Zutphen

GEMEENTEBLAD

Officiële uitgave van de gemeente Zutphen

Nr. 300053

9 juli

2025

Privacybeleid gemeente Zutphen 2025

1 Inleiding en leeswijzer

Sinds 25 mei 2018 moet de gemeente Zutphen voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Ook dient de gemeente Zutphen zich te houden aan de Wet politie gegevens (Wpg). Deze wet is sinds 21 juli 2007 van kracht. Politiegegevens zijn persoonsgegevens die in het kader van de politietaak worden verwerkt. Naast de politie moeten ook andere organisaties zich aan de Wpg houden: de bijzondere opsporingsdiensten (BOD) en de buitengewoon opsporingsambtenaren (boa's).

Daarnaast is het belangrijk dat de gemeente Zutphen proactief inspeelt op de aankomende wijzigingen op het gebied van informatiebeveiliging zoals de Network & Information Systems Directive 2 (NIS2). Gemeenten hanteren vanaf 1 januari 2020 samen met de rijksoverheid, de waterschappen en de provincies één uniform normenkader voor informatiebeveiliging. Dit is de Baseline Informatiebeveiliging Overheid (BIO). Wanneer de gemeente Zutphen de eisen van de AVG, Uitvoeringswet AVG (UAVG), Wpg en de BIO implementeert en borgt, draagt dit bij aan:

- Het voorkomen van (grootschalige) beveiligingsincidenten en datalekken;
- Het minimaliseren van financiële en imago schade voor de gemeente Zutphen en/of voor inwoners veroorzaakt door de gevolgen van beveiligingsincidenten datalekken;
- Compliance op het gebied van wet- en regelgeving en informatiebeveiligingsstandaarden, in het bijzonder de AVG, Wpg en de BIO;
- Het voorkomen van boetes vanuit de toezichthouder, de Autoriteit Persoonsgegevens (AP).
- Verantwoording afleggen aan de gemeenteraad hoe de gemeente omgaat met gegevens van inwoners en medewerkers.

Leeswijzer
Vele gemeenten stellen de vraag "hoe moet dat nou, met die privacy". De vraag komt vaak voort uit de wirwar van informatie en opvattingen over privacy van onder meer medewerkers en inwoners. Het antwoord hebben we gezocht in de pragmatiek: pak privacy bij de kop zoals de gemeente ermee moet werken.

Het centrale uitgangspunt hierbij is dat persoonsgegevens slechts mogen worden verwerkt als er een wettelijke grondslag voor is én het doel van de verwerking redelijkerwijs niet op een andere wijze kan worden verwezenlijkt. Dit houdt in dat je persoonsgegevens alleen mag verwerken als de gegevens noodzakelijk zijn om het beoogde doel te bereiken. Ga dus altijd na of het doel ook bereikt kan worden zonder dat gegevens gebruikt worden die te herleiden zijn tot een natuurlijke persoon.

Dit document beschrijft transparant en concreet over het privacybeleid en hoe ook netjes te voldoen aan de wettelijke vereisten om boetes, imagoschade en schadeclaims te voorkomen. Door proactief werk te maken van Privacy, kunnen er bewust keuzes worden gemaakt over hoe er met welke informatie wordt omgegaan en weten de medewerkers wat dat in hun dagelijkse werk betekent en vooral waarom. Daarnaast verschaft dit document ook inzicht aan de inwoners om te laten zien dat de gemeente Zutphen zorgvuldig en vertrouwelijk met hun persoonsgegevens omgaat.

Geldigheidsduur
Dit beleid is in 2025 vastgesteld door de raad, als kaderstellend bestuursorgaan, en door de raad, het college van burgemeester en wethouders en de burgemeester, ieder voor zijn eigen bevoegdheid, als verwerkingsverantwoordelijke voor de (persoons)gegevensverwerking, binnen
(een deel van) de gemeente. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Als daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's kan het college besluiten tot een tussentijdse herziening.

2 Visie en doelstelling gemeente Zutphen

Visie
De gemeente Zutphen respecteert de privacy van natuurlijke personen, zoals inwoners, ondernemers en medewerkers, en bouwt, door het zorgvuldig omgaan met persoonsgegevens, aan maatschappelijk vertrouwen en draagvlak.

Doelstelling

Dit privacybeleid, geeft handvatten voor het beantwoorden van vragen op het gebied van privacy. Er wordt onder meer aandacht besteed aan:
- het verwerken van persoonsgegevens in het algemeen, waaronder het borgen van een zorgvuldige verwerking;
- datalekken, en
- de rechten van burgers/ inwoners en medewerkers.

Privacybeleid is niet zozeer een extra last; het biedt ook voordelen. Door de bescherming van de persoonsgegevens te borgen in de werkprocessen:
- beschermt het college zijn inwoners tegen risico's van de informatiemaatschappij;
- beheerst het college gemeentelijke afbreuk- en aansprakelijkheidsrisico's;
- bevordert het college de kwaliteit, continuïteit, veiligheid en klantgerichtheid van de gemeentelijke administratieve organisatie;
- bouwt het college aan maatschappelijk vertrouwen en draagvlak;
- respecteert de gemeente Zutphen de privacy;
- kan het college met vertrouwen verantwoording afleggen aan de raad en, in voorkomende gevallen, de Autoriteit Persoonsgegevens of de rechter.

