op een veilige manier met informatie en gegevens werkt.

Missie gegevensbescherming
Als inwoner van een gemeente moet je erop kunnen vertrouwen dat de gemeente op een zorgvuldige en veilige wijze omgaat met jouw gegevens. Het is de gemeente die vanuit deze toegekende vertrouwensfunctie haar taak moet uitvoeren. Dit betekent dat iedereen erop moet kunnen vertrouwen dat de gemeente gegevens op een veilige manier verwerkt. Het is de gemeente die hierin vanuit haar rol als overheid het goede voorbeeld dient te geven en het fundament vormt voor gegevensbescherming in haar stad. Gemeente Breda kiest er daarom voor om transparant en in control te zijn op de bescherming van gegevens en informatie.

De gemeente Breda zet zich in om het fundament te zijn waar gegevens en informatie op een zorgvuldige, doelmatige en veilige wijze worden verwerkt. Voor haar eigen burgers en voor de burgers van omliggende gemeenten, die voor de verwerking van hun gegevens op de Gemeente Breda rekenen. De belangrijkste uitgangspunten hierbij zijn:

1. Risico gebaseerd werken.
Dit betekent dat het management verantwoordelijkheid neemt voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.

2. Verstevigen van de governance .
De verantwoordelijkheid voor gegevensbescherming is een gezamenlijke verantwoordelijkheid van RDI en de proceseigenaren. Dit betekent een belangrijke rol voor directeuren, afdelingshoofden en teamleiders. Hierbij is het essentieel dat elk bedrijfsproces een aanwijsbare eigenaar heeft en dat de belangrijkste processen voor inwoners, bedrijven of medewerkers van gemeente Breda als organisatie in beeld zijn.

3. Integratie in de planning- en control cyclus.
Er wordt op diverse manieren gecontroleerd en gerapporteerd in hoeverre er wordt voldaan aan de verplichtingen en eisen die gelden op het gebied van gegevensbescherming. Verantwoording hierover vindt plaats in verschillende gremia, namelijk: I-board, Directeuren Overleg (DO), College van B&W en Gemeenteraad. Gegevensbescherming wordt hierdoor onderdeel van de Planning en Control cyclus.

4. Strategische doelen gegevensbescherming gemeente Breda

Het bestuur, de directie en afdelingshoofden (proceseigenaren) spelen een cruciale rol bij het uitvoeren van dit strategisch beleid voor gegevensbescherming. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor gegevensbescherming op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Het gehele gemeentelijk management geeft een duidelijke richting aan gegevensbescherming en demonstreert dat zij gegevensbescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven ervan voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, samenwerkingsverbanden, objecten, informatiesystemen en gegevens(verzamelingen).

Strategische doelen
De strategische doelen van het gegevensbeschermingsbeleid zijn:
- Het beschermen en correct verwerken van (persoons)gegevens
- Het organiseren van gegevensbescherming.
- Adequate bescherming van bedrijfsmiddelen.
- Het beperken van risico's van menselijk gedrag.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen en voorkomen van ongeautoriseerde toegang.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het waarborgen van de naleving van dit beleid.

5. Risico gebaseerde gegevensbescherming

We leven in een informatie- en netwerksamenleving die steeds complexer wordt. Als gemeente maken we de stap naar een digitaal georiënteerde dienstverlening en bedrijfsvoering. Van oudsher beschikt de gemeente Breda over vertrouwelijke en privacygevoelige gegevens.

In het geval van samenwerking met externe partijen (zoals ketenpartners en leveranciers), waarbij sprake is van verwerking van persoonsgegevens, maakt de gemeente Breda indien nodig afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken zijn actueel en voldoen aan wet- en regelgeving. In situaties waarin de gemeente Breda als centrumgemeente fungeert heeft zij een belangrijke rol in de gegevensbescherming van haar samenwerkingspartners en de gemeentes voor wie zij (delen van) het gemeentelijke beleid uitvoert. Als centrumgemeente neemt zij het voortouw, ook op het gebied van gegevensbescherming en maakt zij ook met hen duidelijke afspraken. De gemeente Breda houdt toezicht op naleving van deze afspraken.

