Gemeente Delft

GEMEENTEBLAD

Officiële uitgave van de gemeente Delft

Nr. 57286

20 maart

2018

Beleidsregel van het college van burgemeester en wethouders van de gemeente Delft houdende regels omtrent het Privacy beleid

INHOUDSOPGAVE

Bijlage 2: Eisen verwerkersovereenkomst, artikel 28 AVG
Bijlage 3: Stroomschema rechtmatige verwerking

1 AANLEIDING

Vanaf 25 mei 2018 zal de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing zijn. Deze verordening, vastgesteld door het Europees Parlement en de Raad van Ministers van de Europese Unie op 27 april 2016, is de opvolger van de - nationale - Wet bescherming persoonsgegevens (Wbp). De AVG heeft rechtstreekse werking in alle lidstaten van de Europese Unie. Er is vanaf 25 mei 2018 dus sprake van één gezamenlijk privacy-regime binnen de Europese Unie [1].

2 WAAROM BELEID ?

Omdat de gemeente veel, complexe, bijzondere en gevoelige persoonsgegevens verwerkt, is de gemeente verplicht [2] om een gegevensbeschermingsbeleid te hebben. Daarnaast dient de gemeente - door het hanteren van gegevensbeschermingsbeleid (kortweg: 'privacy-beleid') te voldoen aan de verplichting uit de AVG om aan te tonen dat aan de zogenaamde verantwoordingsplicht [3] wordt voldaan. Verder kan dit privacy-beleid er aan bijdragen dat besluiten op grond van de AVG binnen gemeente op een eenduidige manier worden genomen, en dat ook de procedures eenduidig zijn.

Het college wil daarnaast transparantie naar de burger toe betrachten en deze informeren. De burger moet er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. Het is van belang dat de burger op eenvoudige wijze toegang krijgt tot het gevoerde privacy-beleid, aangezien van deze zelfde burger erg veel persoonsgegevens worden verwerkt. Deze nota wil daar in voorzien.

De AVG verplicht de gemeente om steeds te kijken of het beleid nog voldoet en of het aangepast moet worden. Technologische en maatschappelijke ontwikkelingen volgen elkaar snel op. Dit kan reden zijn om het beleid aan te passen. Omdat daarnaast nog niet geheel duidelijk is hoe de toezichthouder, de Autoriteit Persoonsgegevens (zie hoofdstuk 6) zijn taak zal opvatten, is het daarom noodzakelijk om het privacy-beleid periodiek - in ieder geval per twee jaar - te evalueren. Er is immers sprake van nieuwe wetgeving, die volop in beweging is, en waar door de rechtspraak en de toezichthouder nog nader invulling aan zal worden gegeven.

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacy-beleid is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. De gemeente heeft BV's waarvan ze voor 100% eigenaar is , Ontwikkelingsbedrijf Spoorzone (OBS) Integraal Parkeerbedrijf Delft (IPD), Delft Support BV, en de BV's van Werkse! . Of een BV verplicht is zelf privacybeleid te maken hangt van diverse factoren af. Hierop wordt ingegaan in hoofdstuk 7.

3 OPZET VAN HET BELEID

In deze nota wordt eerst op de basisbeginselen van de AVG ingegaan, daarna worden deze verder uitgewerkt en wordt indien mogelijk aangegeven hoe de gemeente het in praktijk brengt.
Er is voor gekozen om sommige zaken verder uit te werken in afzonderlijke protocollen, omdat de omvang van deze nota anders te groot zou worden (bijvoorbeeld bij het onderwerp 'rechten van betrokkenen' in hoofdstuk 9). Op het moment van vaststellen van deze nota zijn nog niet alle gewenste protocollen gereed. Deze zullen op een later moment worden toegevoegd. Deze beleidsnota is derhalve te beschouwen als een levend document, dat regelmatig aangevuld en/of gewijzigd kan worden.

4 KERNBEGRIPPEN BINNEN DE AVG

Voor een goed begrip van de AVG is het noodzakelijk eerst enkele kernbegrippen te duiden:

1) Sommige zaken moeten door de lidstaten zelf geregeld worden, zoals bijvoorbeeld de aanwijzing- en bevoegdheden van de nationale toezichthouders. In Nederland is daartoe het wetsontwerp 'Uitvoeringswet AVG' (UAVG) ingediend (TK 2017/2018, 34821, nr 2).

2) Zie artikel 24 lid 1 en lid 2 AVG

3) Op grond van artikel 5 lid 1 AVG (zie paragraaf 4.2)

1. Toepasselijkheid AVG
2. Verantwoordingsplicht en invulling verantwoordingsplicht
3. Persoonsgegevens
4. Verwerking (van persoonsgegevens)
5. Verwerkingsgrondslagen
6. Doelbinding
7. Verwerkingsverantwoordelijke en verwerker
8. Betrokkene
9. Bijzondere en gevoelige persoonsgegevens

4.1 Toepasselijkheid AVG

De AVG is van toepassing op 'de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen' (zie bijlage 1 voor een stroomschema).

Dit betekent kort gezegd dat wanneer de gemeente persoonsgegevens per computer verwerkt, de AVG van toepassing is. Maar de AVG is ook van toepassing in situaties waar handmatig wordt verwerkt, en er dus géén geautomatiseerde verwerking aan de orde is. Als er bijvoorbeeld sprake is van geschreven gespreksnotities van ambtenaren met inwoners van Delft, verzameld in mappen, dan is de AVG ook van toepassing. [4]

De AVG is niet alleen van toepassing op de relatie tussen gemeente als overheid en zijn burgers, bedrijven en instellingen, maar ook op de verhouding die de gemeente als werkgever heeft met zijn werknemers.

4.2 Verantwoordingsplicht

Feitelijk is de verantwoordingsplicht ('accountability') het centrale begrip binnen de AVG. Het is opgenomen in artikel 5 AVG. Het eerste lid van artikel 5 somt de zes basisbeginselen van de AVG op De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (in de meeste gevallen het college van burgemeester en wethouders) verantwoordelijk is voor het naleven van deze beginselen, en deze kan aantonen. [5]

De principes zijn:

1. Rechtmatigheid, behoorlijkheid, transparantie

De gemeente mag niet in strijd met de wet handelen, moet behoorlijk handelen en voor betrokkenen duidelijk zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkene moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen (zie hoofdstuk 9).

2. Doelbinding

Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld , en vervolgens alleen verder verwerkt worden wanneer er sprake is van een verenigbaar doel (zie paragraaf 4.7)

3. Minimale gegevensverwerking (' dataminimalisatie')

Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is voor het doel. Verder moet steeds worden gekeken of het doel niet op een minder ingrijpende wijze kan worden bereikt (dit zijn de principes van proportionaliteit en subsidiariteit).

4. Juistheid

4) Zie artikel 2 lid 1 samen met artikel 4 lid 6 AVG. Tevens 'De Algemene Verordening Gegevensbescherming, ed.2017, Engelfriet e.a , p.25.

5) Artikel 5 lid 2 AVG

Het is van belang dat voortdurend moet worden nagegaan of de persoonsgegevens die de gemeente van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn moeten ze door de gemeente gewijzigd of verwijderd worden (zie onder andere hoofdstuk 9).

5. Opslagbeperking

Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking (zie paragraaf 8.9).

6. Integriteit en vertrouwelijkheid

De gemeente dient te zorgen voor een goede beveiliging van persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen. De gemeente moet er voor zorgen dat ongeoorloofde toegang tot- en gebruik van persoonsgegevens voorkomen wordt.

4.3 Invulling verantwoordingsplicht

De gemeente (strikt genomen het college van burgemeester en wethouders als verwerkingsverantwoordelijke) moet actief aantonen dat ze aan deze voorgaande zes beginselen voldoet. Er is sprake van een omgekeerde bewijslast. Het is niet zo dat een betrokkene of de toezichthouder moet aantonen dat de gemeente niet aan een verplichting voldoet. Dit alles vraagt om een actieve houding van de gemeente, waarbij desgevraagd aan toezichthouder of betrokkene kan worden aangetoond dat de zes beginselen worden nageleefd. De invulling van de verantwoordingsplicht komt met name tot uiting in:

- *Beschermings / beveiligingsbeleid*
  In dit kader is door het college de Nota Informatiebeveiligingsbeleid 2017-2019 vastgesteld. Deze nota gaat deels over de beveiliging van persoonsgegevens. U wordt verwezen naar bedoelde nota. Informatiebeveiligingsbeleid is verbonden met privacybeleid. Voor zover het gaat over beveiliging van persoonsgegevens is het er een onderdeel van. In het informatiebeveiligingsbeleid is onder andere geregeld welke principes gehanteerd worden met betrekking tot te verlenen autorisaties. Enkel diegenen waarbij het noodzakelijk is dat met persoonsgegevens werken, krijgen een autorisatie (zie verder hoofdstuk 7).
- *Verwerkingsregister*
  De gemeente moet[6] een register bijhouden van alle verwerkingsactiviteiten die door of namens de gemeente plaatsvinden. In dit register dient o.a. opgenomen te worden: de categorieën van betrokkenen, de soorten persoonsgegevens en met wie deze gegevens gedeeld worden (zie paragraaf 8.1).
- *Privacy Impact Assessments (PIA)*[7]
  Wanneer een verwerking van persoonsgegevens veel risico's inhoudt voor betrokkenen, moet de gemeente vooraf beoordelen wat het effect hiervan is op bescherming van persoonsgegevens. Er moet dus van tevoren worden gekeken wat de risico's zijn en of die ondervangen kunnen worden (zie paragraaf 8.5).
- *Procedure datalekken*
  Er is sprake van een datalek[8] wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die in strijd is met de AVG. Indien er sprake is van een datalek, dient de gemeente, als verwerkingsverantwoordelijke, dit zo spoedig mogelijk te melden bij de toezichthouder - de Autoriteit Persoonsgegevens - zo mogelijk binnen 72 uur. Wanneer er grote kans bestaat dat de datalek negatieve gevolgen heeft voor betrokkenen, moeten deze ook worden gewaarschuwd. Onder de Wbp bestaat de meldplicht datalekken al. De gemeente heeft hiervoor al een meldprotocol. Dit protocol zal ook gehanteerd worden onder de AVG.

4.4 Persoonsgegevens

De AVG formuleert persoonsgegevens als volgt: "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; 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". [9]

6) Op basis van artikel 30 AVG.

7) Ook wel genoemd 'Data Protection Impact Assesment (DPIA)' of 'Gegevensbeschermingseffectbeoordeling' (in de termen van de AVG zelf).

8) Zie artikel 4 lid 12, alsmede artikel 33 en 34 AVG

9) Zie artikel 4 lid 1 AVG

Een postcode alleen is niet direct herleidbaar tot een natuurlijke persoon. Er is meer informatie nodig om dat te kunnen doen. Bijvoorbeeld een huisnummer. Of de verwerkingsverantwoordelijke de middelen en de mogelijkheden heeft om iemand te kunnen identificeren, is niet doorslaggevend. Er moet gekeken worden naar alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon. Een kenteken is een persoonsgegeven, maar dus zelfs ook wanneer de verwerkingsverantwoordelijke zelf geen toegang heeft tot de bestanden van de Rijksdienst voor het Wegverkeer! [10]

4.5 Verwerking (van persoonsgegevens)

De AVG definieert verwerking als volgt: '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 (artikel 4 lid 2 AVG).' Kort gezegd: iedere handeling met persoonsgegevens geldt als verwerken. De lijst die wordt opgesomd in de definitie is niet limitatief.