Reikwijdte
Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente Zutphen en haar bestuursorganen waarin persoonsgegevens worden verwerkt.

3 Wettelijke uitgangspunten voor gegevensverwerking

De uitgangspunten met betrekking tot de omgang van persoonsgegevens volgens de AVG zijn:
1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

   Als een beoogde verdere verwerking onverenigbaar is met het oorspronkelijke verwerkingsdoeleind, mag deze verder verwerking toch plaatsvinden als:
   a. de betrokkene zijn toestemming heeft gegeven;
   b. of als de verwerking gebaseerd is op een wettelijke verplichting;
   c. of een taak van algemeen belang.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: wettelijke verplichting, taak van algemeen belang of uitvoering van openbaar gezag, uitvoering overeenkomst, vitaal belang of gerechtvaardigd belang. Toestemming kan ook, maar moet echt worden gezien als 'restrechtsgrond', die alleen gebruikt mag worden als geen van de andere grondslagen van toepassing is. Toestemming moet wel vrijelijk gegeven zijn. Deze grondslag is vanwege de machtsverhouding tussen overheid en inwoners daarom praktisch moeilijk te hanteren.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt (proportionaliteit). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer worden bewaard dan noodzakelijk of wettelijk vereist.
4. **Behoorlijk en transparant**: de verwerking van persoonsgegevens moet in het belang zijn van de persoon over wie de gegevens gaan. Dit houdt in dat de verwerking eerlijk en in overeenstemming met de redelijke verwachtingen van de betrokkenen moet plaatsvinden. De gemeente informeert betrokkenen hierbij op een transparante wijze over de verwerking van hun persoonsgegevens, inclusief de doeleinden, de rechtsgrondslag en met wie de gegevens worden gedeeld. Deze informatievoorziening vindt ongevraagd plaats.
5. **Rechten van betrokkenen**: betrokkenen hebben:
   a. Het recht op inzage
   b. Het recht op rectificatie en aanvulling
   c. Het recht op vergetelheid
   d. Het recht op dataportabiliteit (ook wel gegevensoverdraagbaarheid)
   e. Het recht op beperking van de verwerking
   f. Het recht om bezwaar te maken.

6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
7. **Vertrouwelijkheid**: er zijn passende organisatorische en technische beveiligingsmaatregelen getroffen zodat een passende beveiliging van de verwerking van persoonsgegevens is gegarandeerd.

Persoonsgegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

8. **Verantwoording**: onder de verantwoordelijkheid van zowel het college van burgemeester en wethouders als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. Het gemeentebestuur stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.
9. **Verantwoordingsplicht**: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze uitgangspunten (beginselen) en kan dit aantonen.
10. **Gegevens worden op tijd vernietigd**: de gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.
11. **Privacy by Design en Privacy by Default**: de gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.
12. **Samenwerking**: de gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

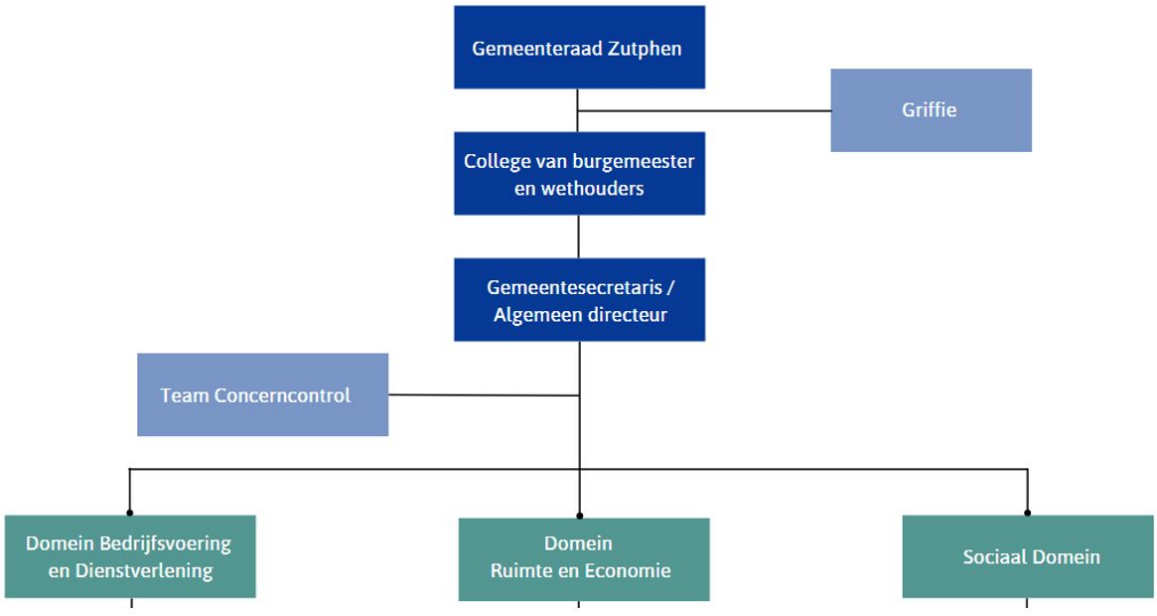
    Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids-) organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.
13. **Doorgifte buiten de EER**: doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.
14. **Geschillenbeslechting**: als de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen via de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.
15. **Register van Verwerking**: de gemeente beschikt over een actueel Register van Verwerking, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.
16. **Data Privacy Impact Assessments**: als een verwerking mogelijk een hoog risico inhoudt voor de persoonlijke levenssfeer van de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een DPIA uit (zie bijlage 1). Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.
17. **Functionaris Gegevensbescherming**: de gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Wij zijn daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het college van burgemeester en wethouders van zijn werkzaamheden, bevindingen en aanbevelingen.
18. **Plan-Do-Check-Act (PDCA) cyclus**: de gemeente dient rondom de verwerking van persoonsgegevens 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. 'In control' betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van