Dit betekent dat helder moet worden gemaakt:
- Wat binnen de gemeente de meest waardevolle of (privacy)gevoelige gegevens zijn;
- Welke mogelijke gebeurtenissen schade kunnen toebrengen aan deze gegevens;
- Wat de gemeente wel en niet gaat doen om de gegevens te beschermen tegen deze gebeurtenissen.

6. Wet- en regelgeving

Dit beleid is in overeenstemming met de Baseline Informatiebeveiliging Overheid (BIO v2) en de internationale standaard voor informatiebeveiliging de ISO27001/2.

Naast bovengenoemde standaarden moet de gemeente Breda de eisen en verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), de Wet politiegegevens (Wpg) en het besluit politiegegevens voor buitengewoon opsporingsambtenaren toepassen. Het voldoen aan de eisen en verplichtingen uit de AVG, de UAVG en Wpg zorgt ervoor dat privacybescherming van personen geborgd is.

Daarnaast verwerkt de gemeente Breda ook politiegegevens waarop de Wpg van toepassing is. De Wpg verwerkingen die door de gemeente Breda worden verwerkt worden gevonden in artikelen 8 en 9 omvatten:
- Artikel 8: uitvoering van de dagelijkse politietaak.
- Artikel 9: verwerkingen specifiek gericht op bepaalde personen of gebeurtenissen.

Verder heeft de gemeente Breda te maken met aanvullende wettelijke kaders voor beveiliging waaronder Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), Wet basisregistratie personen (Wet BRP), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en Paspoortuitvoeringsregeling Nederland 2001 (PUN), en de Archiefwet. De beveiligingseisen voor deze wettelijke kaders zijn voor de gemeente Breda uitgewerkt in een aantal deelbeveiligingsplannen, namelijk:
- Beveiligingsbeleidsplan Suwinet: dit plan beschrijft de wijze waarop de gemeente Breda de beveiliging rondom Suwinet geregeld heeft.
- Beveiligingsplan BRP/PUN: dit plan beschrijft de wijze waarop de gemeente Breda de beveiliging rondom de basisregistratie personen (BRP) en paspoorten en Nederlandse identiteitskaarten (PUN) geregeld heeft. Voor BRP geldt tevens het normenkader uit de wet BRP zoals dat jaarlijks middels zelfevaluaties wordt getoetst en waarover wordt gerapporteerd aan de toezichthouders.

Het beveiligingsbeleid is in lijn met het algemene beleid en de hiervoor genoemde relevante landelijke en Europese wet- en regelgeving. Onderdeel van het takenpakket van beveiliging is het volgen van de ontwikkelingen in de wet- en regelgeving, respectievelijk het vertalen van de betreffende eisen naar één of meerdere beveiligingsmaatregelen.

Dit Strategisch Beleid voor Gegevensbescherming treedt in werking na vaststelling door het college van B&W van de gemeente Breda.

7. Organisatie van gegevensbescherming

Three Lines model
Het three lines model is bedoeld voor het goed laten verlopen van governance, risicomanagement en compliance door interne beheersing. Het three lines model heeft als uitgangpunt dat het lijnmanagement als proceseigenaar verantwoordelijk is voor haar eigen processen en daarmee verantwoordelijk voor het integreren en borgen van gegevensbescherming in deze processen. Dit vraagt om bewustwording van deze verantwoordelijkheid, daadwerkelijk sturen op gegevensbescherming en hier verantwoording over afleggen. De proceseigenaar krijgt hierbij ondersteuning van de Decentrale Security en Privacy Officers (DSPO'ers).

