gemeente
DEN HELDER

Bartels Consultancy B.V.
t.a.v. [redacted]
Postbus 14000
[redacted] UTRECHT

verzendgegevens
datum : 14 augustus 2023
zaaknummer : 2023-033138
bijlagen : 1

behandeld door
team Bestuur & Organisatie
[redacted]
telefoon 14 0223

uw gegevens
brief van : 24 juli 2023
kenmerk :

onderwerp
Reactie op uw verzoek

Geachte [redacted]

Per brief van 24 juli 2023, door ons ontvangen op 26 juli 2023, heeft u namens Bartels Consultancy B.V. een verzoek bij ons ingediend. In uw verzoek geeft u aan dat het gaat om een WOO-annex informatieverzoek. Per brief van 7 augustus 2023 hebben wij de ontvangst van uw verzoek bevestigd. Hierbij ontvangt u onze reactie op uw verzoek.

Inhoud van uw verzoek
U verzoekt, namens Bartels Consultancy B.V., om reeds geproduceerde bescheiden die zien op de hierna volgende situaties:

1. *'Een integrale update van mijn voorgaande verzoek {destijds nog ingevolge artikel 3 lid 1 WOB) gedateerd 20 december 2021. Ik verzoek u de inhoud en strekking van dit epistel als hier herhaald en ingelast te beschouwen.*
2. *Alle grondstaffels van uw gemeente, niet alleen van de grondgebonden woningen maar óók die van niet-woningen alsmede van de bovenwoningen, appartementen, flats en wat dies meer zij (die objecten "staan" immers óók op een specifiek grondoppervlak). Plus graag van alle evenementenlocaties.*
3. *De permanente marktanalyse terzake alle aan- en verkopen van alle geregistreerde objecten. Hoe luiden de gevolgen voor uw mode/matige analyse?*
4. *De specifieke /eegstandsanalyse per winkel-, kantoor- en industriegebied per 1 januari 2023 alsmede uw inschatting voor de komende 10 jaren van het /eegstandsrisico zoals bedoeld bij de totstandkoming van de kapitalisatiefactor?*
5. *Wat is de status van naleving van de AVG binnen uw gemeentelijke organisatie?*
6. *De toepassing van de NEN-2580 methode bij alle binnen uw gemeentegrens gelegen objecten alsmede de tot op heden door u en/of derden geconstateerde afwijkingen. Welke missives hebt u aan belanghebbenden en andere betrokkenen verstuurd sedert 20 december 2021?*
7. *De berekening én uitvoering van de beleidswijziging om voortaan te kijken naar de vierkante i.p.v. de kubieke meters én dienovereenkomstig te gaan aanslaan.*
8. *De stand van zaken van uw openbare (én "besloten" algoritme(n)register(s)? Hoe groot is de impact op burgers en bedrijven en welk "risicoprofiel" hoort hierbij?*
9. *Uw voormalige, huidige én toekomstige beleid t.a.v. de bepaling van de toestandsdatum én hoe kijkt u aan tegen een "ingezetenenheffing"?*
10. *De invloed van {de aanvang van) de Derde Wereldoorlog op de waardeontwikkeling van de door u te belasten objecten én de door u reeds doorgevoerde c.q. nog door te voeren tariefsverhogingen c.q.mutaties.'*

Beantwoording door Cocensus
In onze brief van 7 augustus 2023 hebben wij u laten weten dat wij uw verzoek hebben doorgezonden naar Cocensus. In uw verzoek stelt u namelijk vragen dan wel verzoekt u om documenten over de WOZ en aanverwante onderwerpen. De gemeenschappelijke regeling Cocensus voert voor ons de Wet WOZ uit.

Cocensus zal separaat richting u reageren dan wel heeft reeds separaat richting u gereageerd.

In deze brief zullen wij nader ingaan op onderdelen 5 en 8 van uw brief.

Beantwoording onderdelen 5 en 8 van uw brief
5. Wat is de status van naleving van de AVG binnen uw gemeentelijke organisatie?
Wij hebben een document hierover onder ons. Aangezien de Wet open overheid (hierna: Woo) is bedoeld om informatie neergelegd in documenten openbaar te maken en wij beschikken over een document, beschouwen wij onderdeel 5 van uw verzoek als onderdeel van een Woo-verzoek.

Het document 'Beleidskader Privacy' betreft het actuele privacybeleid van de gemeente Den Helder. Wij besluiten dit document gedeeltelijk openbaar te maken. Openbaarheid is het uitgangspunt van de Woo, maar er zijn in hoofdstuk 5 van de Woo verschillende gronden opgenomen die van dit uitgangspunt afwijken. Wij kunnen op grond van hoofdstuk 5 van de Woo besluiten informatie niet of niet volledig te overleggen. In een aantal gevallen moet eerst een belangenafweging plaatsvinden. Daarom is beoordeeld of het document al dan niet volledig verstrekt dient te worden, waarbij zo nodig de betrokken belangen afgewogen zijn.

Op pagina 2 van het 'Beleidskader Privacy' zijn namen van medewerkers van de gemeente opgenomen. Het betreft medewerkers die niet in de openbaarheid treden vanwege hun functie. Openbaarmaking van deze gegevens zou de bescherming van de persoonlijke levenssfeer onevenredig schaden. De bescherming van de persoonlijke levenssfeer heeft voor ons in redelijkheid een zwaarder gewicht dan openbaarmaking van de namen. De namen van de medewerkers zijn daarom op grond van artikel 5.1, tweede lid, onder sub e, van de Woo weggelakt.