de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

19. **Borgingsproduct**: daarnaast gebruikt de gemeente het borgingsproduct van de Vereniging Nederlandse Gemeenten (VNG) als het beoordelingskader voor het waarborgen van AVG compliance binnen de gemeente. Het borgingsproduct is een normenkader om de effectiviteit van ons Privacybeleid te evalueren en ervoor te zorgen dat de gemeente voldoet aan de geldende wet- en regelgeving. De gemeente past het beleid en d procedures aan op basis van de bevindingen van deze beoordelingen.
20. **Bewustwording**: beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de bestuurlijke en ambtelijke organisatie binnen de gemeente voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere bestuurder en medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.
21. **Externe certificeringen**: de BIO is gebaseerd op de internationaal geaccepteerde standaarden ISO 27001 en de ISO 27002. De gedachte hierbij is dat het hanteren van deze internationaal geaccepteerde standaarden de afstemming van de informatiebeveiligings-behoefte met externe leveranciers meestal vergemakkelijkt.

    Ondanks dat het gesprek met leveranciers eenvoudiger is, kan het in sommige gevallen juist onduidelijkheid scheppen of in een concreet geval de BIO of de ISO 27001 (in zijn geheel) of slechts een subset van één van beide zou moeten gelden voor leveranciers. Ook geeft het soms enig ongemak wanneer aan leveranciers een ISO-certificering als verplichting gevraagd wordt en overheidsorganisaties zichzelf dit dan weer niet opleggen als verplichting. Ook hier wordt, net als eerder, het punt naar voren gebracht dat wellicht een ISO-certificering met een BIO als addendum met aanvullende maatregelen wellicht passender is. Dit heeft als bijkomend voordeel dat het onderhoud van de BIO lichter en eenvoudiger wordt, omdat organisaties zich nu eenmaal moet aanpassen aan vernieuwingen van de ISO-standaard bij certificering.

4 Governance en organisatorische borging



4.1 Inleiding

De gemeente Zutphen heeft een Functionaris Gegevensbescherming en een Privacy Officer aangesteld. Deze zijn beide werkzaam binnen het team Concerncontrol, welke als staf hangt boven de domeinen.

Om goed te kunnen voldoen aan de AVG, is het noodzakelijk dat er, naast de Privacy Officer, ook in de verschillende teams Privacy ambassadeurs (PA) worden aangesteld. De PA's bieden advies en ondersteuning vanuit de teams aan de organisatie op het gebied van privacy en gegevensbescherming, en werken nauw samen met de Privacy Officer (PO). De PA is meewerkend voorman en ondersteunt de vakinhoudelijke teams en teammanagers bij de naleving van de AVG en andere privacywetgeving.

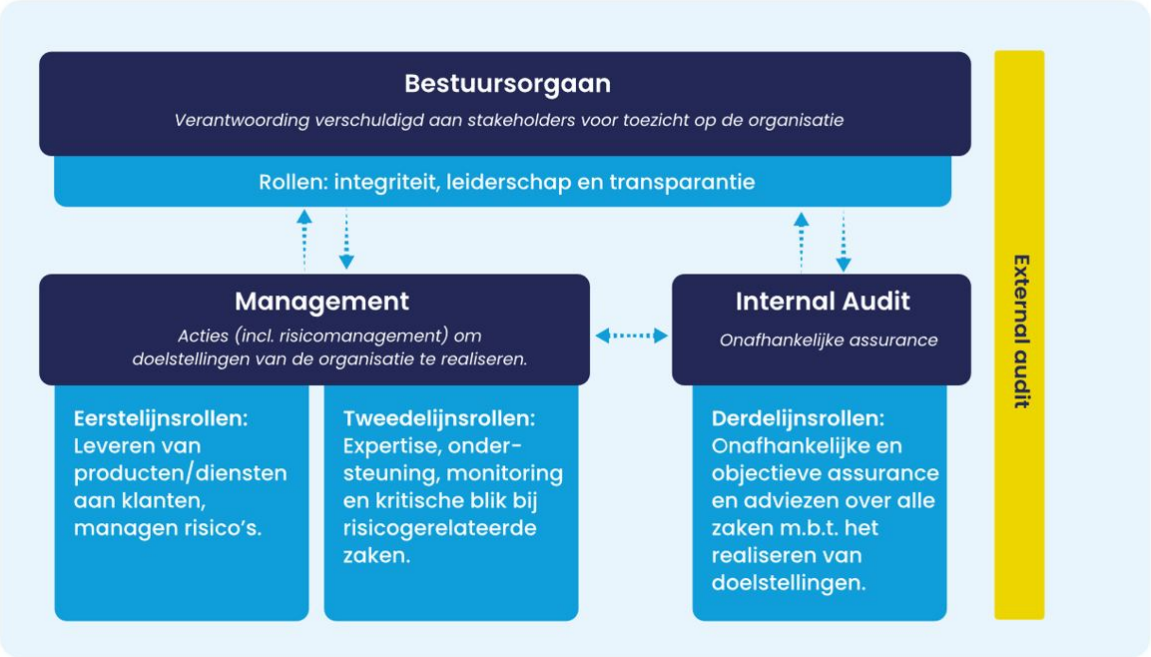
Naast tijd hebben zij ook een mandaat, aandacht en opleiding nodig. PA is een extra rol van een aantal medewerkers naast hun normale functie. Er is hiervoor nog geen concrete taakomschrijving of tijdsinvulling voor opgesteld.