4.6 Verwerkingsgrondslagen

Een van de eisen die de AVG stelt is dat persoonsgegevens rechtmatig worden verwerkt [11] . Artikel 6 AVG geeft in dat kader de grondslagen voor verwerking. Persoonsgegevens mogen alleen worden verwerkt indien één van die grondslagen van toepassing is. Hieronder worden de belangrijkste grondslagen besproken.

4.6.1 Toestemming

Betrokkene heeft toestemming gegeven voor het verwerken van persoonsgegevens voor een of meer specifieke doeleinden.

De AVG verstaat onder toestemming 'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.'

In deze definitie zitten een aantal elementen:
Van belang is dat de toestemming in vrijheid is gegeven. Als er een afhankelijke relatie (bijvoorbeeld tussen werkgever en werknemer, of- binnen de gemeente- in het sociaal domein) bestaat tussen degene die toestemming geeft en degene die de persoonsgegevens wil gebruiken, is er een grote kans dat de gegeven toestemming niet in vrijheid is gegeven. In de Delftse situatie zal toestemming veelal niet vrijelijk kunnen worden gegeven gezien de vaak afhankelijke relatie tussen de gemeente en de betrokkene.

Verder dient de toestemming specifiek geïnformeerd te zijn. Dat wil zeggen: deze mag niet te ruim en algemeen geformuleerd zijn, en het moet voor de betrokkene duidelijk zijn welke persoonsgegevens voor welke doeleinden verwerkt worden. Toestemming is ondubbelzinnig wanneer er geen onduidelijkheid kan bestaan of de betrokkene daadwerkelijk toestemming heeft gegeven voor een specifieke verwerking.

Nieuw is dat de gemeente zal moeten kunnen aantonen dat de betrokkene toestemming heeft gegeven. Dat betekent bijvoorbeeld dat de baliemedewerkers bij het KCC een verleende toestemming goed moeten vastleggen. Het is daarbij ook van belang het verzoek om toestemming zo eenvoudig, duidelijk en specifiek mogelijk te formuleren [12] *.*

Verder is van belang dat degene die toestemming verleent hiervoor een duidelijke actieve handeling moet verrichten. Bijvoorbeeld: het op een webformulier vast aanvinken van het hokje 'ik verleen toestemming' is niet toegestaan. Betrokken moet zelf het vinkje zetten.

Een gegeven toestemming kan te allen tijde worden ingetrokken. Dit betekent dat er dan geen grondslag voor verwerking overblijft. Toestemming is dus een risicovolle grondslag. Er zullen modellen voor de

10)Engelfriet, p.20.
11)Zie artikel 5 lid 1 samen met artikel 6 AVG.
12)Zie artikel 7 AVG.

verschillende vormen van toestemming worden gemaakt. Deze zullen aan dit beleid worden toegevoegd. Toestemming moet in ieder geval altijd schriftelijk geschieden. Daarbij moet steeds blijken dat betrokkene weet waarvoor hij toestemming heeft gegeven.

4.6.2 Wettelijke verplichting [13]

Het verwerken van persoonsgegevens is noodzakelijk om aan een wettelijke verplichting te voldoen. Een voorbeeld: de Participatiewet verplicht het college van burgemeester en wethouders in bepaalde gevallen om (persoons)gegevens te verstrekken aan instanties als de belastingdienst. Om aan deze verplichting te voldoen is het noodzakelijk dat het college gegevens verwerkt.

4.6.3 Publiekrechtelijke taak

De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag [14]. Hiervan is bijvoorbeeld sprake als de gemeente een bij wet geregelde - publiekrechtelijke - taak uitvoert. Er moet sprake zijn van een typische overheidstaak. Een voorbeeld hiervan is het beslissen op een aanvraag voor een maatwerkvoorziening op grond van de Wmo 2015.

4.7 Doelbinding

Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld [15]. Let wel: verzamelen is ook verwerken! Voordat er aan verwerking van persoonsgegevens gedacht kan worden, moet er dus eerst duidelijkheid zijn over een specifiek en concreet, dus precies omschreven doel . Wanneer er geen wettelijke grondslag is, is er in ieder geval geen sprake van een gerechtvaardigd doel.
Vervolgens kan de gemeente deze persoonsgegevens verder verwerken (bijvoorbeeld door het verstrekken aan derden). Dat mag alleen maar wanneer het doel voor deze verdere verwerking verenigbaar is met het oorspronkelijke doel.
Dit bij elkaar wordt *doelbinding* genoemd.

Een voorbeeld: een zorgverzekeraar mag persoonsgegevens van een klant verzamelen in het kader van de uitvoering van de verzekeringsovereenkomst. Stel dat de klant medicijnen declareert die een relatie hebben met het hebben van overgewicht. De verzekeringsmaatschappij mag vervolgens de gegeven van de klant niet doorgeven (verkopen) aan bedrijven die dieetproducten verkopen. Het doel waarvoor de persoonsgegevens in de eerste instantie verzameld zijn door de zorgverzekeraar (het uitvoeren van de zorgpolis) komt immers niet overeen met het nieuwe doel (het verkopen van profielen van klanten).

Bedenk dat de noodzaak van het hebben van een specifiek en gerechtvaardigd doel ook geldt binnen de gemeente. Voor het uitvoeren van een wet als de Wmo 2015 mogen persoonsgegevens verzameld worden: er is een wettelijke grondslag en een welbepaald doel. Maar die persoonsgegevens mogen vervolgens niet zomaar voor andere doeleinden worden gebruikt, bijvoorbeeld voor het koppelen met Jeugdwetbestanden. Er moet op zo'n moment altijd eerst gekeken worden of er sprake is van verenigbaar doel.

4.8 Verwerkingsverantwoordelijke en verwerker

Binnen de AVG wordt onderscheid gemaakt tussen:

- de verwerkingsverantwoordelijke [16] (onder Wbp: 'verantwoordelijke')
- de verwerker (onder de Wbp: 'bewerker')

4.8.1 Een verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke [17] is de entiteit (natuurlijke persoon, rechtspersoon, instantie of (bestuurs)orgaan) die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerkingsverantwoordelijke dient te zorgen voor passende waarborgen voor het naleven van de AVG. Dàt de waarborgen zijn ingesteld moet door de verwerkingsverantwoordelijke kunnen worden aangetoond. In feite is de verwerkingsverantwoordelijke aanspreekbaar op het handhaven van de zes basisbeginselen binnen de AVG (zie paragraaf 0).

13)Artikel 6 lid 1 onderdeel c AVG.
14)Artikel 6 lid 1 onderdeel e AVG.
15)Artikel 5 lid 1 onderdeel b AVG.
16)Artikel 4 lid 7 AVG.
17)Artikel 4 lid 7 AVG.

De doelen die worden vastgesteld moeten welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn[18]. Met middelen worden alle gereedschappen en andere middelen bedoeld waarmee een verwerking wordt uitgevoerd, bijvoorbeeld software.
Wie is verwerkingsverantwoordelijke? In de meeste gevallen zal dat het college van burgemeester en wethouders zijn, vooropgesteld dat het college doel en middelen van de verwerking vaststelt. Maar ook de burgemeester of de raad kunnen verwerkingsverantwoordelijke zijn. De burgemeester bijvoorbeeld als onderdeel van het Veiligheidshuis kamer Delft.
De AVG kent ook de figuur van de 'gezamenlijke verwerkingsverantwoordelijken'. In dat geval stellen twee of meer verwerkingsverantwoordelijken doel en middelen van de verwerking vast. In die gevallen waarbij de gemeente Delft is betrokken bij samenwerkingsovereenkomsten (samenwerking in de keten) waarbij er sprake is van meerdere verwerkingsverantwoordelijken, dan dient te worden vastgesteld welke partij welke verantwoordelijkheden op zich neemt[19]. De gemeente Delft zal hiervoor een standaard data-leveringsovereenkomst gaan hanteren. In deze overeenkomst moeten onder andere afspraken worden opgenomen over de vraag waar betrokkenen terecht kunnen voor hun recht op inzage et cetera. Uiteraard dient deze informatie aan betrokkenen zelf worden verstrekt (zie hoofdstuk 9).

4.8.2 Een verwerker

Een verwerker[20] is een entiteit (natuurlijke persoon, rechtspersoon, instantie of (bestuurs)orgaan) die een verwerking uitvoert binnen het doel en middelen die de verwerkingsverantwoordelijke heeft vastgesteld. Een verwerker heeft geen zeggenschap over de wijze van verwerken, en werkt strikt onder instructies en in opdracht van de verwerkingsverantwoordelijke. Een verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

Het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker is niet altijd makkelijk te maken. Het is dus zaak om daar in zo vroeg mogelijk stadium advies over in te winnen van de afdeling Juridische Zaken. Vaak is het immers zo dat een verwerker zelf zijn software kiest. In zo'n geval moet dan ook gekeken worden naar wie het doel van de verwerking bepaalt. Indien de gemeente bijvoorbeeld de salarisadministratie uitbesteedt aan een marktpartij, dan is het nog steeds de gemeente die bepaalt voor welk doel de marktpartij haar software dient te gebruiken: het uitvoeren van de salarisadministratie volgens de instructies en de wensen van de gemeente.

Het onderscheid is wel van belang: Een verwerkersverantwoordelijke is in beginsel voor alle schade aansprakelijk, ongeacht of die door hem of de verwerker wordt veroorzaakt.[21] Een verwerker is daarentegen slechts aansprakelijk voor de schade die door een verwerking is veroorzaakt wanneer bij die verwerking niet is voldaan aan de specifieke verplichtingen binnen de AVG die zijn gericht tot verwerkers (bijvoorbeeld het toepassen van een passend beveiligingsniveau), of wanneer de schade is ontstaan doordat de verwerker zich niet aan de instructies van verwerkingsverantwoordelijke houdt.

Van belang is om te noemen dat een betrokkene zowel verwerker als verwerkingsverantwoordelijke voor het geheel van de schade kan aanspreken[22]. Er bestaat tussen verwerker en verwerkersverantwoordelijke wel een mogelijkheid om de vergoede schade te verhalen op de ander.[23]. Het is om meerdere redenen van groot belang om vast te stellen wie verwerkingsverantwoordelijke is en wie verwerker.

De AVG legt de meeste verantwoordelijkheden bij de verwerkingsverantwoordelijke neer: deze is aanspreekbaar op de verantwoordingsplicht, is aanspreekpunt voor wat betreft de rechten van betrokkenen, is aanspreekbaar op (het melden van) datalekken etc. Zodra een verwerker zelf het doel en de middelen van de verwerking gaat vaststellen wordt deze automatisch verwerkingsverantwoordelijke, zie artikel 28 lid 10 AVG.