In het document lijkt soms te worden verwezen naar andere vermeende documenten. Voor zover deze vermeende documenten niet gevonden zijn, is opnieuw gezocht naar de documenten. Dit heeft echter niet tot resultaten geleid. Hoewel de Woo niet verplicht tot het geven van een toelichting, doen wij dat hier toch. In het document wordt bijvoorbeeld aangegeven dat het beleid elke twee jaar wordt geëvalueerd. De functionaris gegevensbescherming bekijkt het beleid en als er wijzigingen doorgevoerd moeten worden, worden deze aan het college voorgelegd. Dit heeft zich nog niet voorgedaan sinds 2021. Wij beschikken daarom niet over andere documenten. Aangezien dit laatste een feitelijke beantwoording is van uw vraag, kunt u hieraan verder geen rechten ontlenen.

8. De stand van zaken van uw openbare (én "besloten" algoritme(n)register(s)? Hoe groot is de impact op burgers en bedrijven en welk "risicoprofiel" hoort hierbij?
Op 22 december 2022 hebben wij een besluit genomen op een Woo-verzoek over algoritmes. Dit verzoek is toen afgewezen, aangezien wij niet over documenten beschikten. Wij verwijzen u voor meer informatie over dat verzoek en ons besluit naar de website van de gemeente Den Helder. Het betreffende verzoek en het besluit kunt u raadplegen via de volgende link:
https://www.denhelder.nl/Onderwerpen/Bestuur_en_organisatie/Beleid/Woo_verzoek_bekijken/Woo_verzoek_algoritmes

Wij hebben gezocht naar documenten (opgesteld dan wel ontvangen na 22 december 2022) over algoritme registers. Wij hebben geen documenten aangetroffen. Wij wijzen uw verzoek op dit onderdeel dan ook af, voor zover dit ziet op documenten. Wij werken niet met algoritmes. Aangezien dit laatste een feitelijke beantwoording is van uw vraag, kunt u hieraan geen rechten ontlenen.

Verstrekking op papier
In uw brief geeft u aan dat u de informatie en bescheiden graag per post ontvangt. Het document treft u als bijlage bij deze brief aan.

De bijlage bestaat uit 17 pagina's. Op grond van onze Legesverordening Den Helder 2022 zijn de eerste 6 pagina's gratis. Dit betekent dat er voor 11 pagina's leges dienen te worden geheven. Op grond van het Besluit maximumtarieven open overheid mogen wij maximaal €0,05 leges per pagina op A4-formaat heffen (zwart-wit en enkelzijdig). In dit geval betekent het dat wij €0,55 aan leges mogen heffen. Wegens kostenefficiëntie heffen wij de leges van €0,55 in dit geval niet.

Publicatie op onze website
Documenten die op grond van de Woo worden verstrekt, worden openbaar gemaakt. Een afschrift van de stukken wordt geanonimiseerd op onze website gepubliceerd zodat de informatie voor een ieder inzichtelijk is.

Vragen?
Heeft u naar aanleiding van deze brief nog vragen, dan kunt u contact opnemen met [redacted] via de contactgegevens in het briefhoofd.

Met vriendelijke groet,
namens burgemeester en wethouders van Den Helder,

[redacted]

[redacted] team Bestuur en Organisatie

Bent u het niet eens met het besluit in deze brief?
Wanneer u naar aanleiding van het hierboven vermelde besluit vragen mocht hebben, dan kunt u ons altijd voor een verdere toelichting bellen. Het telefoonnummer staat bovenaan deze brief.

Bezwaar maken gaat als volgt. U kunt als belanghebbende tegen dit besluit binnen zes weken na de bovenaan deze brief vermelde dag waarop het besluit is verzonden met een brief (niet per e-mail) een bezwaarschrift indienen bij het College van Burgemeester en Wethouders van Den Helder, ter attentie van het secretariaat van de Commissie voor de bezwaarschriften, Postbus 36, 1780 AA Den Helder. In het bezwaarschrift moet het volgende staan:

- *uw contactgegevens zoals uw naam en adres (en telefoonnummer);*
- *de dagtekening;*
- *het kenmerk van het besluit en een omschrijving van het besluit waartegen u bezwaar maakt (u kunt een kopie van het besluit (deze brief) meesturen);*
- *de reden(en) waarom u bezwaar indient en wat het besluit volgens u moet zijn;*
- *uw handtekening.*

Het indienen van een bezwaarschrift of tussentijds bellen schort niet de werking van het hierboven vermelde besluit op. Dat betekent dat het besluit blijft gelden in de tijd dat uw bezwaarschrift in behandeling is. Kunt u vanwege de spoedeisendheid van de betrokken belangen een beslissing op uw bezwaarschrift niet afwachten? Dan kunt u gelijktijdig met of na de indiening van uw bezwaarschrift de Voorzieningenrechter van de Rechtbank Noord-Holland, Postbus 1621, 2003 BR Haarlem, vragen een voorlopige voorziening te treffen om de werking van het besluit voor de duur van uw bezwaarschriftprocedure te schorsen. Houdt u er rekening mee dat de rechtbank hiervoor kosten in rekening brengt. Zie ook: www.rechtspraak.nl.

gemeente DEN HELDER

Beleidskader Privacy

Versie 2.0 – Juli 2020

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	Februari 2018	[redacted]	Eerste versie
2.0	Juli 2020	[redacted]	Actualiseren i.v.m digitalisering en integrale toeleiding

Inhoudsopgave

1. Inleiding

1.1. Algemeen

Iedereen heeft recht op privacy. De gemeente Den Helder verzamelt en gebruikt veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van taken. De gemeente Den Helder is verantwoordelijk voor de bescherming van deze persoonsgegevens.

De bescherming van persoonsgegevens speelt een steeds belangrijker rol door de:

- digitalisering van de dienstverlening;
- toename in het verzamelen en delen van gegevens;
- integrale toeleiding binnen het sociale domein;
- datagedreven werken;
- data-analyses
- risico's van cybercrime en identiteitsfraude;
- samenleving die steeds kritischer wordt (de opkomst van social media en de snelheid van nieuws in combinatie met toegenomen transparantie in de zorg en nadruk op "slecht nieuws");
- behoefte en rechten van inwoners om inzicht in de verwerking van zijn of haar persoonsgegevens;
- toename van de hoeveelheid gevoelige informatie van personen (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning, de zorg voor chronisch zieken, ouderen en gehandicapten, leerling zaken.)