In het kader van de Wpg kan de bovengenoemde privacy organisatie inclusief functionarissen die betrokken zijn bij de AVG worden gehandhaafd bij de gegevensverwerking voor de Wpg. Dit heeft geen invloed op de structuur, maar er dient wel tijd, geld en energie te worden gestoken in de opbouw van kennis en kunde op het gebied van de Wpg.

4.2 Rollen en verantwoordelijkheden

Zie bijlage 2.

4.3 Three lines Model



Het nieuwe Three Lines Model (3LM) is de opvolger van het Three Lines of Defence (3LOD) model dat wereldwijd als standaard wordt gezien voor risicomanagement. Met dit model wordt een organisatie op een bepaalde manier ingericht zodat de buitenwereld kan zien dat de organisatie 'in control' is. Hierbij zijn de beschreven functies niet alleen bedoeld om waarde van de organisatie te beschermen, maar ook om deze te vergroten. Het 3LM legt ook sterker een koppeling met de doelstellingen van de organisatie.

Centraal voor alle functies staan dus de doelen van de organisatie. De functies zijn geen silo's, maar stemmen af en werken samen; ieder vanuit de eigen rol. De inrichting van het model moet worden afgestemd op de risico's en specifieke situatie van de organisatie.

De drie lijnen op een rijtje

De business (1st line): Deze groep is eindverantwoordelijk voor de keuzes die worden gemaakt en de risico's die in de dagelijkse praktijk worden genomen.

Controle (2nd line): Deze groep ontwikkelt de control systemen voor een goed proces van risicomanagement en beheersing, altijd ter ondersteuning en advies aan de eerste lijn.

Internal audit (3rd line): Deze groep voorziet de hoogste leiding van zekerheid (assurance) over de kwaliteit van sturing en beheersing op het gebied van beveiligings- en privacymaatregelen binnen de organisatie.

De sleutel tot het functioneren van het Three Lines Model

Binnen het 3-lines model is het management (de eerste lijn) het meeste in staat om risico's te managen en 'in control' te zijn. De internal audit, als derde lijn, dient erop toe te zien dat de beheersmaatregelen

en in controls daadwerkelijk operationeel zijn. De FG houdt hier toezicht op. De tweede lijn heeft een belangrijke rol om de eerste lijn te faciliteren met deze verantwoordelijkheden en te controleren of dit ook daadwerkelijk gebeurt.

Een goede coördinatie van de tweede lijn werkzaamheden is de sleutel tot het daadwerkelijk effectief functioneren van het Three Lines Model. Door een integrale risk based samenwerking te hebben, kan de directie de assurance verkrijgen dat men 'in control' is. Zie ook 'Governance van de Informatiebeveiliging 2024'.

De invoering van het Three Lines Model zal de komende maanden worden gespecificeerd en in de Informatie Beveiliging en Privacy (IB&P) planning worden opgenomen.

4.4 RASCI Model

In 2025 zal het RASCI model worden geïmplementeerd, dat de onderlinge verantwoordelijkheden en rollen op het gebied van privacy en informatiebeveiliging binnen de gemeente Zutphen duidt. Het toebedelen van deze rollen of verantwoordelijkheden is een taak van de proceseigenaar. Hierbij worden volgende rollen onderscheiden:

Responsible is diegene die verantwoordelijk is dat een taak of handeling gedaan wordt
Accountable is de eindverantwoordelijke voor het (deel)proces
Consulted zijn diegenen die voor een definitieve beslissing moeten worden geraadpleegd
Informed zijn diegenen die geïnformeerd worden over een genomen beslissing

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Teammanagers en Domein Directeuren • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het college van burgemeester en wethouders
C	Consulted/ Adviserend	• Privacy Officer • CISO/ISO • Functionaris Gegevensbescherming • Privacy Ambassadeurs
I	Informerend/ Geïnformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Voor de overzichtelijkheid en de eenvoud hier bovenstaand de beknopte RASCI tabel. Voor uitgebreide RASCI tabel zie bijlage 5.