Wanneer het college een verwerker inschakelt voor het verwerken van persoonsgegevens, dient er een verwerkersovereenkomst gemaakt te worden. Deze moet schriftelijk of elektronisch worden aangegaan. De AVG bepaalt in artikel 28 welke zaken in zo'n verwerkersovereenkomst opgenomen moeten worden (zie bijlage 2). Onder andere het nemen van passende technische en organisatorische maatregelen.

18 Zie onder noot 8.
19 Zie artikel 26 AVG
20 Artikel 4 lid 8 AVG samen met artikel 28 AVG.
21 Artikel 82 lid 2 AVG
22 Artikel 82 lid 1 AVG
23 Artikel 82 lid 5 AVG

De gemeente Delft zal een standaard-verwerkersovereenkomst hanteren die in alle gevallen wordt aangeboden aan verwerkers en wordt opgenomen in het aanbestedingstraject. Daarnaast stelt de gemeente eisen aan verwerkers (zie paragraaf 4.10.1 en 8.3).

4.9 Betrokkene
De betrokkene is de natuurlijke persoon op wie de persoonsgegevens betrekking hebben.

4.10 Bijzondere en gevoelige persoonsgegevens
Bijzondere persoonsgegevens en gevoelige persoonsgegevens spelen een belangrijke rol. Bijzonder persoonsgegevens worden in de AVG geregeld, in de praktijk speelt ook het ruimere begrip 'gevoelige gegevens' een rol.

4.10.1 Bijzondere persoonsgegevens
Net als in de Wbp worden er in de AVG een aantal categorieën van bijzondere persoonsgegevens gehanteerd, die extra privacygevoelig zijn. Het betreft: ras of etniciteit, politieke opvattingen, religie/levensbeschouwing, vakbondslidmaatschap, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens betreffende seksualiteit [24].
In principe is het verboden om deze gegevens te verwerken, tenzij. De AVG en de Uitvoeringswet AVG bepaalt in welke gevallen bijzondere of gevoelige gegevens verwerkt mogen worden. Er zijn uitzonderingen op dat verbod [25], bijvoorbeeld in het geval betrokkene uitdrukkelijke toestemming heeft gegeven, of in het geval de gemeente de gegevens moet verwerken voor het uitvoeren van een wettelijke taak, zoals bijvoorbeeld de Wmo 2015. De gemeente zal uiterst zorgvuldig omgaan met bijzondere persoonsgegevens.

Nieuw is dat genetische en biometrische [26] gegevens tot de bijzondere persoonsgegevens worden gerekend. Bij biometrische gegevens moet gedacht worden aan een pasfoto op een rijbewijs of paspoort, of een vingerafdruk. Het wordt enkel gebruikt om iemand te identificeren. Ook hier geldt dus: verwerking is verboden, tenzij. De gemeente verwerkt biometrische gegevens enkel als dit nodig is voor het uitvoeren van een wettelijke taak (bv het uitgifte paspoort op grond van de Paspoortwet). Ook kunnen ze worden verwerkt voor beveiligingsdoeleinden [27], bijvoorbeeld voor de toegang tot het gemeentekantoor.
Net als onder de Wbp behoren strafrechtelijke gegevens tot de bijzondere persoonsgegevens. Er wordt onder de AVG hiervoor een apart artikel 10 aan gewijd. De gemeente mag o.a. strafrechtelijke gegevens verwerken in het kader van het Veiligheidshuis [28]. Uiteraard mag dat alleen wanneer het strikt noodzakelijk is.
Ook al wordt het onder de AVG geen bijzonder persoonsgegeven genoemd, voor het burger- servicenummer (BSN) blijft gelden dat het enkel gebruikt mag worden wanneer het door de wet is voorgeschreven, en enkel voor de doeleinden gebruikt mag worden die die wet bepaalt [29]. Nederland gaat hier dus verder dan de AVG, en heeft gebruik gemaakt van de beleidsvrijheid die de AVG biedt.
Gezien het risico van het verwerken van bijzondere persoonsgegevens voor betrokkenen, zal de gemeente deze niet door derden laten verwerken, tenzij dat er zwaarwegende belangen zijn. Dit ter beslissing van de FG. Indien desondanks bijzondere persoonsgegevens niet 'in house' worden gedraaid (maar bij een verwerker), dient het beschermingsniveau gegarandeerd te zijn. Dit betekent dat bijzondere persoonsgegevens in beginsel binnen de EER gehost dienen te worden. De FG zal hier op toezien (zie paragraaf 4.8.2 en 8.3).

4.10.2 Gevoelige persoonsgegevens
Onder gevoelige persoonsgegevens [30] worden ten eerste de bijzondere persoonsgegevens gerekend. Daarnaast behoren financiële persoonsgegevens tot de gevoelige gegevens (bijvoorbeeld gegevens over schulden, salarisstroken, etc). Verder persoonsgegevens op grond waarvan mensen kunnen worden 'nagewezen' (stigmatisering), zoals gegevens over een goksverslaving. Tenslotte worden wachtwoorden, inloggegevens, burgerservicenummers, kopieën van identiteitsbewijzen, en bankreke-

24 Zie artikel 9 AVG.
25 Zie artikel 9 lid 2 AVG, samen met artikel 22 e.v. Uitvoeringswet AVG (UAVG).
26 Zie voor de definitie artikel 4 lid 13 AVG.
27 Artikel 29 UAVG
28 Zie artikel 33 lid 1 onderdeel b UAVG
29 Zie artikel 46 UAVG
30 Zie beleidsregels datalekken AP, p.5, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

ningnummers tot de gevoelige gegevens gerekend. Indien iemand ten onrechte toegang krijgt tot deze gegevens, kan daarmee (identiteits)fraude gepleegd worden. Dat is een groot risico.
Van belang is op te merken dat ook al zou iemand vinden dat het niet erg is als een gevoelig persoonsgegeven bekend wordt ('ze mogen alles van me weten') niet relevant is bij de beoordeling of een persoonsgegeven gevoelig is.
Of een persoonsgegeven gevoelig van aard is speelt onder andere een rol bij de bepaling of de gemeente persoonsgegevens die voor een bepaald doel zijn verzameld ook mag verwerken voor een ander doel (zie paragraaf 4.7) . Hoe gevoeliger het persoonsgegeven, hoe minder snel de gemeente mag aannemen dat er sprake is van een verenigbaar doel.

5 DE AVG EN ANDERE WETTEN

In deze paragraaf wordt de relatie tussen de AVG en andere wetten kort behandeld. Over het algemeen geldt dat de AVG geldt als algemene wet waarvan de bepalingen niet van toepassing kunnen zijn wanneer er bijzondere wetgeving van toepassing is. AVG versus BRP

De AVG en Wet Basisregistratie personen (Wet BRP). De AVG is niet van toepassing op de (Wet BRP) [31] . De wet BRP heeft een eigen, streng, privacy-regime.

5.1 AVG versus WOB

Onder de Wbp gold dat de Wet openbaarheid van bestuur (Wob) een bijzondere wet is tegenover de (algemene) Wbp. In zo'n geval gaat de bijzondere wet voor. Aannemelijk is dat dit ook zal gelden in de nieuwe situatie. Indien de Wob van toepassing is, is de AVG dat niet. Dat betekent niet dat de bescherming van persoonsgegevens geen rol speelt bij de uitvoering van de Wob. Binnen de Wob zijn er namelijk twee weigeringsgronden waarbij de persoonlijke levenssfeer een rol speelt. [32]

5.2 AVG versus Archiefwet

De AVG kent een aantal specifieke uitzonderingen voor verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. Een aantal uitzonderingen werkt rechtstreeks, zie artikel 89 AVG: "Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden'.
Bij verwerkingen onder de kop van onderzoek en archivering dienen de rechten van betrokkenen te worden gewaarborgd. Het accent hierbij ligt bij het beginsel van gegevensminimalisering (dataminimalisatie). Dit betekent dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk voor het doel. Zodra het mogelijk is om het archiveringsdoel te halen met ontkoppelde gegevens (ofwel geanonimiseerde gegevens, niet langer herleidbaar tot een natuurlijke persoon en dus niet langer persoonsgegevens) moet deze ontkoppeling worden uitgevoerd. Als tussenvorm mag gewerkt worden met pseudonimisering (zie paragraaf 8.7.2) waarbij koppeling nog wel mogelijk is, maar de daarvoor benodigde informatie niet direct beschikbaar is [33]
Artikel 89 lid 3 AVG bevat een specifieke bepaling op grond waarvan de lidstaten kunnen afwijken van enkele voorschriften van de AVG. Het gaat hier om de mogelijkheid om af te wijken van de artikelen 15 (het recht op inzage), 16 (het recht op rectificatie), 18 (het recht op beperking van de verwerking), 19 (kennisgevingsplicht), 20 (het recht op overdraagbaarheid van de gegevens) en 21 (het recht op bezwaar).
Er is voor gekozen om op grond van artikel 89 lid 3 AVG een aantal uitzonderingen op te nemen in artikel 45 van de UAVG [34] voor verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden die berusten in een archiefbewaarplaats. Daarbij wordt aangesloten bij de begrippen zoals deze gedefinieerd zijn in de Archiefwet 1995.
De gemeente dient kritisch te blijven kijken binnen de eigen werkprocessen voorafgaand aan archivering en deze te toetsen op dataminimalisatie, zodat kan worden aangetoond dat ook voor wat betreft het gemeentelijke archief voldaan is aan de vereiste passende waarborgen die voortkomen uit de AVG en de UAVG.

5.3 AVG versus Wet politiegegevens

Daarnaast hebben wetten als de Wet politiegegevens een eigen privacyregime. De AVG is hierop niet van toepassing. [35]

31)Dit blijkt uit artikel 2 UAVG.
32)Zie artikel 10 lid 1 onderdeel d, en artikel 10 lid 2 onderdeel e Wob
33)De positie van archieven onder de nieuwe Europese Privacywetgeving, Van Heijst Information consulting.
34)Memorie van Toelichting Uitvoeringswet Algemene Verordening Gegevensbescherming.
35)Artikel 2 lid 2 onderdeel d AVG.

5.4 AVG versus identiteitsbewijs

In veel gevallen is een burger verplicht zich te identificeren met een geldig identiteitsbewijs (de Wet Identificatieplicht en bijzondere wetten). Dat betekent niet per se dat dan ook een kopie daarvan bewaard mag worden. Een identiteitsbewijs bevat een burgerservicenummer en kan bijzondere persoonsgegevens bevatten (ras). Verwerken is dus verboden tenzij.. Een voorbeeld: de wet op de loonbelasting verplicht de gemeente als werkgever een kopie van een identiteitsbewijs van een ambtenaar/werknemer tot 5 jaar te bewaren na het jaar waarin deze persoon uit dienst is getreden. Hier is dus een wettelijke grondslag voor het bewaren van een kopie van een identiteitsbewijs (zie paragraaf 4.10.1).