Iedereen heeft recht op correcte, veilige en betrouwbare informatieverwerking en moet erop kunnen vertrouwen dat de gemeente Den Helder zorgvuldig met deze gegevens omgaat.

1.2. Reikwijdte en de scope van privacy

Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente Den Helder gegevens verwerkt (of laat verwerken). Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is, wordt aangemerkt als persoonsgegevens..

Het verwerken van persoonsgegevens omvat o.a.: 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, combineren, afschermen, wissen of vernietigen van gegevens.

Verdere definities met betrekking tot de verwerking van persoonsgegevens zijn opgenomen in de Algemene Verordening Gegevensbescherming (AVG)

1.3. Scope

Het privacybeleid is van toepassing op:

- alle gemeentelijke informatieprocessen. Hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen.
- de ambtelijke organisatie, (de leden van) het college van burgemeester en wethouders, dit geldt ook voor de Gemeenteraad en de Griffie, tenzij zij zelf een privacybeleid opstellen;
- Informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente Den Helder (intern en extern) verantwoordelijk is;
- Alle ruimten en devices die door bestuurders en medewerkers intern en extern worden gebruikt waar (op) persoonsgegevens worden verwerkt;
- Alle geldende normen en regels op het gebied van privacy.

1.4. Opbouw privacybeleid

Het privacybeleid geldt als algemeen beleid. Hierin zijn de kaders met de risico's en maatregelen beschreven, om te voldoen aan wet- en regelgeving. Voor bepaalde domeinen kan het nodig zijn om aanvullend specifiek privacybeleid vast te stellen. De organisatie van verantwoordelijkheden, functies en rollen waarmee de gegevensbescherming bij de gemeente Den Helder wordt geborgd, is opgenomen in hoofdstuk 3 en het Organisatiemodel informatieveiligheid (Bijlage 1). Volledigheidshalve wordt hier vermeld dat onder informatieveiligheid wordt verstaan de informatiebeveiliging en privacybescherming.

1.5 Wetten en regels

De juridische grondslag voor privacy is terug te vinden in wet- en regelgeving. De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:

- Europees Verdrag voor de Rechten van de Mensen (art. 8)
- Internationaal Verdrag burgerrechten en politieke rechten (art. 17)
- Grondwet (art. 10)
- Handvest van de grondrechten van de Europese Unie (art. 8)
- Internationaal Kinderrechtenverdrag (IVRK) (art. 16)

De belangrijkste wet die invulling geeft aan de bescherming van persoonsgegevens is de Algemene Verordening Persoonsgegevens (AVG). De AVG is op 25 mei 2018 in werking getreden en is een Europese verordening die rechtstreekse werking heeft in alle lidstaten. Dit betekent dat decentrale overheden en betrokkenen rechtstreeks aan de regels gebonden zijn en zich ook direct op de bepalingen kunnen beroepen. De AVG biedt de lidstaten de ruimte om bepaalde keuzes te maken. In Nederland zijn deze uitgewerkt in de Uitvoeringswet AVG (UAVG).

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals:

- Wet maatschappelijke ondersteuning (WMO)
- Jeugdwet
- Wet Basisregistratie Personen (Brp)
- Participatiewet
- Wet algemene bepalingen Burgerservicenummer
- Archiefwet

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. In het Informatiebeveiligingsplan zijn maatregelen opgenomen om de gegevens te beschermen. Deze maatregelen ('controls') worden op basis van de Baseline Informatiebeveiliging Overheid (BIO) geïmplementeerd en geborgd.

Het privacybeleid omvat de gehele 'data life cycle'; van het genereren of verzamelen van gegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan. De AVG geldt zowel voor de papieren als de digitale informatieverwerking.

2. Privacybeleid

2.1. Doelstelling

Het doel van dit privacybeleid is het beschrijven van beleidkaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen, waarvan de gemeente Den Helder persoonsgegevens verwerkt.

Het privacybeleid draagt bij aan:

- het beschermen van de privacy van personen van wie de gemeente Den Helder gegevens verwerkt of laat verwerken;
- maatschappelijk vertrouwen en draagvlak;
- beheersen van afbreuk- en aansprakelijkheidsrisico's;
- het met vertrouwen verantwoording af kunnen leggen aan de gemeenteraad en waar nodig de Autoriteit Persoonsgegevens (AP) of de rechter;
- het in kunnen spelen op wettelijke en technologische ontwikkelingen.
- het voldoen aan geldende wet- en regelgeving

2.2. Uitgangspunten

Iedereen die werkzaam is binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens, gegevensbescherming en het waarborgen van de privacyrechten van personen. Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken. (art. 5 AVG e.v. ' beginselen betreffende verwerking van persoonsgegevens')

De uitgangspunten hierbij zijn:

- betrokkene heeft toestemming gegeven voor de verwerking of de verwerking is noodzakelijk:
    - op basis van de wet of een overeenkomst;
    - ter bescherming van vitale belangen;
    - voor een taak in het algemeen belang of voor de uitoefening van een publieke taak;