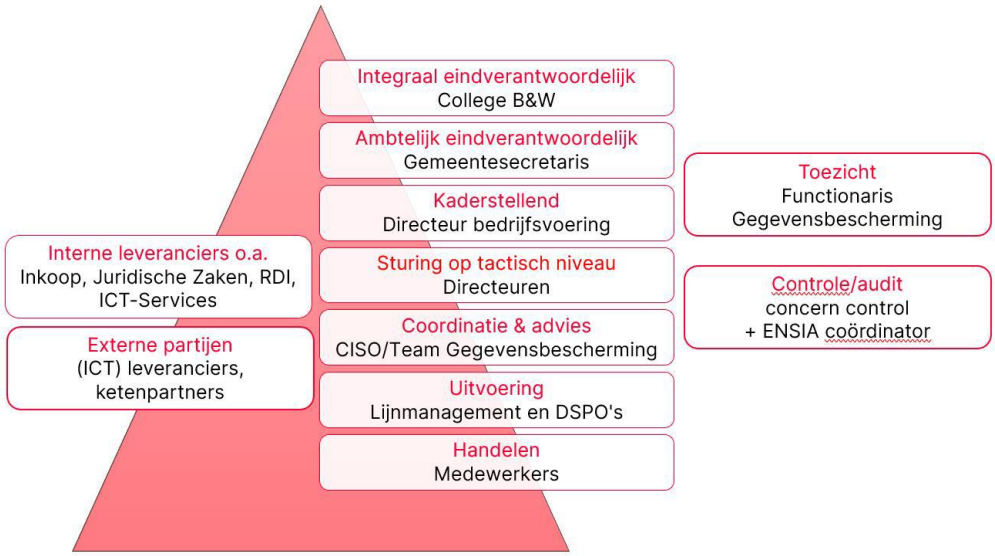
De eerste lijn wordt ondersteund door de tweede lijn. Binnen de tweede lijn bevinden zich rollen die adviseren, coördineren en bewaken maar ook zorgen voor integraal beleid op het gebied van gegevensbescherming. Vanuit het Team Gegevensbescherming worden er tweede lijns rollen vervuld door de Privacy Officers (PO's) en Information Security Officers (ISO's) en de ENSIA coördinator.

De derde lijn bestaat uit een onafhankelijke (interne) auditfunctie.

Het management zorgt voor acties (inclusief risicomanagement) om doelstellingen van de organisatie te realiseren.

Rollen en verantwoordelijkheden
Binnen de gemeente Breda zijn de verantwoordelijkheden rondom privacy, security en data gestuurd werken verdeeld over verschillende rollen en functies. We brengen de bescherming van (privacy) gevoelige data en security onder in hetzelfde risicomanagementproces ten behoeve van gegevensbescherming.

In onderstaand schema zijn de rollen en verantwoordelijkheden schematisch in beeld gebracht:



College van B&W
De gemeente Breda maakt gebruik van een 'Top-Down approach' waarin het College van B&W integraal eindverantwoordelijk is voor gegevensbescherming. In het college is één portefeuillehouder verantwoordelijk.

Directeur Bedrijfsvoering
De directeur bedrijfsvoering is verantwoordelijk voor kaderstelling en de directeuren voor sturing op tactisch niveau. Afhankelijk van de beschikbaar gestelde middelen, kan het gegevensbeschermingsbeleid uitgevoerd worden.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming houdt (onafhankelijk) toezicht op de naleving van de eisen uit de AVG en Wpg en geeft gevraagd en ongevraagd advies. De FG kan zelf onderzoeken doen of informatie en inlichtingen uit de organisatie ontvangen om de effectiviteit van genomen privacy en security maatregelen en de naleving van wet- en regelgeving te kunnen beoordelen.

De FG informeert en adviseert het bestuur, directie, management, verwerkingsverantwoordelijken en medewerkers over hun verplichtingen op grond van de AVG, de uitvoeringswet AVG en andere privacywetgeving.

Chief Information Security Officer
De Chief Information Security Officer (CISO) is strategisch adviseur voor het bestuur en ondersteunt het bestuur en organisatie vanuit een onafhankelijke positie. Overeenkomstig de behoeften en de risicobereidheid van de gemeente adviseert de CISO (on)gevraagd over informatiebeveiliging, stelt organisatie breed beleid op en coördineert de implementatie van het beleid.