6 SANCTIES IN DE AVG

De nationale toezichthouder op het gebied van de AVG is de Autoriteit Persoonsgegevens (AP).

De AP heeft een taak op het gebied van handhaving en op het gebied van voorlichting en bewustwording. Om haar taken goed te kunnen uitoefenen heeft de AP bevoegdheden, die zijn opgenomen in de artikel 57 en 58 AVG.

De Autoriteit Persoonsgegevens:
- kan om alle relevante informatie vragen, en de gemeente is verplicht om die te verstrekken.
- heeft toegang tot de gebouwen, computers etc. van de gemeente
- kan een waarschuwing of berisping geven
- kan een verwerking van persoonsgegevens verbieden
- kan bestuursdwang toepassen (zelf een eind maken aan de overtreding) of een last onder dwangsom opleggen (de gemeente verbeurt dan een dwangsom indien de overtreding niet voor een bepaalde termijn wordt beëindigd).
- kan een boete opleggen
- kan de publiciteit zoeken wanneer zij constateert of vermoedt dat er in strijd met de AVG wordt gehandeld.

Met betrekking tot de boete: de UAVG [36] geeft duidelijk aan dat ook overheden beboet kunnen worden. De boete kan maximaal € 20.000.000,- bedragen.

De AVG hanteert twee categorieën van boetes, maximaal € 10.000.000,- voor relatief lichte (administratieve) vergrijpen, en maximaal € 20.000.000,- voor de zwaarste categorie. Een voorbeeld van de eerste categorie: het ten onrechte niet toepassen van een Privacy Impact Assesment . Een voorbeeld van laatste categorie: het niet naleven van de voorwaarden voor toestemming.

Overigens valt te verwachten dat de AP niet zonder meer boetes gaat uitdelen. Hiervoor is dan al een traject afgelegd. Maar indien de gemeente bijvoorbeeld niet goed heeft meegewerkt aan het opvolgen van aanwijzingen van de AP, valt wel een boete te verwachten.

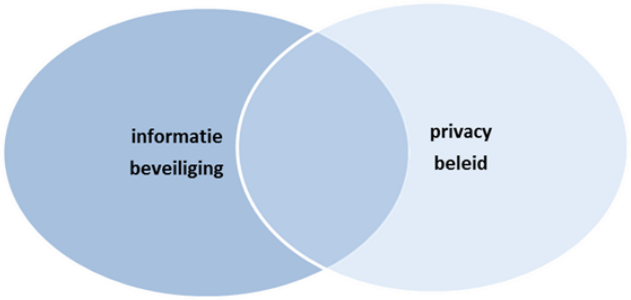
7 GOVERNANCE

In deze nota Privacybeleid worden normen en kaders gesteld voor het omgaan met persoonsgegevens. Om een goede uitvoering te kunnen borgen, is het noodzakelijk om ook besturing en verantwoording op het gebied van bescherming van persoonsgegevens afdoende in te richten. De governance richt zich op de verdeling van verantwoordelijkheden binnen de gemeentelijke organisatie, de cyclus van besturing en verantwoording over het beleid, de relatie met de deelnemingen van de gemeente, en de samenhang met informatiebeveiligingsbeleid.

7.1 Relatie informatiebeveiligingsbeleid – privacybeleid

Informatiebeveiligingsbeleid en privacybeleid zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacybescherming vallen echter niet één op één samen. Ze hebben een gemeenschappelijk raakvlak, en beide ook een eigen domein daarbuiten.

36)Artikel 18 UAVG.



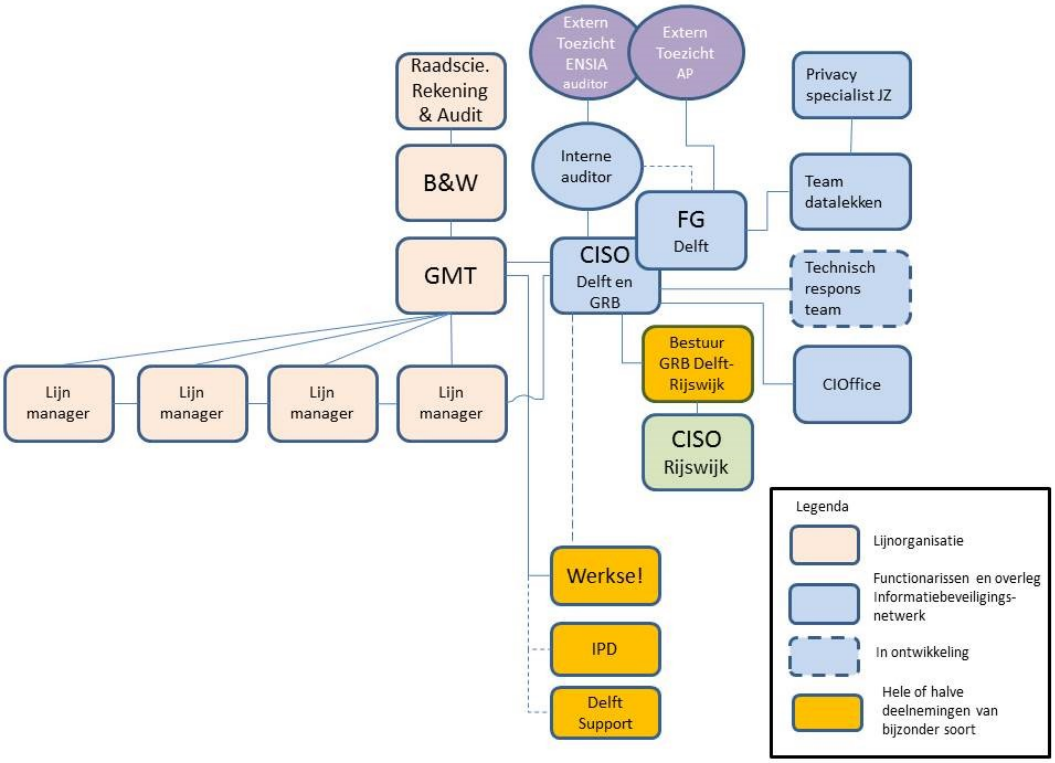
Adequaat informatiebeveiligingsbeleid is een voorwaarde voor de privacyregelgeving, en als zodanig benoemd in de AVG. Dan gaat het met name om de verwerking van persoonsgegevens. Ieder datalek is ook een beveiligingsincident.

Informatiebeveiliging heeft echter een veel bredere scope dan persoonsgegevens. Het gaat om de bescherming van alle data tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Privacybescherming gaat niet alleen over de beveiliging van persoonsgegevens tegen inbreuken, maar ook om het beperken van het verzamelen en gebruiken van persoonsgegevens tot het minimaal noodzakelijke. Een belangrijk thema is de toegang van een burger tot zijn of haar persoonsgegevens en de mogelijkheid om deze gegevens of het gebruik ervan te corrigeren.

De nota Informatiebeveiligingsbeleid 2017-2019 en de nota Privacybeleid 2018 vormen samen een tweeluik over informatiebeveiliging & privacybescherming.

7.2 Organisatie

Voor kaderstelling en uitvoering van privacybeleid is een heldere inrichting van de organisatie nodig, met een duidelijke afbakening van verantwoordelijkheden, taken en bevoegdheden.
In onderstaand schema zijn de verschillende actoren (instanties en functionarissen) weergegeven die een rol en een verantwoordelijkheid hebben in de sturing en de implementatie van het privacybeleid. In dit schema is ook de samenhang zichtbaar met het informatiebeveiligingsbeleid.



7.3 Lijn

Het college van B&W is integraal verantwoordelijk voor de bescherming van persoonsgegevens en de uitvoering van de AVG binnen de werkprocessen van de gemeente. De specifieke rol van het college is het vaststellen van kaders en normen voor privacybescherming en het voldoen aan wet- en regelgeving (compliance) op dit gebied. Het College legt verantwoording af over uitvoering en handhaving van deze kaders en normen. Om de AVG volledig te implementeren en risico's bij de verwerking van persoonsgegevens te beheersen, stelt het college jaarlijks een werkprogramma vast (de Agenda voor privacybescherming) . De gemeenteraad wordt over de hoofdlijnen van privacybeleid geïnformeerd. De monitoring van de agenda voor privacybescherming en actuele risico's is belegd bij de raadscommissie voor Rekening & Audit (R&A).

De gemeentesecretaris is binnen het GMT de verantwoordelijke directeur voor informatiebeveiliging en privacybescherming, mede vanuit het oogpunt van risicomanagement. De functionaris Gegevensbescherming (FG) ondersteunt als toezichthouder de gemeentesecretaris bij het waarmaken van die verantwoordelijkheid op het gebied van bescherming van persoonsgegevens. De FG is gepositioneerd bij de onder de gemeentesecretaris vallende afdeling Controlling onder leiding van de gemeentecontroller, gezien ook de vereiste van onafhankelijke oordeelsvorming. Het gemeentelijk managementteam (GMT) is verantwoordelijk voor de voorbereiding van voorstellen voor kaderstelling en voor de jaarlijkse agenda voor privacybescherming aan het college van B&W. Bij accordering van het beleid door het college van B&W komt de verdere uitwerking en sturing te liggen bij het gemeentelijk managementteam. Het GMT stelt de richtlijnen vast.
Het gemeentelijk managementteam stuurt hierbij op risico's en controleert of de getroffen maatregelen overeenstemmen met de eisen die zijn gesteld vanuit wet- en regelgeving.

De uitvoering van het privacybeleid is in principe belegd bij het lijnmanagement.
De lijnmanager als afdelingshoofd is verantwoordelijk voor de implementatie van het privacybeleid en de bijbehorende richtlijnen, en het uitdragen van de maatregelen binnen zijn of haar afdeling. Hij of zij stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen. Het eigenaarschap van bepaalde processen en systemen waarmee wordt gewerkt , is belegd bij lijnmanagers. In die rol zijn zij verantwoordelijk voor het zorgvuldig beheer van alle gegevens in deze systemen, in het bijzonder voor persoonsgegevens, voor deugdelijke classificatie van gegevens en bijbehorende bescherming en voor het toekennen van rechten in deze systemen. Zij zijn verantwoordelijk voor het zodanig uitvoeren van het beleid dat privacyrisico's tot een minimum worden beperkt.

Bij verschil van mening tussen de FG en de lijnmanager, wordt het geschilpunt voorgelegd aan de gemeentesecretaris, als verantwoordelijk directeur voor privacybescherming, en zo nodig besproken in het GMT. Indien een Collegelid betrokken is bij het geschilpunt, wordt het voorgelegd aan het College, als eindverantwoordelijke instantie voor privacybescherming.

7.4 Informatiebeveiligingsnetwerk

Het beleid voor privacybescherming en voor informatiebeveiliging wordt uitgevoerd en ondersteund door een netwerkorganisatie. Er is geen specifieke afdeling voor deze taken. Privacybescherming vergt kennis op het gebied van gegevensmanagement en IT, juridische kennis van wet- en regelgeving, auditexpertise voor de PIA's, kennis van informatiebeveiliging en van werkprocessen en systemen. Een multidisciplinaire aanpak in een netwerkorganisatie is dan het meest voor de hand liggende model. Samenwerken in een netwerkorganisatie vereist duidelijke rollen, het goed beleggen van taken en verantwoordelijkheden, heldere afspraken over de plannen en prioriteiten en regelmatig overleg.