  Hierbij moet worden opgemerkt dat er niet snel sprake zal zijn van toestemming omdat er tussen burger en gemeente Den Helder meestal een afhankelijkheidsrelatie bestaat. Toestemming moet door de burger geheel vrij gegeven kunnen worden.
- betrokkene is vooraf in eenvoudige en duidelijke taal geïnformeerd dat zijn/haar persoonsgegevens worden verwerkt en voor welk doel;
- alleen persoonsgegevens die noodzakelijk zijn voor het doel worden verwerkt;
- persoonsgegevens zijn correct en actueel;
- de gemeente hanteert de wettelijke bewaartermijn voor persoonsgegevens. Voor die verwerkingen waarvoor er geen wettelijke bewaartermijn is bepaald bewaart de gemeente de persoonsgegevens niet langer dan strikt noodzakelijk en worden de persoonsgegevens geanonimiseerd of verwijderd;
- verzoeken van betrokkene op het gebied van rechten zoals 'het recht om vergeten te worden' , 'recht op inzage' , 'recht op rectificatie' worden opgevolgd overeenkomstig de wettelijke voorwaarden (o.a. toereikende identificatie);
- persoonsgegevens zijn beveiligd door middel van technische en organisatorische maatregelen.
- Zorg voor privacy is evenals beveiliging een kwaliteitsaspect en maakt deel uit van de integrale verantwoordelijkheid van de proces- of de systeemeigenaar;
  Voor bedrijfsprocessen en verwerkingen waaraan privacyrisico's zijn verbonden wordt een Data Protection Impact Assessment (DPIA) uitgevoerd. Aan de hand van deze DPIA wordt een inschatting

gemaakt van de gevolgen met betrekking tot de privacy van betrokkenen, de impact van de verwerking, de risico's en / of er mogelijkheden bestaan die minder gevolgen hebben voor de privacy. De gemeente gebruikt voor het uitvoeren van de DPIA een gestandaardiseerd DPIA-model.

De algemeen directeur van de gemeente Den Helder is verantwoordelijk voor het naleven van deze uitgangspunten en moet dit kunnen aantonen.

2.3. Risico's

De gemeente Den Helder is verwerkingsverantwoordelijke. Dat betekent o.a. dat bij schending van de gegevensbescherming van persoonsgegevens is de gemeente Den Helder aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van schadevergoeding. Elke benadeelde heeft hier recht op;
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding AVG kan de Autoriteit Persoonsgegevens, de landelijk toezichthouder, een boete opleggen tot maximaal 20 miljoen.
- De burger kan geschaad worden in zijn eigen persoonlijke levenssfeer

Binnen bepaalde domeinen wordt er gewerkt met zeer gevoelige bijzondere persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn het sociaal domein, leerlingzaken, burgerzaken en het veiligheidsdomein. Aan de verwerking van deze persoonsgegevens zijn aanvullende voorwaarden gesteld, (art. 9, art. 10 AVG 'verwerking van bijzondere persoonsgegevens'). De risico's bij de verwerking van bijzondere persoonsgegevens zijn hoger.

De risico's van schending van de privacy voor personen variëren van ongemak, identiteitsfraude, stigmatisering, uitsluiting of gevaren voor de gezondheid en de persoonlijke veiligheid.

Om de risico's te beperken moeten maatregelen worden getroffen. Deze maatregelen zijn beschreven in hoofdstuk 4. Leidend daarbij is dat privacy-eisen zoveel mogelijk worden geïntegreerd in regulier en/of al bestaand (domein) beleid en vertaald naar processtappen die worden geïntegreerd in het reguliere werkproces, bijv. in het Inkoop- en aanbestedingsbeleid en personeelsbeleid (Privacy bij Default en Privacy by Design)..

2.4. Evaluatie

Het privacybeleid wordt uiterlijk elke twee jaar geëvalueerd. Indien daartoe aanleiding bestaat, wordt het privacybeleid (eerder) bijgesteld.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot gegevensbescherming op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Het inrichten van de organisatie van de gegevensbescherming heeft als doel het benoemen van het eigenaarschap van de bedrijfsprocessen, met bijbehorende (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden. Dit heeft als resultaat dat er een verankering ontstaat in de gemeentelijke organisatie van de verantwoordelijkheden, taakomschrijvingen, coördinatie en rapportagemechanismen met betrekking tot gegevensbescherming.

3.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamcoach. De directie zorgt dat de teamcoaches zich verantwoorden over de gegevensbescherming en de persoonsgegevens die onder hen berusten. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin gegevensbescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie draagt zorg voor het uitwerken van tactische gegevensbeschermingsbeleidsonderwerpen en laat zich hierin bijstaan door de FG van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen.

3.1.1 Verantwoordelijkheden gemeentelijke (informatie)systemen

Gemeentelijke (informatie)systemen worden technisch onder de verantwoordelijkheid van team I&T gefaciliteerd en onderhouden. Deze systemen, die door meer dan één organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd.

Voor ieder gemeentelijk (informatie)systeem is de directie bevoegd het beheer hiervan te beleggen bij een organisatieonderdeel, een procesverantwoordelijke en/of een systeemeigenaar die daarmee organisatorisch verantwoordelijk wordt voor de gehele gegevensverzameling en/of het (informatie)systeem.

De organisatorisch verantwoordelijke voor een gemeentelijk (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor autorisatie en instructie voor alle betrokken partijen duidelijk zijn.

Het organisatorisch verantwoordelijke organisatieonderdeel voor het gemeentelijke (informatie)systeem stelt minimaal de volgende richtlijnen op voor de gebruikers van het (informatie)systeem:

- De voorwaarden voor het toegestane gebruik van het gemeentelijke (informatie)systeem;
- De verantwoordelijkheden voor de persoonsgegevens in het gemeentelijke (informatie)systeem;
- Een instructie die de gebruikende organieke eenheid verplichten voorzieningen te treffen voor een passend niveau van gegevensbescherming;
- Procedure(s) betreffende de autorisatie van gebruikers van het (informatie)systeem;
- Procedure(s) betreffende het toezicht en controle op de naleving van beveiligingsrichtlijnen;
- Het recht op inzage in de resultaten van inspecties, audits en zelf assessments bij de gebruikende organieke eenheid.

3.2 De eerste lijn: uitvoering & teamcoaches

3.2.1 Alle medewerkers

Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van alle activiteiten die behoren tot hun eigen rol, functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met persoonsgegevens. Zij zijn zich bewust van de eisen ten aanzien van de rechtmatigheid, de proportionaliteit en de subsidiariteit van de gegevensverwerking waarbij zij zijn betrokken.