5 Wet- en regelgeving

Zie voor wet- en regelgeving bijlage 3.
Zie voor aankomende wet- en regelgeving bijlage 4.

6 Verwerkingen van persoonsgegevens

Er zijn diverse beleidsonderwerpen waar verwerking van persoonsgegevens aan de orde is. Zonder uitputtend te willen zijn worden hier de belangrijkste beleidsvelden vermeld:

- Bedrijfsvoering en Dienstverlening: dienstverlening aan inwoners, bedrijven en instellingen
- Sociaal domein: uitvoering Participatiewet en aanverwante uitkeringen, Wet maatschappelijke ondersteuning, Jeugdwet en onderwijswetten (inclusief leerlingenvervoer)
- Domein Ruimte en Economie: Omgevingswet
- Verzoeken om informatie van inwoners, bedrijven en instellingen (al dan niet gebaseerd op de Wet open overheid)
- Personeelszaken

6.1 PERSOONSGEGEVENS

De AVG onderscheidt drie typen van persoonsgegevens (gewone, bijzondere en strafrechtelijke persoonsgegevens) en stelt verschillende eisen aan een rechtmatige gegevensverwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Als bijzondere persoonsgegevens, gevoelige persoonsgegevens, unieke identificerende kenmerken, BSN-nummers of andere gegevens verwerkt worden waarvoor geldt dat sprake is van een verhoogde gevoeligheid, betekent dit een verhoogd risico op misbruik. Dat heeft een (potentieel grote) impact op de betrokkene en vraagt daarmee om betere beveiliging. Het verwerken van deze persoonsgegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden. Ook geldt dat het risico bestaat dat betrokkenen minder snel willen meewerken, of het vertrouwen in de gemeente vermindert. Er wordt dan ook geadviseerd om andere minder ingrijpende persoonsgegevens te gebruiken. Bovendien loopt de gemeente compliance risico's als dit het geval is.

Strafrechtelijke persoonsgegevens

Persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor verwerkingsdoeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een Burgerservicenummer (BSN), BIG-nummer (Beroepen in de Individuele Gezondheidszorg), A-nummer (administratienummer basisregistratie personen), onderwijsnummer, strafrechtketennummer (SKN) en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoon identificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die geen bijzondere of strafrechtelijke persoonsgegevens zijn worden aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/ of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits-)fraude;
- communicatie- en locatiegegevens.

Een belangrijke vraag die steeds gesteld moet worden is of het doel met minder ingrijpende (andere) persoonsgegevens kan worden bereikt. Als dit niet mogelijk is, moet gekeken worden of de persoonsgegevens kunnen worden geanonimiseerd of pseudo-anoniem kunnen worden gemaakt. Hierdoor kan het nemen van verdere maatregelen ter bescherming van de privacy van de betrokkenen worden geminimaliseerd. Er wordt wel geadviseerd om periodiek na te gaan of de persoonsgegevens niet indirect herleidbaar zijn. Geanonimiseerde persoonsgegevens zijn niet te herleiden naar een specifiek persoon en vallen daarmee dus niet onder de AVG.

6.2 VOORWAARDEN VOOR VERWERKING

Hoofdregel is dat persoonsgegevens alleen *in overeenstemming met de wet* en op *behoorlijke* en *zorgvuldige wijze* worden *verwerkt*. Dit noemen we rechtmatigheid.
Daarnaast mogen persoonsgegevens slechts verzameld worden als daarvoor een precieze doelomschrijving wordt gegeven. Bovendien bepaalt de wet dat persoonsgegevens slechts mogen worden verwerkt voor zover zij *toereikend, ter zake dienend* en *niet bovenmatig* zijn. Dit noemen we proportionaliteit.

De betrokkene heeft ook *recht op informatie* als er persoonsgegevens van hem worden verwerkt. Degene die persoonsgegevens vraagt moet hem onder andere laten weten wie hij is en wat voor gegevens hij waarvoor verwerkt. Dit noemen we transparantie.
Behalve bovenvermelde algemene regels geldt dat er voor elke verwerking van persoonsgegevens een grondslag aanwezig moet zijn.

In het merendeel van de gevallen verstrekt de betrokkene de persoonsgegevens zelf. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd. Denk hierbij aan: persoonsgegevens, adresgegevens, bedrijfsgegevens, inkomensgegevens, gezinssamenstelling, uitkeringen, onderwijsgegevens, zorgindicaties, etc. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid en de gemeente wordt voorgestaan. Als voor het uitvoeren van bepaalde wettelijke taken en/ of wet- en regelgeving persoonsgegevens verwerkt moeten worden, dan worden deze gegevens opgevraagd uit de basisregistratie personen (zie artikel 1.7 Wet BRP).

Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van de taak. Gegevens worden niet zonder wettelijke grondslag gedeeld.