7.5 FG en CISO en privacyspecialist JZ

De functie van Functionaris Gegevensbescherming (FG) is ingesteld in de Algemene Verordening Gegevensbescherming (AVG). De FG houdt toezicht op de gegevensverwerking in de organisatie, in het bijzonder van de persoonsgegevens. De FG:

- is verantwoordelijk voor het register van interne en externe gegevensverwerkingen
- ziet toe op het naleven van bijbehorende verplichtingen zoals verwerkersovereenkomsten en dataleveringsovereenkomsten
- ziet toe op de toegankelijkheid van burgers tot hun gegevens
- is verantwoordelijk voor de afhandeling en evaluatie van datalekken
- toetst ontwerpen en voorstellen vanuit het oogpunt van privacybescherming
- signaleert risico's op het gebied van bescherming van persoonsgegevens
- coördineert Privacy Impact Assessments (PIA"s)
- behandelt vragen en klachten van mensen binnen en buiten de organisatie.

De FG is een toezichthouder, geen adviseur, en is als het ware de autoriteit persoonsgegevens voor de Delftse organisatie. Het zwaartepunt in de functie van de FG ligt op informatiseringskennis, nodig om processen en systemen te kunnen analyseren op het gebruik van gegevens, aangevuld met kennis van de relevante privacywetgeving.

Gezien de complexiteit van de privacywetgeving is daarnaast centraal georganiseerde juridische expertise onontbeerlijk. Deze expertise wordt geborgd door de privacyspecialist van de afdeling Juridische Zaken (JZ) die het lijnmanagement adviseert over privacyvraagstukken en de FG ondersteunt en aanvult op juridisch gebied.

In de ondersteuning van informatiebeveiliging en de uitvoering van het informatiebeveiligingsbeleid is de Chief Information Security Officer (CISO)[37] de centrale figuur. Deze centrale informatiebeveiligingsfunctionaris heeft tot taak:

- bevorderen van het bewustzijn op het gebied van informatiebeveiliging
- verantwoordelijkheid voor informatiebeveiligingsbeleid uitdragen naar het management
- risico's signaleren op het gebied van informatiebeveiliging
- bij incidenten te zorgen voor de juiste maatregelen, ook in acute situaties
- monitoren van en rapporteren over risico's, uitvoeren van beleid en incidenten
- adviseren over beleid en beleidsvoorbereiding bij nieuwe ontwikkelingen
- het behartigen van het specifieke belang van informatiebeveiliging in de afstemming met gegevens- en systeemeigenaren
- centraal aanspreekpunt zijn voor vraagstukken met betrekking tot informatiebeveiliging

Zowel de functie van CISO als de functie van FG zijn gepositioneerd bij de afdeling Controlling. Beide functionarissen rapporteren rechtstreeks aan de gemeentesecretaris. Voor beide functies is een onafhankelijke positie in de organisatie vereist om kritisch te kunnen oordelen over de informatievoorziening en het informatiemanagement van de organisatie. De afdeling Controlling heeft die positie. Daarnaast wordt voor beide functionarissen een statuut opgesteld waarin het onafhankelijk oordeel wordt geborgd, vergelijkbaar met het auditstatuut.
De privacy specialist van de afdeling Juridische Zaken is belast met het gevraagd en ongevraagd adviseren over de juridische vraagstukken op het gebied van de AVG In deze afdeling wordt juridisch advies

37)CISO is als begrip ingeburgerd in het domein van informatiebeveiliging en wordt met name ook in audits en evaluaties gebruikt. Daarom wordt in dit document de term CISO eveneens gebruikt.

en juridische control geborgd. De AVG is een clusteroverstijgend onderwerp, en daarom is de afdeling Juridische Zaken verantwoordelijk voor de juridische advisering m.b.t. dit onderwerp.

Gezien de overlap tussen beide werkvelden informatiebeveiliging en privacybescherming is een goede samenwerking tussen FG en CISO onontbeerlijk.

7.6 Audit

Het externe toezicht op de bescherming van de persoonsgegevens en de uitvoering van de AVG door de gemeente ligt bij de Autoriteit Persoonsgegevens (AP). De AP houdt toezicht op de uitvoering van de privacywetgeving door organisaties in Nederland en kan zelf onderzoeken doen bij deze organisaties. Het interne toezicht ligt bij de FG. De PIA's worden deels uitgevoerd door de interne IT-auditor van de gemeente, deels uitbesteed aan een externe auditor. De FG coördineert de PIA's.

7.7 Overleggen: team Datalekken

Het team Datalekken is ingesteld bij besluit van B en W van 16 december 2015 (nota Implementatie Wet Datalekken). Het team bestaat oorspronkelijk in de kern uit de CISO, de privacy jurist van de gemeente en de adviseur informatiebeveiligingsbeleid van ID, en kan worden aangevuld met extra benodigde specialisten. Met het in werking treden van de AVG neemt de FG de coördinatie van dit team over. Opdracht van het team is het inrichten en beheren van een procedure voor het melden en afhandelen van datalekken, het adviseren over het voorkomen van datalekken en over het afsluiten van bewerkersovereenkomsten en dataleveringsovereenkomsten.

7.8 Deelnemingen

De gemeente Delft heeft verschillende soorten deelnemingen. Bij de meeste deelnemingen heeft de gemeente wel invloed, maar is niet alleen bepalend voor het uitzetten van de koers.
Bij een aantal specifieke deelnemingen echter, heeft de gemeente Delft wel 100% zeggenschap. Dit betreft

- Werkse! , deels gemeente, deels BV
- BV IPD (1-1-2018)
- BV Delft Support (1-1-2018 / 1-1-2019)
- OBS

Voor het beantwoorden van de vraag of deze deelnemingen een eigen privacybeleid behoeven, zijn de volgende criteria van belang:

1. Is de deelneming verwerkingsverantwoordelijke? en
2. Verwerkt de deelneming veel persoonsgegevens?

Of de deelneming een eigen Functionaris Gegevensbescherming moet aanstellen, hangt af van de volgende criteria:

3. Is de deelneming een overheid of overheidsorgaan, met overheidstaken? en/of
4. Verwerkt de deelneming op grote schaal bijzondere persoonsgegevens?

Het organisatieonderdeel Werkse! valt, voor wat betreft het overheidsdeel van het bedrijf, onder het privacybeleid van de gemeente. De BV voert de WSW uit hetgeen een forse verwerking van bijzondere persoonsgegevens met zich meebrengt. De BV dient daarom formeel een eigen privacybeleid vast te stellen, en kan daarbij in principe het gemeentelijk beleid volgen.
Het verdient de voorkeur om een eigen functionaris gegevensbescherming aan te stellen bij Werkse!
Voor het uitvoeren van de meldplicht datalekken en het afsluiten van verwerkersovereenkomsten en dataleveringsovereenkomsten wordt vooralsnog aangesloten bij de gemeentelijke procedures.

Bij de andere genoemde deelnemingen (IPD en Delft Support) is in dit stadium de verwerkingsverantwoordelijkheid nog niet scherp afgebakend, omdat de wijze waarop de opgedragen taken worden uitgevoerd, nog niet helemaal uitgewerkt is. Op dit moment is het uitgangspunt dat zij op mandaat van de gemeente werken en niet zelf verwerkingsverantwoordelijke zijn. Zij vallen daarmee vooralsnog onder het privacybeleid van de gemeente en het toezicht door de FG van de gemeente.
Als verwerker zal Delft Support vanaf 1-1-2019 op grote schaal bijzondere persoonsgegevens verwerken en zal daarom een eigen FG moeten aanstellen.

OBS BV wordt in de loop van 2018 opgeheven. Tot die tijd volgt OBS BV het gemeentelijk beleid.

De GRB IT-beheer Delft-Rijswijk heeft een aparte positie. Conform de gemeenschappelijke regeling volgt de GRB het informatiebeveiligingsbeleid van Delft. De GRB heeft geen eigen privacybeleid. Ook op dit punt wordt het beleid van Delft gevolgd voor zo ver van toepassing op de levering van IT-beheer. Als leverancier van IT-beheer heeft de GRB een verwerkersovereenkomst afgesloten met de gemeente Rijswijk. Daaronder ligt eenzelfde overeenkomst tussen Delft en GRB.
De verwerking betreft geen overheidsactiviteit. Het is dus niet noodzakelijk om een FG te hebben voor de GRB.
Het aanstellen van een eigen FG is niet verplicht.

7.9 Besturing en verantwoording

De beleidscyclus voor privacybescherming loopt synchroon met de cyclus voor informatiebeveiliging. Zoals in onderstaand schema weergegeven

Toelichting: De nota Privacybeleid bevat de kaders en de uitgangspunten. Deze nota wordt in principe 1x per 2 jaar geactualiseerd en vastgesteld door het College.

7.10 Plan – Do – Check - Act

De implementatie van maatregelen die voortvloeien uit deze nota, volgt de jaarlijkse cyclus zoals hierboven gevisualiseerd.

7.10.1 Plan

De cyclus start met een integrale risico - analyse en de GAP-analyse. Op basis hiervan wordt de samenstelling en prioritering van de agenda voor privacybescherming voor 2018 voorbereid, besproken in het GMT en vastgesteld in het college, met een doorkijk naar 2019.[38] Ter informatie naar de commissie R&A.

De geplande activiteiten worden opgenomen in de werkplannen van de betrokken afdelingen en – voor zo ver mogelijk gezien de lange voorbereidingstijd van de begroting – in de eerstvolgende programmabegroting.

7.10.2 Do

Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces. Dan wel er is gekozen voor uitwerking in projecten.

7.10.3 Check

FG rapporteert 2x per jaar aan GMT, College en commissie R&A over het actuele risicoprofiel (dreigingen), incidenten en de voortgang van de agenda.

38 De jaartallen zijn voorbeelden

In het gemeentelijk jaarverslag wordt een afrondende verantwoording over het jaar opgenomen (in de paragraaf bedrijfsvoering). Omdat het werkveld nog volop in ontwikkeling is, zal in de eerste 2 jaar uitgebreider worden gerapporteerd over de resultaten en risico's in een afzonderlijke rapportage.

7.10.4 Act

De cyclus is rond met de uitvoering van verbeteracties op basis van check en externe controle.
Als de bevindingen bij de tussentijdse rapportages daartoe aanleiding geven, wordt de nota Privacybeleid geactualiseerd. De nota heeft een geldigheidsduur van 2 jaar en zal dus minimaal iedere 2 jaar worden geëvalueerd en opnieuw worden vastgesteld.