3.2.2 Teamcoaches

Informatiebeveiliging en gegevensbescherming valt onder de verantwoordelijkheden van de teamcoaches binnen hun eigen afdeling. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamcoaches rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging en gegevensbescherming te bespreken in het bedrijfsvoeringsoverleg.

Taken van de teamcoaches in het kader van informatiebeveiliging en gegevensbescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van gegevensbescherming, bedrijfscontinuïteit en op naleving van wetten, regels en richtlijnen.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan persoonsgegevens zijn blootgesteld.
- Bespreking van datalekken en de consequenties die dit moet hebben voor beleid en maatregelen.
- Het uitvoeren van een (verplicht) Data Protection Impact Assessment.
- Opdracht geven tot en het toezien op het uitvoeren van periodieke gegevensbeschermingsassessments en –audits.
- Het rapporteren over compliance ten opzichte van het privacybeleid en de daarmee verband houdende wet- en regelgeving in de P&C rapportages.

3.3 De tweede lijn: CISO, functionaris gegevensbescherming, controler informatieveiligheid en beveiligings- en privacybeheerders(s)

3.3.1 De Chief Information Security Officer (CISO)

Deze rol is in de gemeente verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het aansturen van de uitvoering van het beleid en het adviseren bij projecten. De CISO heeft in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de gemeentesecretaris en het bestuur;
- Coördineert het opstellen en evalueren van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Stelt een agenda op voor overleg en rapportage met betrekking tot informatieveiligheid met de gemeentesecretaris en/of het college;
- Ondersteunt de gemeentesecretaris met kennis over informatieveiligheid, zodat deze zijn of haar verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kan invullen;
- Is een aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden en ontwikkelingen die van invloed zijn op het informatieveiligheidsbeleid;
- Geeft gevraagd én ongevraagd advies over informatieveiligheid aan de gehele organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en evalueert de incidenten;
- Onderhoudt contact met de Informatiebeveiligingsdienst;

- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages door middel van een in control statement.

3.3.2 De controller informatieveiligheid

Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid. De controller informatieveiligheid, in dit geval de concerncontroller, is in ieder geval verantwoordelijk voor:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van het informatieveiligheid;
- De controle op de voortgang van het uitvoeren van activiteiten uit het informatieveiligheidsplan;
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- De toetsing van het evaluatieproces van beveiligingsincidenten;
- De rapportage van bevindingen aan het college.

De rol van controller informatieveiligheid heeft op de deelgebieden reisdocumenten en rijbewijzen een voorgeschreven benaming:

- Beveiligingsfunctionaris reisdocumenten: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- Beveiligingsfunctionaris rijbewijzen: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

3.3.3 De beveiligingsbeheerder(s)

Deze rollen zijn verantwoordelijk voor het dagelijkse beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid binnen een specifiek werkveld.

De audit- en/of inspectie plichtige werkvelden waarvoor een beveiligingsbeheerder is aangewezen zijn:

- Suwinet (Werk en Inkomen)[1]
- DigiD (Dienstverlening)
- BRP (Basisregistratie personen)
- Waardedocumenten (Reisdocumenten[2], Nederlandse identiteitskaarten en rijbewijzen[3])
- BAG (Basisregistratie adressen)
- BGT (Basisregistratie grootschalige topografie)
- BRO (Basisregistratie ondergrond)

Naast beveiligingsbeheerders voor audit- en/of inspectie plichtige werkvelden worden ook beveiligingsbeheerders aangewezen voor werkvelden waarvoor een verplicht zelfassessment van toepassing is of die onderdeel zijn van de jaarlijkse accountantscontrole:

- Facilitair
- Inkoop
- Personeelszaken
- Financiën
- I.T.

---

[1] *Formeel de beveiligingsbeheerder Suwinet: verantwoordelijk voor het beheer van beveiligingsprocedures en maatregelen in het kader van Suwinet. De beveiligingsbeheerder Suwinet verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het college en vraagt daarnaast meerdere keren per jaar een rapportage op bij de toezichthouder BKWI over het gebruik van Suwinet*

[2] Formeel de Autorisatiebevoegde Reisdocumenten/Aanvraagstations: Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).

[3] Formeel de Autorisatiebevoegde Rijbewijzen: Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

De beveiligingsbeheerder is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van het informatieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelf assessment-onderdelen gelden.

3.3.4 De functionaris gegevensbescherming (FG)

De FG is de interne toezichthouder voor de verwerking van persoonsgegevens en heeft in ieder geval de volgende taken (AVG Art 39), vertaald naar de situatie bij de gemeente:

- Informeren en adviseren van de raad, het college, de directie en de medewerkers over verplichtingen en beperkingen met betrekking tot de bescherming van persoonsgegevens;
- Toezien op naleving van de AVG en andere aanpalende wetten met betrekking tot gegevensbescherming alsmede het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de bewerker;
- Desgevraagd adviseren omtrent het Privacy Data Impact Assessment (PDIA), en toezien op de uitvoering daarvan;
- Toezicht houden op de registratie en afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezicht houden op het melden van een datalek bij de Autoriteit Persoonsgegevens (AP) en bij de betrokkenen;
- Samenwerken met en als contactpunt optreden voor de AP;
- Rekening houden met risico's naar de aard, omvang en context van verwerkingen van persoonsgegevens;
- Rapporteren aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen het college van burgemeester en wethouders of de burgemeester en in sommige gevallen de gemeenteraad.

De FG heeft een toezichthoudende taak, vergelijkbaar met de taak van de controller informatieveiligheid. De uitvoering en implementatie van het beleid is belegd bij de procesverantwoordelijken of systeemeigenaren.