De CISO biedt ook ondersteuning bij het uitvoeren van risicoanalyses. Ten slotte verzorgt hij/zij ook integrale statusrapportages, monitort hij/zij de naleving en doet hij/zij voorstellen voor verbeteringen. De CISO is het overkoepelend aanspreekpunt op het gebied van informatiebeveiliging en zorgt ervoor dat de beveiligingsorganisatie goed functioneert.

De CISO is hiërarchisch of functioneel leidinggevende van de IB organisatie.

Team Gegevensbescherming
Privacy- en Informatiebeveiligingsadviseurs

Het team gegevensbescherming bestaat uit een aantal privacy- en informatiebeveiligingsadviseurs. Deze adviseurs zijn verantwoordelijk voor het geven van (complex) gevraagd en ongevraagd advies op het gebied van informatiebeveiliging en privacy aan de organisatie. Het team adviseert de lijn bij het uitvoeren van risicoanalyses en het opstellen van rapportages. Daarnaast ondersteunt het team bij het uitdenken, het implementeren en het monitoren van security- en privacy maatregelen.

Decentrale Security- en Privacy Officers

De Decentrale Security- en Privacy Officers (DSPO's) ondersteunen de lijnorganisatie bij het (gaan) voldoen aan de privacy en security vereisten.

Management
Het management van elke afdeling en elk team is verantwoordelijk voor de gegevensbescherming. De afdelingshoofden (proceseigenaren) zijn operationeel eindverantwoordelijk voor de bedrijfsprocessen. Medewerkers handelen conform richtlijnen en voorschriften.

Leveranciers
De organisatie heeft interne leveranciers. Dit zijn o.a. de teams Inkoop, Juridische Zaken, HR, ICT-Services, RDI/ Applicatiebeheer en Facilitair. Zij zorgen ervoor dat de aangeboden diensten voldoen aan het gegevensbeschermingsbeleid en de daarop van toepassing zijnde standaarden.

Externe partijen zijn aantoonbaar compliant met het Strategisch gegevensbeschermingsbeleid van de gemeente Breda en voldoen aan de gegevensbeschermingseisen die aan de betreffende leveranciers, ketenpartners en andere samenwerkingspartijen worden gesteld vanuit Inkoop of een organisatieonderdeel.

Interne controle
Binnen de gemeente Breda vervult Concern Control een rol bij het intern auditen van de gegevensbescherming.

De ENSIA-coördinator voert de taken rondom de ENSIA-verantwoording uit.

In Bijlage I, de werking van de governance, zijn bovengenoemde rollen, taken en verantwoordelijkheden verder uitgewerkt.

8. Communicatie en bewustwording

Zoals bij de visie in hoofdstuk 1 is aangegeven, is gegevensbescherming het recht van alle personen op de bescherming van hun persoonlijke levenssfeer. Management en medewerkers van de gemeente Breda dienen zich derhalve bewust te zijn van de risico's die samenhangen met de omgang met vertrouwelijke gegevens en van de noodzaak van beveiliging. Het is daarom belangrijk dat medewerkers over voldoende kennis- en bewustzijn beschikken en blijven beschikken. In de jaarlijkse bewustwordingsplannen wordt de focus en het primaire communicatiedoel, bepaald voor het betreffende jaar. Onderwerpen hierbij zijn:

- Een streven naar kwaliteitsverbetering. Door het verhogen van het besef van de waarde van informatie voor de gemeente, houden gemeentelijke medewerkers zich beter aan procedures op dit gebied, waardoor het aantal fouten wordt verkleind.
- Het verkrijgen/behouden van een betrouwbaar imago. Voor de gemeente is vertrouwen één van de basisprincipes. Hierdoor is het van groot belang dat de gemeente betrouwbaar overkomt. Beveiligingsincidenten hebben een negatief effect op de betrouwbaarheid van de gemeente. Door een verhoging van het beveiligingsbewustzijn neemt het aantal beveiligingsincidenten af.
- De kracht van beveiliging wordt bepaald door een samenspel van technische en organisatorische factoren. Gedrag van mensen speelt hier bij een belangrijke rol. Het is daarom belangrijk dat de medewerkers van de gemeente Breda zich bewust zijn van beveiliging. Het moet een natuurlijk onderdeel zijn van hun werk. Belangrijk hierbij is uiteraard dat mensen moeten worden geholpen bij het goed uitvoeren van beveiliging, bijvoorbeeld door het zorgen voor voldoende concrete richtlijnen.