8 RECHTMATIGHEID

Bij het woord rechtmatigheid moet in het algemeen gedacht worden aan de vraag of er gehandeld wordt conform de AVG. In onderstaande paragrafen komen zaken voor die er aan bijdragen dat deze rechtmatigheid geborgd wordt, maar worden ook zaken genoemd waarbij er een groot risico is dat in strijd met de AVG, en daarmee onrechtmatig, gehandeld wordt, en er dus extra aandacht vereist is.

8.1 Verwerkingsregister

In paragraaf 4.3 is het verwerkingsregister al genoemd. De gemeente moet een overzicht bijhouden van alle verwerkingen (structureel en incidenteel) van persoonsgegevens, door of namens de gemeente. Dit register komt in de plaats van de meldingsplicht van verwerkingen van persoonsgegevens aan de toezichthouder, zoals die onder de Wbp bestaat. De FG is verantwoordelijk voor het verwerkingsregister.

In het register moeten de volgende gegevens staan [39]:

- Naam en contactgegevens van de gemeente en van de FG
- Naam en contactgegevens van eventuele medeverantwoordelijken. Denk hierbij aan de gezamenlijke verwerkingsverantwoordelijkheid die kan bestaan wanneer de gemeente een samenwerkingsovereenkomst sluit met andere partijen (zie paragraaf 4.8.1)
- De verwerkingsdoeleinden
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens (algemene of bijzondere persoonsgegevens)
- De categorieën van ontvangers aan wie de persoonsgegevens aan wie gegevens zijn of zullen worden verstrekt
- Informatie over doorgifte aan derde landen
- Indien mogelijk: de beoogde bewaartermijnen
- Indien mogelijk: een beschrijving op hoofdlijnen hoe de persoonsgegevens beveiligd zijn

De gemeente zal in het register ook de grondslag voor de verwerking opnemen. Strikt genomen is dit niet verplicht, het biedt echter wel meer waarborgen voor het rechtmatig en bewust omgaan met persoonsgegevens. Indien 'toestemming' als verwerkingsgrond wordt gebruikt, dan wordt verwezen naar alle documentatie waaruit kan blijken de toestemming geïnformeerd en specifiek is.
Verder zal bij elke verwerking die in het register wordt opgenomen de 'interne eigenaar' worden opgenomen. Vaak zal dat het afdelingshoofd zijn.
Voor de nieuwe verwerkingen zal een apart protocol, inclusief checklist, worden opgesteld. Het is immers van belang om nieuwe verwerkingen vooraf en tijdig te toetsen aan alle eisen die de AVG stelt, bijvoorbeeld voor het verwerkingsregister. Maar ook voor alle overige elementen van de verantwoordingsplicht. Zie voor een stroomschema 'rechtmatige verwerking', bijlage 3.

8.2 Persoonsgegevens delen

In hoofdstuk 4.7 is het principe van doelbinding besproken. Bij de wens om persoonsgegevens zowel intern als extern te delen moet steeds gekeken worden in hoeverre het doel waarvoor de gegevens in de eerste instantie zijn verzameld, voldoende overeenkomt met het doel waarvoor de persoonsgegevens vervolgens worden gebruikt.

Denk bij het delen bijvoorbeeld aan het aan elkaar koppelen van systemen. Verder delen van persoonsgegevens vergt dus steeds een toets van de FG, met advies van de privacyspecialist van Juridische zaken.

8.3 Verwerkersovereenkomst en datadeelovereenkomst

Bij het starten van een nieuwe verwerking dient eerst de vraag gesteld te worden wie verwerkingsverantwoordelijke is. Als de gemeente verwerkingsverantwoordelijke is maar de verwerking uitbesteedt

39 Zie artikel 30 AVG.

aan een derde dan wordt er een verwerkingsovereenkomst afgesloten. Bij verwerking in de keten wordt een datadeelovereenkomst afgesloten.
De FG is verantwoordelijk voor het deugdelijk afsluiten van deze overeenkomsten en moet daarom in een vroeg stadium op de hoogte worden gebracht van geplande nieuwe verwerkingen en wijzigingen in bestaande verwerkingen.

Zoals in hoofdstuk 4 is aangegeven zal de gemeente een standaardverwerkersovereenkomst hanteren. In de komende periode zullen de bestaande verwerkersovereenkomsten in overeenstemming worden gebracht met de AVG. Voor nieuwe verwerkingen waarbij een verwerker wordt ingeschakeld zal de standaard verwerkingsovereenkomst meteen worden gebruikt. De standaardovereenkomst wordt ingebracht bij aanbestedingstrajecten, als onderdeel van het af te sluiten contract.
Voor verwerkingen die op externe servers worden verricht , al dan niet als SaaS-oplossing, wordt een toetsingskader ontwikkeld. Deze verwerking hoeft op zich geen probleem te zijn, zolang door middel van een goede verwerkersovereenkomst kan worden geborgd dat de verwerking op een zorgvuldige manier wordt uitgevoerd. Een probleem ontstaat wanneer een applicatie op een server zou draaien die zich buiten de Europese Economische Ruimte (EER) bevindt. Het risico bestaat dan er dat daar een onvoldoende passend beschermingsniveau is. De AVG bepaalt dat persoonsgegevens niet zonder meer buiten de EER mogen worden gebracht.
Uitgangspunt voor de gemeente Delft is dat persoonsgegevens niet buiten de EER worden gebracht. Slechts indien er geen enkele andere oplossing is en de noodzakelijkheid kan worden aangetoond, kan de FG , met advies van de privacyspecialist JZ, bezien of er binnen de AVG een rechtmatige en veilige manier is om de persoonsgegevens buiten de EER te brengen.

Ook voor datadeelovereenkomst zal gebruik gemaakt worden van een standaardovereenkomst.

8.4 Privacy by design en privacy by default

Privacybescherming bestaat niet alleen uit toetsen en controle achteraf. Om de zes principes van privacybescherming zoals verwoord in hoofdstuk 4, zo goed mogelijk door te voeren, dient juist ook aan de voorkant van het ontwerpen en inrichten van processen en systemen privacybescherming als uitgangspunt genomen te worden. Voor de AVG zijn privacy by design en privacy by default belangrijke onderdelen van de verantwoordingsplicht van de gemeente.

8.4.1 Privacy by design

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.
Bij de inrichting van proces of systeem wordt gekeken naar de eisen die vanuit de invalshoek van privacy gesteld kunnen worden. Dataminimalisatie is bijvoorbeeld één van de uitgangspunten die hierbij gehanteerd worden: zo min mogelijk persoonsgegevens verzamelen, alleen datgene wat strikt noodzakelijk is voor het bereiken van het doel. Ook kunnen privacyverhogende maatregelen worden meegenomen, bijvoorbeeld door gevoelige gegevens in een afgesloten bestand te bewaren.

Voorbeelden van privacy by design: het op eenvoudige wijze uit kunnen draaien van alle persoonsgegevens van een betrokkene die in een applicatie voorkomen, wanneer de betrokkene daar om vraagt. Of de mogelijkheid inbouwen dat persoonsgegevens na verloop van een bepaalde periode automatisch verwijderd worden, of in ieder geval het systeem laten waarschuwen dat de bewaartermijn verstreken is. Of er aan de poort voor te zorgen dat de instellingen van systemen waarbij gevoelige persoonsgegevens worden verwerkt zodanig zijn dat de optie 'benaderbaar voor alle medewerkers' ontbreekt. Het proces aanpassen zodat een ID alleen getoond behoeft te worden en geen kopie ID wordt bewaard.

Om privacy by design te borgen in de organisatie zullen medewerkers worden getraind in denken in privacy by design. Daarnaast zal actief geadviseerd worden door de privacyjurist JZ , de CISO en de afdeling IT over de invulling van privacy by design en zal de FG toetsen op de (tussentijdse) resultaten. Dit proces dient in komende jaren nader te worden uitgewerkt en beproefd.

8.4.2 Privacy by default

Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat , als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat moet worden bereikt. Bijvoorbeeld:
- een app niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op de website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- persoonsgegevens niet met collega's wordt gedeeld wanneer daarvoor geen noodzaak is.

De uitwerking van deze werkwijze wordt meegenomen in het nog te ontwikkelen proces voor privacy by design.

8.5 Privacy Impact Assessment

Een Privacy Impact Assessment (PIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Is hiervoor geen garantie te geven dan moet de gemeente de toezichthouder (AP) verplicht om advies vragen voordat met de verwerking van de persoonsgegevens begonnen wordt.

De gemeente moet dus zelf bepalen of er sprake is van een risicovolle verwerking. Daartoe wordt een methode ontwikkeld om periodiek risico-analyses te maken, te bepalen welke PIA's noodzakelijk en urgent zijn en deze uit te voeren. Als 0-meting worden privacy risicosessies gehouden op 8 risicovolle onderdelen van de organisatie. De uitkomsten van deze risicosessies worden gebruikt om te bepalen op welke verwerkingen een PIA zal worden toegepast. De IT-auditor is verantwoordelijk voor de ontwikkeling en toepassing van de PIA, de FG coördineert de uitvoering van de PIA's.

De AVG noemt drie categorieën verwerkingen waarin een PIA in ieder geval moet worden uitgewerkt:
- systematische, uitgebreide en geautomatiseerde beoordeling van persoonlijke aspecten van de betrokkenen (bv profilering);
- grootschalige verwerking van bijzondere of strafrechtelijke gegevens;
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten

8.6 Cameratoezicht

De gemeente maakt gebruik van cameratoezicht op openbare plaatsen. Persoonsgegevens die in dat kader verwerkt worden vallen op dit moment onder de Wet politiegegevens, ze worden immers verwerkt met als doel het handhaven van de openbare orde. De AVG is niet van toepassing op politiegegevens (zie hoofdstuk 5).

De gemeente maakt geen gebruik van cameratoezicht op de werkplek (in het kader van bijvoorbeeld het voorkomen van diefstal), behalve bij de publiekszaal van Archief Delft .

Wel gebruikt de gemeente camera's in de publiekshal van het stadskantoor en in het stadhuis, ter beveiliging van hen die zich daar bevinden. De camerabeelden worden slechts voor dat doeleinde gebruikt.

8.7 Anonimisering / Pseudonimisering

Als gegevens niet meer te herleiden zijn tot natuurlijke personen, zijn het geen persoonsgegevens, en is de AVG niet van toepassing. We spreken dan van anonieme gegevens. Indien persoonsgegevens worden versleutel, en die sleutel wordt apart opgeborgen, is er sprake van pseudonomisering. Hier is de AVG nog wel van toepassing. Goed uitgevoerde pseudonimisering geniet de voorkeur boven het gebruik van onversleutelde persoonsgegevens.

8.7.1 Anonimisering

Wanneer gegevens niet meer herleidbaar zijn tot natuurlijke personen, zijn ze anoniem. De AVG is dan niet van toepassing. In veel gevallen is het niet nodig om te werken met persoonsgegevens, om toch het gestelde doel te bereiken. Indien de gemeente bijvoorbeeld de gemiddelde leeftijd van een bezoeker van museum het Prinsenhof zou willen weten, is het niet nodig om de gegevens van alle individuele bezoekers in een bestand te zetten. Beter is dan om alle gegevens 'weg te gooien' behalve de leeftijd. Nu zijn de gegevens niet meer te herleiden tot personen.