3.3.5 De privacy beheerders

Deze rol is gericht op de directe uitvoering en naleving van de AVG. De privacy beheerder adviseert over privacybescherming en over activiteiten ter bescherming van persoonsgegevens binnen het eigen werkveld. De privacy beheerder heeft in ieder geval de volgende verantwoordelijkheden:

- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van privacywetgeving en adviseert de procesverantwoordelijke of systeemeigenaar bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een DPIA;
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens;
- Uitleggen van de privacy voorschriften in de AVG, en in de sectorale wetgeving;
- Coördineren van privacy werkzaamheden, informeren en het verzorgen van meldingen bij de FG;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Rapporteren aan de procesverantwoordelijke of systeemeigenaar;
- Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
- Beheer en onderhoud van de standaarddocumenten voor bewerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

3.4 Werkgroep informatieveiligheid

De werkgroep informatiebeveiliging bestaat uit de team coach I&T, de FG, de CISO, de controler, een medewerker systeembeheer. Op ad hoc basis wordt het team aangevuld met één of meer taakspecialisten, bijvoorbeeld een materiedeskundige of adviseur communicatie en juridische zaken. De werkgroep informatiebeveiliging komt maandelijks bij elkaar of vaker wanneer daartoe aanleiding is, bijvoorbeeld bij grootschalige datalekken of incidenten. In dat geval kunnen zowel de FG als CISO het team bij elkaar roepen. De reguliere vergaderingen worden in onderling overleg georganiseerd door de FG en CISO.

In bijlage 1 wordt de organisatie geprojecteerd op de reguliere organisatiestructuur van de gemeente Den Helder. Zowel de FG als de CISO hebben ten aanzien van hun toezichthoudende taken een onafhankelijke rol. Dit geldt ook voor het melden van datalekken en beveiligingsincidenten. Beide functionarissen kunnen rechtstreeks aan de directeur rapporteren en (on)gevraagd adviseren. In het schema zijn zij daarom naast de directie gepositioneerd. De directie is niet gehouden adviezen over te nemen. Over de niet-toezichthoudende taken rapporteren de FG en de CISO aan hun leidinggevende.

3.5 Kernteam informatieveiligheidscrisis

Er dient een kernteam informatieveiligheidscrisis ingesteld te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. De richtlijnen voor de werkwijze tijdens grote incidenten of calamiteiten worden in een handboek uitgewerkt. Het kernteam informatieveiligheidscrisis bestaat uit:

- De gemeentesecretaris
- De CISO
- De FG
- De (betrokken) beveiligingsbeheerder I.T.
- De betrokken procesverantwoordelijken of systeemeigenaren
- De betrokken beveiligingsbeheerder(s)
- Relevante experts of andere deskundigen
- Een medewerker crisiscommunicatie

3.6 Controle en verantwoording

Dit Privacy beleid is een verantwoordelijkheid van het bestuur van de gemeente Den Helder. De bestuurders en directeuren van de gemeente Den Helder richting en sturing geven aan het onderwerp informatiebeveiliging & gegevensbescherming door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging & privacy aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

4. Maatregelen

4.1. Doelstelling

Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen van het privacy beleid worden gehaald en de risico's worden beperkt.

4.2. Maatregelen

Onderstaande maatregelen zijn getroffen om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, volgens geldende wet- en regelgeving.

4.2.1 Transparantie

Betrokkene(n) ontvangen voorafgaande aan de registratie van hun persoonsgegevens duidelijke informatie (via de website en voorafgaande aan de dienstverlening) over het doel van de verwerking van hun persoonsgegevens.

4.2.2 Naleving van het informatiebeveiligingsbeleid

Op basis van het informatiebeveiligingsbeleid zijn maatregelen getroffen om de bescherming van persoonsgegevens te waarborgen. Informatiebeveiliging is een eerste voorwaarde voor gegevensbescherming in het kader van privacy, zowel technisch als organisatorisch.

4.2.3 Bewustwording en communicatie

Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat alle medewerkers van de gemeente Den Helder, die werken met persoonsgegevens, zich bewust zijn van het belang om zorgvuldig met persoonsgegevens om te gaan. De privacybeheerders binnen de individuele teams vervullen een belangrijke rol om direct binnen de eigen werkprocessen en in werkoverleg, als adviseur, gegevensbescherming onder de aandacht te brengen en knelpunten te signaleren. Doorlopend wordt er in de gemeente aandacht geschonken aan de bewustwording waarvoor er gebruik wordt gemaakt van een communicatieprogramma.

4.2.4 Register van verwerkingsactiviteiten

De gemeente is op grond van artikel 30 AVG verplicht een verwerkingsregister op te stellen en te beheren. In dit register dienen alle verwerkingsactiviteiten van persoonsgegevens te zijn opgenomen en op aanvraag van de toezichthouder te verstrekken. Per verwerking dient de gemeente te registreren welk bestuursorgaan voor de verwerking verantwoordelijk is, voor welke doeleinden de verwerking plaatsvindt, met welke grondslag de activiteiten worden uitgevoerd, de categorieën van betrokkene(n) en persoonsgegevens, welke derden de persoonsgegevens ontvangen, de gehanteerde bewaartermijn en de noodzakelijke beveiligingsmaatregelen die de gemeente heeft getroffen om de veiligheid van deze persoonsgegevens waarborgen.

4.2.5 Dataclassificatie

De gemeente is op grond van artikel 24 AVG verplicht persoonsgegevens te beschermen. De gemeente houdt hierbij rekening met de aard, de omvang, de context en het doel van de verwerking, als ook de waarschijnlijkheid en de ernst van de uiteenlopende risico's voor de rechten en de vrijheden van betrokkene(n). Op basis van de gevoeligheid van de persoonsgegevens en de risico's voor de rechten en vrijheden van betrokkene(n) classificeert de gemeente de persoonsgegevens en stemt, op basis van deze

classificatie, de technische en organisatorische beveiligingsmaatregelen af. De dataclassificatie van persoonsgegevens is per proces opgenomen in het verwerkingsregister.