Bijzondere gegevens worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak en/ of wet- en regelgeving. Zo kunnen op grond van de Wet maatschappelijke ondersteuning en/ of Jeugdwet medische- en gezondheidsgegevens worden gebruikt bij de behandeling van een ondersteuningsverzoek of een hulpvraag.

6.3 BEWAARTERMIJN GEGEVENS

De AVG heeft als uitgangspunt dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is (beperkte bewaartermijn). Met andere woorden: als het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Hierop maakt de AVG een uitzondering als de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische verwerkingsdoeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij gegevensverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Als geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de persoonsgegevens periodiek toetsen aan het uitgangspunt van opslagbeperking. Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de eerder genoemde Archiefwet.

Gemeenten zijn wettelijk gehouden aan de bewaartermijnen van de 'Selectielijst gemeentelijke en intergemeentelijke organen'. In deze selectielijst wordt onder andere aangegeven dat gemeenten persoonsgegevens langer mogen bewaren dan de vastgestelde bewaartermijn als dat noodzakelijk is voor een zorgvuldige uitvoering van hun taken op grond van de wet waarop dit van toepassing is. Het betreft met name resultaten waarbij zorg voor meerdere jaren wordt verleend aan jeugdigen van 0 tot 19 jaar. Dit houdt in dat zaken die betrekking hebben op de betrokken resultaten, altijd aan de proceseigenaren of behandelde ambtenaren zullen moeten worden voorgelegd, voordat tot vernietiging van de archiefbescheiden van deze zaken wordt overgegaan.

6.4 UITGANGSPUNTEN

Het wettelijk kader, zoals hiervoor beschreven, is bepalend bij het formuleren van de uitgangspunten van beleid. Het privacybeleid is gestoeld op de volgende beleidsuitgangspunten:

- Wij verwerken alleen gegevens van en over inwoners/ medewerkers die strikt noodzakelijk zijn voor het uitvoeren van gemeentelijke taken;

- Wij informeren inwoners/ medewerkers over de verwerking van persoonsgegevens;
- Wij bewaren gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en vernietigen deze daarna;
- Wij gaan terughoudend om met informatie van en over inwoners/ medewerkers; medewerkers worden daarover geïnstrueerd;
- Wij gaan bij handhaving terughoudend om met informatie van en over inwoners;
- Wij delen persoonsgegevens intern en extern alleen voor zover dat strikt noodzakelijk is voor de taakuitvoering;
- Wij zorgen ervoor dat persoonsgegevens niet voorkomen in openbare verslagen;
- Als wij gegevens openbaren als gevolg van een WOO-verzoek, dan stellen wij alles in het werk om gegevens van inwoners te anonimiseren;
- Als wij zelf wettelijk gegevens openbaar moeten maken, dan wordt aan betrokkenen eerst om toestemming voor openbaarmaking gevraagd en wordt gegevensverstrekking tot een minimum beperkt;
- Als wij gegevens ter inzage leggen, dan wordt van betrokkenen de gegevensverstrekking tot een minimum beperkt;
- Wij dragen zorg voor het goed uitvoeren van het privacybeleid door medewerkers en samenwerkende instanties;
- Wij voeren toezicht uit op het privacybeleid en de uitvoering ervan;
- Hoe met privacy wordt omgegaan en hoe de privacy te allen tijde wordt geborgd, maken wij op een transparante manier duidelijk;
- Daar waar sprake is van verwerking van persoonsgegevens worden werkwijzen vastgelegd en op zorgvuldige wijze uitgevoerd conform protocollen of procesbeschrijvingen;
- Wij handelen klachten en bezwaren van inwoners/ medewerkers, ondernemers, organisaties en instellingen over privacy aspecten op een toegankelijke, laagdrempelige wijze af;
- Bij samenwerking met externe partners, waar sprake is van verwerking van persoonsgegevens, maken wij afspraken over de voorwaarden voor een zorgvuldige verwerking en de controle daarop.

6.5 NALEVING VAN HET BELEID

Vanuit de gedachte van risicobeheersing, neemt het college van burgemeester en wethouders verschillende maatregelen om de risico's bij de verwerking van persoonsgegevens in kaart te brengen en te verminderen.
Hiervoor gelden vier cycli van risicobeheersing:

- In kaart brengen verwerkingen met persoonsgegevens;
- Uitvoeren DPIA, evaluatie van getroffen maatregelen, of formuleren van aanvullende maatregelen;
- Afleggen verantwoording aan toezichthoudende FG;
- Periodiek evalueren van privacy incidenten.

6.6 DATA PRIVACY IMPACT ASSESSMENT (DPIA)

Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt. Betrokkenen kunnen ervan uitgaan dat persoonsgegevens, door het nemen van passende technische en organisatorische maatregelen, op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is. En dat zij daarmee onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige gegevensverwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Wat een DPIA inhoudt en wanneer van toepassing: zie bijlage 1.

Als niet aan de eisen van de DPIA wordt voldaan, kan dat onder de AVG tot gevolg hebben dat de bevoegde toezichthoudende autoriteit boetes oplegt. Als geen DPIA wordt uitgevoerd terwijl dat voor de gegevensverwerking wel verplicht is, als een DPIA niet correct wordt uitgevoerd, of als de Autoriteit Persoonsgegevens (AP) niet wordt geraadpleegd terwijl dat wel vereist is, kan dat leiden tot een administratieve boete van maximaal 10 miljoen euro.