8.7.2 Pseudonimisering

Iets anders is pseudonimiseren[40] van persoonsgegeven. Daar wordt, in tegenstelling tot bij anonimisering, de 'sleutel' niet weggegooid. Persoonsgegevens worden losgekoppeld van de andere gegevens en vervangen door bijvoorbeeld een code. Zolang de mogelijkheid blijft bestaan dat de codes terugvertaald worden naar persoonsgegevens, blijft de AVG van toepassing.
Pseudonimisering betekent niet dat er geen sprake meer is van persoonsgegevens. Wel is het zo dat eerder zal worden voldaan aan de vereisten van beveiliging en dat de risico's voor betrokkenen minder kunnen zijn (omdat herleiding veel minder makkelijk is) .
Pseudonimisering vereist het nemen van zorgvuldige technische en organisatorische maatregelen om te kunnen waarborgen dat koppeling aan natuurlijke personen niet alsnog nodig is.
De gemeente zal een protocol voor anonimiseren en pseudonimiseren ontwikkelen ten behoeve van passende beveiliging van persoonsgegevens.

40 Zie artikel 4 lid 5 AVG

8.8 Risicoprofilering

Het nemen van besluiten op basis van risicoprofilering [41] is niet toegestaan, tenzij er een (expliciete) wettelijke basis voor bestaat. Het verbod geldt voor geautomatiseerde besluitvorming op basis van algoritmes, zonder menselijke tussenkomst. Een voorbeeld van profilering: bij het online aanvragen van een lening, wordt deze geweigerd om dat de aanvrager een 'risicovolle' postcode heeft. De gemeente Delft zal profilering (met menselijke tussenkomst) slechts dan gebruiken indien daarvoor een aantoonbaar belang mee is gediend. Dit ter beslissing van de FG. Alle bestaande risicoprofileringen zullen opnieuw worden beoordeeld op rechtmatigheid.

8.9 Bewaartermijnen

De AVG bevat het al eerder genoemde beginsel van opslagbeperking (zie paragraaf 0). Dit houdt in dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijkheid is voor de verwerking. De AVG verlangt dat de gemeente concrete termijnen benoemt, maar noemt zelf geen termijnen. Ze moeten in ieder geval een duidelijk vast te stellen einde hebben. De gemeente neemt in het verwerkingsregister de bewaartermijnen van de verschillende verwerkingen op, en stelt deze vast voor zover dat nog niet gebeurd is.

8.10 Big data / tracking

Bij Big data gaat het om het verzamelen en hanteren van zeer grote hoeveelheden data. Data gegenereerd uit elektronische activiteiten van gebruikers, en uit onderlinge communicatie tussen apparaten (machine to machine). Big-data-analyse is het gebruik van technieken, technologieën en softwaretools voor analyse van Big data uit de organisatie en/of uit andere gegevensbronnen. Bij tracking gaat het om het volgen van (het gedrag van) gebruik van gebruikers van mobiele telefoon via een wifi-verbinding, of van het surfgedrag op internet. De gemeente maakt tot op heden geen gebruik van tracking.

Ontwikkelingen in het kader van o.a. Smart Cities vragen van de gemeente steeds meer toe te werken naar het gebruik van nieuwe technologieën zoals Big data en tracking. Deze technologieën kunnen nodig zijn voor het optimaal uitvoeren van bepaalde taken van de gemeente (zie ook Visie en Informatiestrategie 2017-2020).
[1] Een veelgehoord voorbeeld is het opslaan van gegevens over de aanwezigheid van mobiele telefoons om grote stromen (burger)verkeer te monitoren in het kader van de veiligheid van burgers tijdens, bijvoorbeeld, een nationale feestdag. Maar Big data kunnen bijvoorbeeld ook de dienstverlening verbeteren. Het gebruik van Big data en tracking mag niet leiden tot schending van de privacy. Uitgangspunt van deze gegevensverwerking is dat zo min mogelijk (persoons)gegevens worden opgeslagen en deze gegevens geanonimiseerd worden. Als dit niet mogelijk is worden de gegevens gepseudonimiseerd. Dat betekent dat we persoonsgegevens omzetten in iets wat niet meer direct herleidbaar is tot een persoon. Voor Big Data en tracking wordt door de gemeente een aantal uitgangspunten geformuleerd die het mogelijk moeten maken om met Big Data en tracking aan de slag te gaan, zonder daarbij de kaders die de privacywetgeving stelt, te overtreden.

9 RECHTEN VAN BETROKKENEN

Met de invoering van de AVG krijgen burgers meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun rechten en plichten worden namelijk versterkt en uitgebreid in de artikelen 13 t/m 22 AVG. De betrokkene kan zich voor het inroepen van zijn rechten wenden tot de verwerkingsverantwoordelijke, in de meeste gevallen het college van burgemeester en wethouders. De rechten en plichten gelden voor een ieder waarvan persoonsgegevens worden verwerkt door de gemeente. Het gaat dus niet alleen om de rechten en plichten van de inwoners van Delft. De AVG spreekt daarom over de rechten van betrokkenen. Hieronder worden de verschillende rechten uiteengezet.

9.1 Hoe en in welke mate wordt de burger geïnformeerd?

De gemeente moet transparant zijn over de verwerking van persoonsgegevens. Het moet voor betrokkenen duidelijk zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkene moet begrijpelijk zijn, ook met betrekking tot de *rechten* van betrokkenen. De gedachte hierachter is dat de betrokkene beter in staat is om in te schatten wat er met zijn gegevens gebeurt en eventueel actie kan ondernemen.

Een uitwerking hiervan is dat de gemeente op haar website een privacyverklaring [42] publiceert.

41)Artikel 22 lid 1 AVG samen met artikel 40 UAVG.

42)De uitgewerkte privacyverklaring zal zo spoedig mogelijk worden opgesteld en bekend gemaakt.

9.2 Welke rechten hebben betrokkenen?

Hieronder wordt kort aangeduid wat de rechten van betrokkenen zijn. Hoe de gemeente in de uitvoering om zal gaan met deze rechten wordt verder uitgewerkt in een protocol rechten van betrokkenen.

9.2.1 Recht op informatie [43]

De gemeente moet de betrokkene op de hoogte stellen van het feit dat er een verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat het doel is van de verwerking. De gemeente moet in ieder geval informatie verstrekken over de periode, de bron van gegevens, juridische grondslag voor de verwerking en de rechten die de betrokkene heeft. Indien het doel van de verwerking verandert, dan moet de gemeente hier ook over communiceren. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

9.2.2 Het recht op inzage [44]

Iedere betrokkene heeft de mogelijkheid om te controleren of, en op welke manier zijn/haar gegevens worden verwerkt. Betrokkene kan dit recht uitoefenen door een inzageverzoek in te dienen. Dit verzoek hoeft niet te worden gemotiveerd. Een voorwaarde die wordt gesteld is dat de betrokkene zich identificeert. De gemeente moet zorgvuldig omgaan met persoonsgegevens. Het zonder identificatieplicht overleggen van persoonsgegevens zou misbruik van persoonsgegevens in de hand kunnen werken. De identificatieplicht kan worden vervuld door de betrokkene door in te loggen met zijn/haar DigiD, een kopie van een ID of paspoort mee te sturen met het inzageverzoek of de betrokkene kan zich in persoon identificeren bij de behandelaar van het inzageverzoek.
De betrokkene krijgt alleen inzage in zijn eigen persoonsgegevens en krijgt alleen inzage in datgene wat volgt uit de wet.[45] Daar bijkomend moet de gemeente aan de betrokkene een kopie van de verwerkte gegevens verstrekken. Indien de betrokkene meerdere kopieën wilt ontvangen kunnen daarvoor kosten worden berekend. Naar aanleiding van een inzageverzoek kan de betrokkene besluiten zijn verdere rechten uit te oefenen. Mochten er namelijk persoonsgegevens verkeerd zijn opgenomen kan de betrokkene bijvoorbeeld zijn recht van rectificatie gebruiken.

9.2.3 Het recht op rectificatie [46]

Als het duidelijk is dat de gegevens niet kloppen, kan de betrokkene een verbetering van onjuiste persoonsgegevens proberen te verkrijgen. Indien de betrokkene een terecht verzoek indient zal de gemeente het verzoek afhandelen door de gegevens aan te vullen/te wijzingen en hierover een verklaring afleggen aan de betrokkene. Mocht de gemeente van oordeel zijn dat het geen terecht verzoek is mag de betrokkene een aanvullende verklaring aan de gegevens laten toevoegen.

9.2.4 Het recht op vergetelheid [47]

In sommige gevallen heeft de betrokkene het recht om verwijdering van persoonsgegevens te verkrijgen. Dit geldt met name waar de betrokkene toestemming heeft gegeven om gegevens te verwerken. Wanneer betrokkene de toestemming intrekt of de geldigheid er van betwist, heeft de betrokkene het recht om persoonsgegevens te laten verwijderen. De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer persoonsgegevens nog opgeslagen zijn maar de gegevens niet langer nodig zijn voor het bereiken van het doel, worden de gegevens zo snel mogelijk verwijderd.
De gemeente hoeft niet altijd aan het verzoek te voldoen. Het recht op vergetelheid wordt buitenspel gezet indien het nodig is dat de gemeente gegevens verwerkt:

- In verband met recht op vrijheid van meningsuiting en informatie. Hiervan kan sprake zijn als het grondrecht ‘recht op privacy’ botst met het recht op vrije meningsuiting. Dit zal bij de gemeente niet snel spelen, het kan bijvoorbeeld wel voorkomen bij uitingen van journalisten.
- Om een, in een Unierecht of het nationale recht neergelegde, wettelijke verwerkingsverplichting na te komen, een taak van algemeen belang te vervullen of het uitoefenen van het openbaar gezag; een voorbeeld hiervan is de Wob;
- In het belang van de volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;
- in verband met een rechtszaak.

43)Artikel 13 en 14 AVG
44)Artikel 15 AVG
45)Artikel 15 AVG
46)Artikel 16 AVG
47)Artikel 17 AVG

De gemeente zal dus moeten bepalen of er een uitzonderingsgrond van toepassing is waardoor de persoonsgegevens niet kunnen worden verwijderd. Is er geen uitzonderingsgrond? Dan moet de gemeente meteen overgaan tot verwijdering van de persoonsgegevens. Daarbij moet ook iedere koppeling naar, kopie of reproductie van de persoonsgegevens worden verwijderd. Dit geldt ook voor derde partijen.

9.2.5 Het recht op beperking van de verwerking [48]

De betrokkene heeft het recht om beperking van de verwerking te verkrijgen. Dit houdt in dat de gemeente de gegevens alleen nog maar kan gebruiken met toestemming van de betrokkene. De betrokkene kan hier alleen tot verzoeken in de volgende gevallen:

- Hij heeft een verzoek tot verbetering gedaan dat de gemeente nog in behandeling heeft;
- Of de betrokkene heeft bezwaar gemaakt tegen de verwerking, en de gemeente is nog bezig de belangenafweging te maken;
- De gegevens verwerking is onrechtmatig maar de betrokkene wil niet dat u de gegevens weggooit bijvoorbeeld omdat die voor hem van belang kunnen zijn in een rechtszaak.