Er moeten een aantal randvoorwaarden ingevuld zijn om een effectieve en efficiënte invulling te kunnen geven op de vraag: 'Hoe kan het kennis- en bewustzijnsniveau van de medewerkers blijvend gestimuleerd, verhoogd en gestuurd worden op het gebied van beveiliging?'

Deze randvoorwaarden zijn:
Commitment van de directie en het management: De cruciale voorwaarde voor een succesvolle uitvoering van een bewustwordingsprogramma binnen de gemeente Breda is commitment. Zonder dat aan deze voorwaarde wordt voldaan is de slagingskans van een dergelijk programma beperkt.

Het bestuur controleert en evalueert: controle is belangrijk om goed inzicht te krijgen in de mate waarin het gegevensbeschermingsbeleid, bewustwording en risicomanagement ingebed zijn in de gemeente. Naast verslagen en managementrapportages zijn incidenten, en de wijze waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe binnen de gemeente Breda omgegaan wordt met dit onderwerp. Het onderwerp gegevensbescherming zal dan ook periodiek op de agenda van het Directieoverleg en het college van B&W geagendeerd worden, zodat de directie en het college haar verantwoordelijkheid kan nemen en lastige knopen kan doorhakken als dat noodzakelijk is.

Geen eenmalige exercitie: Bewustwording van gemeentelijke medewerkers binnen de gemeente is geen eenmalige zaak. Het is noodzakelijk dat er continu gestimuleerd, gestuurd en gemeten wordt. Zo wordt er constant aandacht besteed aan de ontwikkeling van het kennis- en bewustzijnsniveau. Hierbij is het wel van belang om vooraf het gewenste en het huidige kennis-, bewustzijnsniveau en gedrag in kaart te brengen. Tot slot dient het bewustwordingsprogramma ook aan te sluiten bij de organisatiecultuur van de gemeente Breda.

GEMEENTE BREDA

Bijlage I Werking governance

Aansturing van de gegevensbescherming
Verantwoordelijkheden College van B&W

- Eindverantwoordelijk voor de borging van gegevensbescherming binnen de gemeente Breda en aanspreekpunt vanuit toezichthouders;
- Stelt het strategisch beleid voor gegevensbescherming vast;
- Houdt formeel toezicht op het stelsel van gegevensbescherming dat van toepassing is op alle (persoons)gegevens die in de opdracht en/of onder medeverantwoordelijkheid van de Gemeente worden verwerkt;
- Is verantwoordelijk voor de verwerking van gegevens conform de AVG.

Verantwoordelijkheden directie

- Stelt formeel vast welke normen voor gegevensbescherming van toepassing zijn binnen de gemeente;
- Afhankelijk van de beschikbare middelen, stelt hij/zij capaciteit en budget beschikbaar voor de invoering en borging van dit beleid;
- Spreekt directeuren aan op naleving van dit beleid ook als verbetermaatregelen niet tijdig worden doorgevoerd;
- Legt verantwoording af over het gevoerde beleid en de naleving daarvan, aan het College van B&W;
- Beoordeelt de hogere restrisico's vanuit organisatieonderdelen, inclusief de verwerkingsactiviteiten die in opdracht van organisatieonderdelen elders gebeuren;
- Beslist en bewaakt de risico's die overblijven na het treffen van maatregelen (restrisico's) formeel, binnen de kaders van het College van B&W;
- Voert jaarlijks een directiebeoordeling uit op het gevoerde gegevensbeschermingsbeleid
- Beslist bij onduidelijkheid van eigenaarschap en kan verantwoordelijk voor een proces of informatiesysteem binnen de gemeente toewijzen.