4.2.6 Data Protection Impact Assessmant (DPIA)

Voor (nieuwe en veranderende) processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, kan het verplicht zijn voor de proces- en of systeemverantwoordelijke om een DPIA uit te voeren. Een DPIA is een instrument om voorafgaande aan de verwerking de privacy risico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Per DPIA consulteert de proces- of systeemverantwoordelijke de FG voor een aanvullend advies.

De toezichthouder stelt dat de gemeente verplicht is een DPIA uit te voeren als de gemeente:

- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt ;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht)

Verder stelt de toezichthouder een DPIA verplicht bij activiteiten gerelateerd aan heimelijk onderzoek, gebruik van zwarte lijst, fraudebestrijding, creditscores, financiële situaties, verwerking genetische persoonsgegevens, gezondheidsgegevens, communicatiegegevens, cameratoezicht, flexibel cameratoezicht, controle werknemers, locatiegegevens, samenwerkingsverbanden, communicatiegegevens, profilering, internet of things, monitoring of beïnvloeding van gedrag, biometrische persoonsgegevens.

Als uit een DPIA blijkt dat er na het nemen van alle mogelijk maatregelen nog steeds sprake is van risicovolle verwerkingen dan dient de toezichthouder hiervan in kennis te worden gesteld. De wijze waarop een DPIA wordt uitgevoerd en wat de vervolgacties op basis van de uitkomsten moeten zijn, is nader uitgewerkt in de 'Procedure DPIA" van de gemeente Den Helder.

4.2.7 Privacy by design of privacy by default

Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- gegevensminimalisatie, anonimisering en pseudonimisering;
- de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'. Bij het toepassen van Privacy by design en – default wordt de FG geconsulteerd.

4.2.8 Verwerkersovereenkomst of samenwerkingsconvenant

Een verwerkingsovereenkomst of samenwerkingsconvenant is wettelijk verplicht als het verwerken van persoonsgegevens door een externe partij, in de rol van Verwerker of zelfstandig verantwoordelijke, plaatsvindt.

In een verwerkersovereenkomst of samenwerkingsconvenant worden afspraken vastgelegd over:

- de doeleinden waarvoor de persoonsgegevens aan een externe partij worden verstrekt en of gedeeld;
- het juridische kader dat op deze gegevensverstrekking van toepassing is;

- de verantwoordelijkheid van de gemeente en de externe partij en hoe de verwerker met de persoonsgegevens moet omgaan;
- de beveiligingsmaatregelen die moeten worden genomen;
- de manier waarop de persoonsgegevens veilig worden gedeeld
- de manier waarop de verwerkingsverantwoordelijke toezicht uitoefent;
- de geheimhoudingsplicht;
- de mogelijke inschakeling van derden en onderaannemers;
- de locatie en of de bewaartermijn van de data;
- de rolverdeling bij de afhandeling van datalekken en de uitoefening van rechten van betrokkenen;
- de aansprakelijkheid in geval van schade door het niet naleven van regelgeving.

De gemeente Den Helder hanteert standaard de model Verwerkersovereenkomst van de Informatie Beveiligingsdienst (IBD). Dit model bevat de gemeentelijke standaard voor een verwerkersovereenkomst en betreft een aanvulling op een hoofdovereenkomst om op grond van de AVG (artikel 28.3 en 28.9) nadere afspraken te maken en vast te leggen over de omgang met persoonsgegevens. Het model van de Verwerkersovereenkomst is in het voorjaar van 2019 vastgesteld door het VNG bestuur en de verplichting tot gebruik is bekrachtigd in de ledenvergadering van de VNG.

4.2.9 Meldplicht Datalekken

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens / artikel 33 AVG). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. De meldplicht datalekken regelt wanneer een datalek moet worden gemeld bij de Autoriteit Persoonsgegevens. Een datalek moet aan de betrokkene(n) worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor zijn of haar privéleven. Voor de werkwijze bij een datalek en de rolverdeling wordt verwezen naar de ‘Procedure meldplicht datalekken’.

4.2.10 Audits

Vragen, klachten en het incident management zijn vormen van steekproefsgewijze toetsing van de privacybeleidskader. Om niet voor verrassingen te worden geplaatst, is het belangrijk dat proceseigenaren ook zelf periodiek (laten) controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand van privacy audits op de gehanteerde ijkpunten.

Op basis van de uitkomsten van een DPIA wordt bepaald naar welke zwaarte de audits moeten plaatsvinden. Hierbij worden de volgende typen onderscheiden:

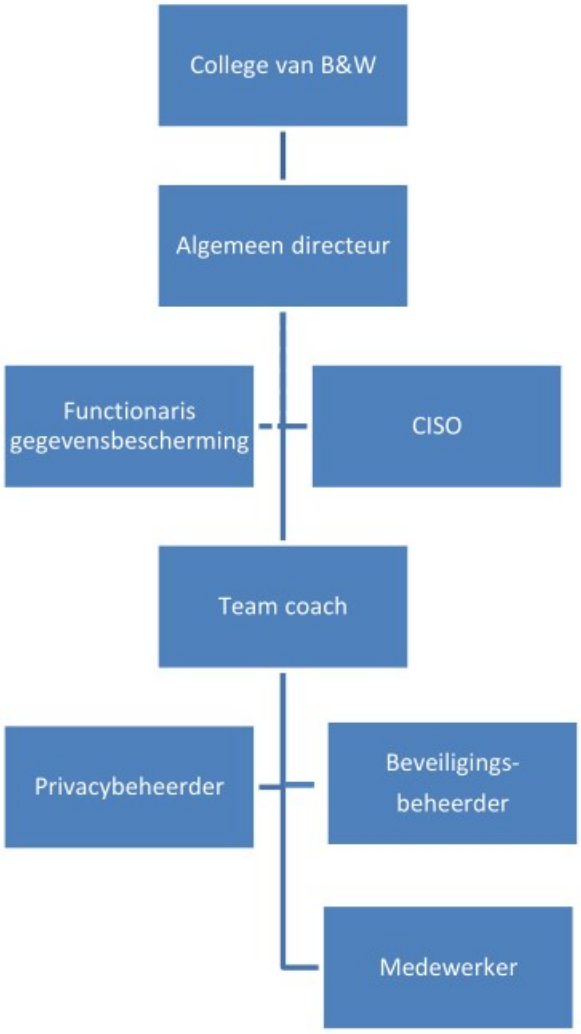
- Quick scan is een beknopte toets onder de verantwoordelijkheid van de proceseigenaar
- Zelfevaluatie is een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar
- Externe audit is een audit die de proceseigenaar organiseert in samenwerking met de FG en waarbij eventueel een professionele auditor wordt betrokken.