6.7 DATALEKKEN

De procedure Datalekken beschrijft hoe te handelen, als er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing, als het datalek bij een derde is ontstaan, bijvoorbeeld een verwerker van persoonsgegevens.
Per gemeld datalek behoudt de verwerkingsverantwoordelijke (het college van burgemeester en wethouders of de burgemeester) de vrijheid te beoordelen of de procedure gevolgd moet worden, of dat afwijking van de procedure Datalekken gerechtvaardigd is. Daarin behoort het advies van zowel de CISO als ook de PO en FG wel zwaarwegend te zijn en dient er onderbouwd te worden waarom er wordt afgeweken van de adviezen van de PO/ FG/ CISO.

6.8 TOEZICHT

Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn.

De verantwoordelijke en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken de FG desgevraagd alle inlichtingen en verlenen de FG alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.

- De FG heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt.
- De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.
- De FG brengt verslag uit over zijn bevindingen aan het college van burgemeester en wethouders.
- Hij geeft aanbevelingen over te nemen maatregelen, die een goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen.
- De FG kan niet ontslagen worden of een sanctie krijgen als gevolg van de uitoefening van zijn FG taken, zoals deze blijken uit artikel 38 AVG.

6.9 REGISTER VAN VERWERKING

De FG houdt toezicht op het register waarin verwerkingen van persoonsgegevens zijn vermeld. Het register vermeldt ten minste de volgende elementen:

- de verantwoordelijke;
- de PO;
- omschrijving van de verwerking;
- doel(en) van de verwerking;
- grondslag(en) van de verwerking;
- welke gegevens of categorieën van gegevens worden verwerkt;
- ontvangers of categorieën van ontvangers aan wie gegevens worden verstrekt;
- doorgifte van gegevens naar landen buiten de EU;
- de bewaartermijn.

Het register wordt ingericht en onderhouden door de PO. De proceseigenaar is verantwoordelijk voor de juiste inhoud.

6.10 RECHTEN VAN BETROKKENE

Namens de verwerkingsverantwoordelijke voeren de teammanagers of proceseigenaren de taken uit met betrekking tot de rechten van betrokkene, zoals omschreven in de AVG. De gemeente heeft de rechten van de betrokkenen opgenomen in de privacyverklaring op de website. Het gaat bij de rechten van de betrokkenen om de volgende rechten:

- Het recht op **vergetelheid**: het recht om ‘vergeten’ te worden als de betrokkene daarom vraagt en er geen wettelijke verplichtingen en/ of geen wettelijke grondslagen (meer) zijn en dat de persoonsgegevens ook niet meer nodig zijn voor het doel waarvoor de organisatie de gegevens heeft verzameld.
- Het recht op **inzage**.
- Het recht op **rectificatie en aanvulling**: het recht om de persoonsgegevens die worden verwerkt te wijzigen.
- Het recht op **beperking van de verwerking**: het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot **geautomatiseerde besluitvorming en profilering**.
- Het recht om **bezwaar** te maken tegen de gegevensverwerking.
- Het recht op **data portabiliteit**: het recht om persoonsgegevens over te dragen.

6.11 BORGING EN BORGINGSPRODUCTEN

De hoofddoelstelling voor het borgen en het hanteren van AVG Borgingsproducten is het geven van een eenduidige baseline voor wat de gemeente moet doen om aan de AVG te voldoen. Een belangrijk uitgangspunt hierbij is dat iedere burger recht heeft op een gelijk basisniveau van privacybescherming, ongeacht in welke gemeente deze burger woont. Verschillen mogen zich hooguit voordoen in de mate waarin gemeenten (of andere gemeentelijke organisaties) zaken optimaliseren.

Opbouw van het Borgingsproduct

Het Borgingsproduct is, net als eerdere versies, opgebouwd uit een zevental thema's waarop getoetst wordt. Een thema gaat over een specifiek onderdeel van de AVG. De AVG-hoofdstukken zijn niet aangehouden, omdat de (volgorde van de) thema’s beter aansluiten bij de gemeentelijke praktijk. De thema’s zijn:

Beleid: De organisatie heeft processen en bijbehorende verantwoordelijkheden en risico's in kaart gebracht en vastgelegd in beleidsstukken. Deze stukken moeten voor alle werknemers goed vindbaar en begrijpelijk zijn.

Processen: De organisatie heeft alle processen waarbinnen persoonsgegevens worden verwerkt in kaart gebracht. De beschrijving van deze processen wordt actueel gehouden, werkinstructies worden nageleefd en processen met een hoog risico worden getoetst op juistheid.

Organisatorische inbedding: De organisatie heeft een FG aangesteld en kan zich voor inhoudelijke vraagstukken tot de PO richten. Er wordt doorlopend aan bewustwording gedaan.

Rechten van betrokkenen: De organisatie voldoet aan alle wettelijke eisen die er zijn op het gebied van rechten van betrokkenen. De organisatie is transparant over hoe en welke persoonsgegevens verwerkt worden.