Uitvoering van de gegevensbescherming
Verantwoordelijkheden directeur

- Verantwoordelijk voor de invoering van het beleid voor gegevensbescherming binnen het directieonderdeel
- Het uitdragen van dit beleid voor gegevensbescherming uit richting alle medewerkers, externe partijen, ketenpartijen en samenwerkingspartners
- Spreekt medewerkers en leidinggevenden aan op navolging van dit beleid en sanctioneert indien nodig gepast
- Formeel eigenaar van alle verwerkingen binnen het directieonderdeel
- Consulteert de CISO en het gegevensbeschermingsteam bij de ontwikkeling van onderliggende normenkaders
- Verantwoordelijk voor de implementatie van de gegevensbescherming binnen het directieonderdeel
- De directeur bedrijfsvoering is vanuit haar rol verantwoordelijk voor het ter beschikking stellen van voldoende budgetten en capaciteit.
- Verantwoordelijk voor het vragen van advies aan de FG over het al dan niet moeten uitvoeren van een DPIA.
- Verantwoordelijk voor het accepteren van restrisico's conform de 'procedure voor het nemen van risicoacceptatie besluiten'.

Verantwoordelijkheden Afdelingshoofd / teamleider

- Bewaakt dat medewerkers binnen de afdeling handelen conform het vastgestelde gegevensbeschermingsbeleid
- Verantwoordelijk voor het toetsen van de processen/informatiesystemen op gegevensbeschermingsaspecten binnen de eigen afdeling en het registreren van de uitkomsten (zgn. BIV-P ranking)
- Zorgt ervoor dat binnen zijn of haar afdeling actuele risicoanalyse(s) (waaronder DPIA's) op processen of informatiesystemen worden uitgevoerd
- Laat het gegevensbeschermingsproces uitvoeren, ondersteund door operationele gegevensbeschermingsspecialist: definieert, implementeert en voert maatregelen risico gebaseerd in
- Verantwoordelijk voor het accepteren van restrisico's conform de 'procedure voor het nemen van risicoacceptatie besluiten'.
- Stelt zeker dat alle betrokken partijen in de afdeling de noodzakelijke gegevensbeschermingsprotocollen hebben geïmplementeerd
- Verantwoordelijk voor de veiligheid van het informatiesysteem, inclusief toegangsrechten. Stelt eisen aan de gegevensbescherming van informatiesystemen binnen de afdeling
- Bewaakt dat gekozen gegevensbeschermingsmaatregelen uit risicoanalyses/DPIA's worden opgenomen in het verbeterregister en juist en volledig worden doorgevoerd en nageleefd binnen de eigen afdeling

- Zet, indien hij of zij vanuit een medewerker een datalek melding ontvangt, deze door aan het team gegevensbescherming en; zet indien hij of zij een melding over een informatiebeveiligingsincident ontvangt, deze door aan de CISO of security adviseur
- Spreekt medewerkers van zijn afdeling aan op navolging van het beleid en sanctioneert, bij niet naleving, indien nodig gepast
- Spreekt externe partijen, ketenpartners aan op navolging van het beleid en sanctioneert, bij niet naleving, indien nodig gepast
- Gaat binnen samenwerkingsrelaties het gesprek aan over navolging van het beleid en initieert verbetering
- Heeft eigenaarschap en verantwoordelijkheid van de webapplicatie en bijbehorende DigiD aansluiting