Wanneer een audit plaatsvindt, wordt de FG vanaf het begin betrokken in het audittraject en is hij medeontvanger van het auditrapport.

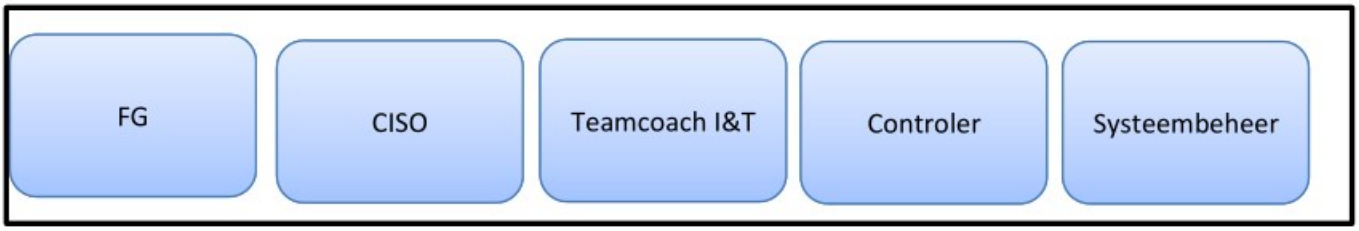
5. Bekendmaking en inwerkingtreding

Het privacybeleid treedt in werking op de dag volgende op de dag van bekendmaking.

Bijlage 1 Organisatiemodel Informatieveiligheid



Werkgroep Informatiebeveiliging / Responseteam Datalekken



Toelichting grondslagen

In dit document kunt u secties terugvinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

Legenda verwijzing	Artikel verwijzing	Uitzonderingsgrond
		Artikel 5.1 lid 1 Woo – Absolute uitzonderingsgronden **De openbaarmaking van deze informatie:**
A	art. 5.1 lid 1 a	Kan de eenheid van de Kroon in gevaar brengen
B	art. 5.1 lid 1 b	Kan de veiligheid van de Staat schaden
C	art. 5.1 lid 1 c	Betreft bedrijfs- en fabricagegegevens die vertrouwelijk aan de overheid zijn meegedeeld
D	art. 5.1 lid 1 d	Betreft persoonsgegevens als bedoeld in paragraaf 3.1 (bijzondere persoonsgegevens) of paragraaf 3.2 (persoonsgegevens van strafrechtelijke aard) van de Uitvoeringswet Algemene verordening gegevensbescherming, waarvoor geen toestemming is gegeven of door de betrokkene kennelijk zelf openbaar zijn gemaakt
E	art. 5.1 lid 1 e	Het betreft nummers die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt
		Artikel 5.1 lid 2 Woo – Relatieve uitzonderingsgronden **Het belang van de openbaarmaking van deze informatie weegt niet op tegen:**
F	art. 5.1 lid 2 a	Het belang van de betrekkingen van Nederland met andere staten en met internationale organisaties
G	art. 5.1 lid 2 b	De economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen
H	art. 5.1 lid 2 c	Het belang van de opsporing en vervolging van strafbare feiten
I	art. 5.1 lid 2 d	Het belang van de inspectie, controle en toezicht door bestuursorganen
J	art. 5.1 lid 2 e	Het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen
K	art. 5.1 lid 2 f	Het belang van de bescherming van andere dan in art. 5.1 lid 1 sub c genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens
L	art. 5.1 lid 2 g	Het belang van de bescherming van het milieu waar deze informatie betrekking op heeft
M	art. 5.1 lid 2 h	Het belang van de beveiliging van personen en bedrijven en het voorkomen van sabotage
N	art. 5.1 lid 2 i	Het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen
O	art. 5.1 lid 4	Het belang dat de geadresseerde erbij heeft om als eerste kennis te kunnen nemen van de informatie (tijdelijke beperking)
P	art. 5.1 lid 5	De onevenredige benadeling welke, in uitzonderlijke gevallen, wordt toegebracht aan een ander belang dan genoemd in art. 5.1 de leden 1 en 2, bij andere informatie dan milieu-informatie.
Q	art. 5.1 lid 6	Het belang genoemd in artikel 5.1 lid 1 c, het hier milieu-informatie betreft waardoor, bij openbaarmaking, ernstige schade wordt toegebracht aan het genoemde belang in artikel 5.1 lid 1c
		Artikel 5.2 lid 1 Woo – Persoonlijke beleidsopvattingen **De informatie uit documenten betreft:**
R	art. 5.2 lid 1	Persoonlijke beleidsopvattingen. Onder persoonlijke beleidsopvattingen worden verstaan ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van intern beraad, niet zijnde feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter
S	Art. 5.2 lid 2	Tot personen te herleiden gegevens, met betrekking tot door het bestuursorgaan, met het oog op een goede en democratische bestuursvoering, verstrekte informatie die kwalificeert als persoonlijke beleidsopvattingen