Voordat de beperking eraf gaat moet de gemeente hierover vooraf de betrokkene informeren.

9.2.6 Kennisgevingsplicht [49]

Mochten de persoonsgegevens verbeterd, verwijderd of beperkt worden, dan moet dit bij de ontvanger aan wie de gegevens zijn verstrekt, aangegeven worden. Echter, wanneer dit onmogelijk blijkt of onevenredig veel inspanning kost, dan hoeft dit niet. De gemeente verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

9.2.7 Het recht op overdraagbaarheid van gegevens [50]

De betrokkene heeft het recht om de persoonsgegevens die hem betreffen te verkrijgen. Ook mag hij deze in principe overdragen aan een andere verwerkingsverantwoordelijke. Dit kan alleen indien de verwerking berust op toestemming of uit een overeenkomst. En de verwerking via geautomatiseerde procedés wordt verricht.

9.2.8 Het recht van bezwaar [51]

Een betrokkene kan indien zijn situatie daarom vraagt gebruik maken van het recht van bezwaar tegen de verwerking van hem betreffende persoonsgegevens, als voldaan aan de in de verordening genoemde eisen. Als een betrokkene bezwaar maakt staakt de gemeente de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen.

9.2.9 Het recht niet te worden onderworpen aan uitsluitend geautomatiseerde individuele besluitvorming, waaronder profilering [52]

Het nemen van besluiten op basis van risicoprofilering [53] is niet toegestaan, tenzij er een (expliciete) wettelijke basis voor bestaat. Bij dit recht kan bijvoorbeeld gedacht worden aan de verwerking van sollicitaties via internet zonder menselijke tussenkomst. In principe doet de gemeente niet aan geautomatiseerde profilering.

9.3 Kunnen deze rechten worden beperkt?

De betrokkene kan niet altijd zijn rechten inroepen. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 13 t/m 22 kunnen worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen [54] die op de gemeente of de verwerker van toepassing zijn. Er is wettelijk gezien geen grondslag om structureel en categorisch beperkingen op te leggen. Dat betekent dat de gemeente per geval een belangafweging moet maken of de betrokkene zijn/haar rechten kan inroepen of niet.

9.4 Beslissing van de gemeente op een verzoek

Indien een betrokkene een recht gaat uitoefenen zal dat vooral zijn door middel van een gericht verzoek aan de gemeente. De beslissing van de gemeente op dit verzoek valt onder de Algemene wet bestuursrecht (hierna: Awb). [55] Dat betekent dat de beslissing op het verzoek een besluit is in de zin van de Awb

48)Artikel 18 AVG
49)Artikel 19 AVG
50)Artikel 20 AVG
51)Artikel 21 AVG
52)Artikel 22 AVG
53)Artikel 22 lid 1 AVG samen met artikel 40 UAVG.
54)Artikel 41 UAVG
55)Artikel 34 UAVG

waartegen bezwaar kan worden gemaakt. Dat betekent dat ook de wet dwangsom bij niet tijdig beslissen van toepassing is.
De termijn om een besluit te nemen is wettelijk bepaald en staat op 4 weken. Wel is er wettelijke bepaald dat bij een complex verzoek de termijn kan worden verlengd met 2 maanden. Concreet betekent dit dat de gemeente binnen 4 weken een eerste reactie moet geven op het verzoek. Indien deze reactie uitblijft is er derhalve sprake van een besluit.[56] En kan er beroep worden ingesteld tegen het niet tijdig nemen van het besluit op voorwaarde dat de gemeente in gebreke is gesteld en twee weken de tijd heeft gekregen om alsnog te besluiten. Dit geldt ook als de reactie uitblijft na opschorting van de termijn. Er zullen geen kosten worden gerekend, mits het verzoek proportioneel is. Wordt er bijvoorbeeld veelvuldig kort op elkaar een zelfde verzoek ingediend dan kan de gemeente beslissen om het verzoek niet in behandeling te nemen. De gemeente is voornemens het verzoek in begrijpelijke en heldere taal af te handelen .

9.5 Wijze van indiening verzoek

De gemeente zet naast de schriftelijke weg ook de elektronische weg open. Er zal, waar mogelijk, gebruik worden gemaakt van een formulier dat de betrokkene helpt om gebruik te maken van zijn recht(en). Deze formulieren zullen op de website van de gemeente beschikbaar komen. Wanneer de betrokkene gebruik maakt van de uitoefening van een recht en daarmee iets verzoekt, zal worden gereageerd via de weg die de betrokkene kiest.
Juridische Zaken is de coördinerende afdeling voor de afhandeling van deze verzoeken, gezien de mogelijke juridische complexiteit. Voor het afhandeling van een verzoek in het kader van de AVG wordt een procedure ontwikkeld.

10 BEWUSTWORDING

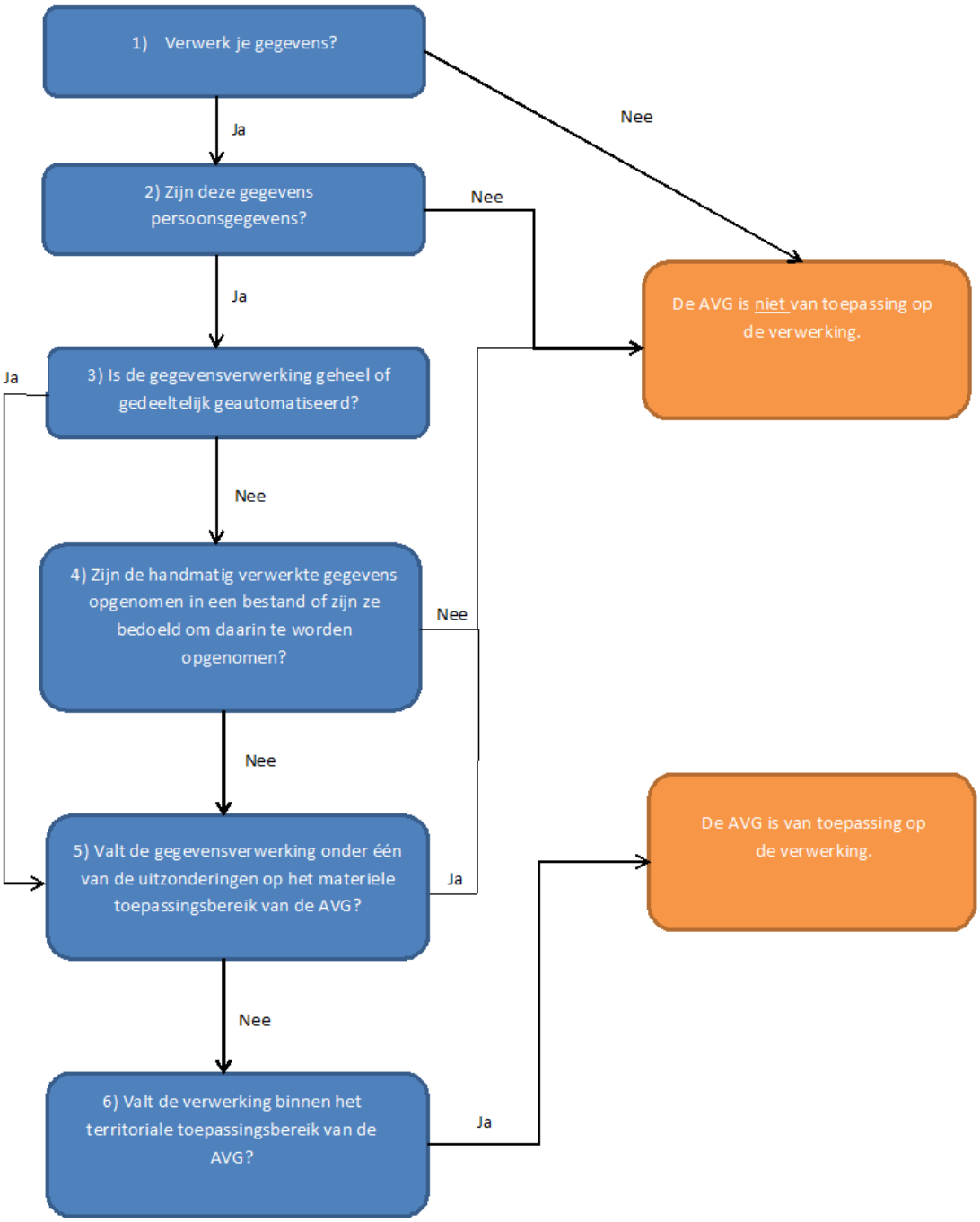
Bewustwording is belangrijk voor het slagen van privacybescherming. Juist bij de uitvoering van het werk is het belangrijk om te onderkennen wat risico's zijn uit het oogpunt van privacy, en hoe daar mee om te gaan. Zonder dit besef zou er alleen gestuurd kunnen worden met hard ingeregelde geboden en verboden en toetsing daarop, en dat is niet te doen en niet gewenst. Het risicobewustzijn bij alle gebruikers wordt vooral via voorlichting en vorming geprikkeld. Daarbij wordt gebruik gemaakt van reële voorvallen, vragen en incidenten omdat aan de hand van echte praktijkvoorbeelden snel duidelijk wordt hoe je als medewerker, manager of bestuurder zou moeten handelen. Ook sturen op sociale controle, bijvoorbeeld over veilig mailen of bellen, en actieve voorlichting in de teams stimuleren het bewustzijn. Werken in één kantoor helpt ook om mensen aan te spreken en – voor de FG en andere privacymedewerkers – om aangesproken te worden over vragen en onduidelijke situaties.

Periodiek wordt de organisatie middels presentaties en via intranet op de hoogte gehouden over de ontwikkelingen op het gebied van informatiebeveiliging. Voor privacybescherming wordt aangesloten op deze werkwijze. Gestructureerde informatie is te vinden op de eigen pagina op KEN en via de e-learning over informatiebeveiliging en privacybescherming. In de introductie van nieuwe medewerkers wordt het belang van privacybescherming en instructie in de zorgvuldige verwerking van persoonsgegevens meegenomen.

GMT, FG en de lijnmanagers hebben de verantwoordelijkheid voor communicatie en bewustwording rondom privacybescherming.

56)Artikel 34 UAVG jo. Artikel 6:2 aanhef en onderdeel b jo. Artikel 6:12 Awb.

BIJLAGE 1: STROOMSCHEMA TOEPASSELIJKHEID AVG



BIJLAGE 2: EISEN VERWERKERSOVEREENKOMST, ARTIKEL 28 AVG

Artikel 28 Verwerker

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen,en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:

    a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;

    b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

    c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;

    d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;

    e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

    f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;

    g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;

    h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

    Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.

6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.

7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.

8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.

9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.

10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

BIJLAGE 3: STROOMSCHEMA RECHTMATIGE VERWERKING