Verantwoordelijkheden Decentrale Security en Privacy Officer
- aanspreekpunt voor medewerkers binnen het bedrijfsonderdeel op het gebied van gegevensbescherming;
- uitvoeren en coördineren van inzageverzoeken (en andere rechten van betrokkenen)
- vertalen van te nemen maatregelen naar concrete taken;
- coördineert in opdracht van een afdelingshoofd/teamleider de uitvoering van gegevensbeschermingsbeleid binnen een afdeling
- bewaakt de naleving van het beleid voor gegevensbescherming binnen het organisatieonderdeel en rapporteert de voortgang periodiek aan het afdelingshoofd/teamleider
- ondersteunt medewerkers binnen de afdeling bij het opvolgen van maatregelen uit risicoanalyses (waaronder DPIA's) en het treffen van verbeterplannen
- uitvoeren van diverse controles om te beoordelen of maatregelen worden opgevolgd;
- beheert namens zijn of haar afdelingshoofd/teamleider het register van verwerkingen op processen/informatiesystemen binnen de eigen afdeling
- ondersteunt het afdelingshoofd/lijnmanager binnen een afdeling bij de gegevensbeschermingsbewustwording.
- handelt ontvangen incidenten – inclusief datalekken – op het gebied van gegevensbescherming af en maakt een analyse van het incident en zet waar nodig de meldingen en initiële analyse door naar de FG (datalek) of aan de CISO (IB-incident).

Verantwoordelijkheden privacy- en security officers uit team Gegevensbescherming
- Adviseert de afdelingshoofden/lijnmanagers proactief op het gebied van gegevensbescherming
- Werkt mee aan de ontwikkeling van nieuw beleid op het gebied van gegevensbescherming
- Coördineert en geeft periodiek trainingen aan de organisatie op het gebied van gegevensbescherming
- De operationele gegevensbeschermingsspecialisten voeren risicoanalyses uit (waaronder DPIA's) en het opstellen van verbeterplannen
- Monitort de inhoud, procesgang en voortgang van het register van verwerkingen
- Beheert het risicoregister voor wat betreft gegevensbescherming

Verantwoordelijkheden informatiemanagers
- Adviseren en ondersteunen de afdelingshoofden/lijnmanagers en de operationele gegevensbeschermingsspecialisten proactief op het gebied van gegevensbescherming.
- Kijken integraal naar vraagstukken van de vakafdelingen en zijn linking pin voor bedrijfsvoering.

Verantwoordelijkheden medewerkers
- Handelen conform richtlijnen en voorschriften
- Signaleren en melden beveiligingsproblemen, incidenten en datalekken
- Bevorderen actief een veilige werkcultuur
- Spreken elkaar aan op naleving.

Gemeente Breda heeft interne leveranciers. Dit zijn o.a. de afdelingen Inkoop, Juridische Zaken, HR, RDI en Facilitair. De verantwoordelijkheden van deze interne leveranciers zijn:

Ervoor zorgen dat de aangeboden diensten voldoen aan het gegevensbeschermingsbeleid en de daarop van toepassing zijnde standaarden

Communiceren binnen de gemeente om bewustwording te vergroten met betrekking tot het aandachtsgebied.

Verantwoordelijkheden externe partijen
- Zijn aantoonbaar compliant met het Strategisch gegevensbeschermingsbeleid van de Gemeente Breda en voldoen aan de gegevensbeschermingseisen die aan de betreffende leveranciers worden gesteld vanuit Inkoop of een afdeling.

- Signaleren risico's voor de beveiliging van informatie en de omgang met (persoons)gegevens proactief
- Melden datalekken en (mogelijke) informatiebeveiligingsincidenten, conform de contractuele afspraken, direct bij de gemeente Breda.

Coördinatie van de gegevensbescherming
Verantwoordelijkheden Chief Information Security Officer (CISO)/teamleider gegevensbescherming:
- Definieert het gegevensbeschermingsbeleid voor de organisatie
- Organiseert gegevensbescherming en de daarvoor benodigde expertise
- Zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, fysieke beveiliging en continuïteitsmanagement
- Zet een informatiebeveiligingscalamiteitenorganisatie op
- Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten
- Zorgt voor een projectportfolio voor gegevensbescherming
- Initieert en coördineert organisatiebrede gegevensbeschermingsactiviteiten en -projecten
- Zorgt voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor gegevensbescherming
- Monitort en borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen
- Monitort en borgt vanuit de tweedelijn het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design
- Monitort en borgt gegevensbewustzijn binnen de organisatie
- Monitort de relevante risico's voor de organisatie
- Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's
- Monitort en borgt de kwaliteit van informatiebeveiligingsassessments
- Monitort op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en relevante wet- en regelgeving
- Informeert bestuur en management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen
- Ondersteunt de tactische gegevensbeschermingsspecialisten bij de werkzaamheden en bepalen de dagelijkse koers en richting t.a.v. gegevensbescherming. Stelt een gecombineerd meerjarig masterplan op t.b.v. gegevensbescherming waarin de koers en richting wordt beschreven.

Controle van de gegevensbescherming
Verantwoordelijkheden concern control ten aanzien van gegevensbescherming:
- Voert in opdracht van de directie interne audits uit naar de opzet, bestaan en werking van de uitvoering van dit strategische beleid, de governance en inrichting van het ISMS. Maar kan ook ongevraagd interne audits uitvoeren en hierover rapporteren richting de directie.

Verantwoordelijkheden ENSIA-coördinator
- Voert de taken omtrent de ENSIA-verantwoording uit
- Draagt zorg voor brede betrokkenheid en draagvlak binnen de organisatie
- Borgen van tijdige inlevering van antwoorden en het volledig uploaden van documenten
- Tijdige afsluiting van implementatie van ENSIA, binnen de overeengekomen afspraken over tijd, geld en kwaliteit
- Overleg met de CISO m.b.t. afstemmen van procedures, maatregelen en controles die wel/niet worden uitgevoerd
- Brengt zijn of / haar specialistische expertise in als dat nodig is
- 'Bewaakt' in samenwerking met concern control de voortgang op audit proces.

Verantwoordelijkheden Functionaris Gegevensbescherming
(artikel 39 AVG, artikel 36 WPG):
De taken, verantwoordelijkheden en bevoegdheden van de FG.
De taken van de FG worden benoemd in art. 39 Algemene Verordening Gegevensbescherming en art. 36 Wet Politiegegevens en omvatten globaal:
- Het onafhankelijk, gevraagd en ongevraagd informeren en adviseren van de organisatie en/of de medewerkers over wettelijke verplichtingen op het gebied van gegevensbescherming.
- Onafhankelijk toezicht houden op de naleving van de AVG, aanverwante wetgeving en het interne beleid.
- Monitort de relevante risico's voor de organisatie
- Advies geven over de uitvoering en opvolging van risicoanalyses zoals een Data Privacy Impact Assessment (DPIA).
- Samenwerken met en optreden als contactpersoon voor Autoriteit Persoonsgegevens.

Onafhankelijk en zonder druk

- De FG moet onafhankelijk toezicht kunnen houden en adviseren. Daarom stelt de AVG in artikel 38 eisen aan waar de FG binnen een organisatie is gepositioneerd. Zo is in Breda de FG ondergebracht bij de afdeling Concern Control.
- De FG mag bij onderzoeken, vragen of het afgeven van adviezen niet onder druk gezet worden, of worden gestraft. Net als de leden van de OR heeft de FG ontslagbescherming daar waar het de uitvoering van haar wettelijke taken betreft.
- De organisatie is verplicht middelen ter beschikking te stellen om te voldoen aan de verplichtingen in de AVG.

GEMEENTE BREDA

Bijlage II DigiD-uitwerking norm B.01

Voor DigiD zijn de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen
- We conformeren ons aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD.
- Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst.
- Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

Eigenaarschap
- Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende afdelingshoofd eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer
- Per DigiD-aansluiting is door het genoemde afdelingshoofd of aangewezen teamleider een functioneel beheerder aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
- Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste
  - de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05)
  - de incidentprocedure en een overzicht van de incidenten (U/WA.02)
  - de dataclassificatie (U/WA.05)
  - bewijs dat de webapplicatie gehardend is (U/NW.06, tav DNSSEC)
  - de beoordeelde releases (C.08).

- Tweemaal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk afdelingshoofd of aangewezen teamleider.

Technisch
Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd.

Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.