Samenwerking: De organisatie heeft in kaart gebracht met wie zij samenwerkt en heeft daarbij passende afspraken gemaakt. Deze afspraken worden door de betrokken partijen nageleefd.

Gegevensbescherming: Hoewel pas echt een volledig beeld kan worden geschetst van de stand van zaken op het gebied van gegevensbescherming middels de Baseline Informatiebeveiliging Overheid (BIO), zijn privacy en informatiebeveiligingsaspecten niet geheel van elkaar los te trekken. Een aantal informatiebeveiligingsaspecten met een duidelijke privacy component zijn dan ook in dit Borgingsproduct opgenomen. Denk bijvoorbeeld aan de handelswijze bij datalekken. De (C)ISO kan helpen bij het beoordelen van de mate waarin aan de bij dit thema opgenomen maatregelen wordt voldaan. Wanneer deze maatregelen voldoende zijn geïmplementeerd, houdt dat dus niet automatisch in dat de organisatie volledig aan de BIO voldoet.

7 Informatie Beveiliging

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

De gemeente is zich bewust van het cruciale belang van de beveiliging van persoonsgegevens voor de betrokkene (inwoners van de gemeenten en ook de medewerkers). Persoonsgegevens van de betrokkenen zijn beveiligd met adequate organisatorische en technische middelen die zijn vastgelegd in het Securitybeleid. Een passend beveiligingsniveau is conform artikel 32 AVG afgestemd op het risico dat de verwerking met zich meebrengt.

7.1 RISICO'S VOOR BETROKKENEN

Met name de beveiligingsincidenten brengen de risico's voor betrokkenen aan het licht. In de meeste gevallen loopt de inwoner of werknemer een risico op schade. Voorkomende risico's zijn:

1. **Reputatieschade**

Als gevoelige gegevens van een persoon bij een bekende of collega terechtkomen, kan die persoon reputatieschade oplopen doordat een bekende of collega meer van zijn privésituatie afweet dan hij zou willen.

2. **Identiteitsfraude**

Met onrechtmatig verkregen documenten kan een kwaadwillend persoon identiteitsfraude plegen en zich voordoen als betrokkene.

3. **Gevoel controle over data te verliezen**

Met de AVG is de controle van betrokkenen op hun gegevens vergroot. Met de ontwikkeling van digitale systemen waren er signalen dat bewoners soms moeite hebben om hun gegevens in te vullen omdat voor hen niet duidelijk was waar gegevens terecht zouden komen. Concrete en transparante toelichting over wat met verzamelde gegevens wordt gedaan helpt het vertrouwen te verhogen.

7.2 RISICO'S VOOR GEMEENTE

Risico's voor de gemeente staan los van de risico's voor de betrokkenen, maar moeten in een DPIA worden meegenomen om de urgentie van voorgestelde maatregelen duidelijk te maken.

1. **Minder succesvolle dienstverlening**

Met name datalekken van bijzondere persoonsgegevens zorgen voor verminderd vertrouwen in de dienstverlening.

2. **Imagoschade**

Slordigheden waarbij inwoners of medewerkers de ontvanger van onjuiste gegevens zijn, kunnen leiden tot het idee dat de gemeente niet professioneel handelt en daarmee tot imagoschade kan leiden. Ook in onderhandelingen met samenwerkingspartners staat de gemeente sterker in zijn schoenen als een professioneel niveau van privacybescherming wordt nagevolgd en afgesproken.

3. **Datakwaliteit**

Datakwaliteit heeft betrekking op de mate van geschiktheid van data voor het uiteindelijke gebruiksdoel. Het is daarom van groot belang dat de gemeente beschikt over betrouwbare en kwalitatief hoogwaardige data. Alleen dan is de gemeente in staat om slagvaardig en succesvol te handelen. Organisaties waarbij de data niet op orde is, ondervinden daar beperkingen van. Zo kunnen diverse activiteiten hun effect missen als deze op verkeerde inzichten gebaseerd zijn. Ook verlopen interacties met inwoners minder gemakkelijk als blijkt dat de database fouten bevat. Organisaties die de kwaliteit van hun data niet kunnen garanderen, lopen bovendien extra risico's met het naleven van hun wettelijke verplichtingen zoals de AVG. De kwaliteit van data kan uitgedrukt worden in een combinatie van de begrippen volledigheid, accuratesse, uniciteit, validiteit, tijdigheid en consistentie.

Van een gedigitaliseerde organisatie mag worden verwacht dat de kwaliteit van data is geborgd door:
- Het eigenaarschap en de verantwoordelijkheid voor data is expliciet belegd en de eindverantwoordelijke van een organisatie erkent het belang van datakwaliteit.
- Het borgen van de datakwaliteit door datakwaliteitseisen, data-definities, data govenance, datastromen en het in kaart te brengen van de relatie tot de informatiebehoefte.
- Duidelijke afspraken maken over de wijze waarop datakwaliteit wordt gemonitord en beheerd.

4. **Dataclassificatie**

Dataclassificatie heeft als doel richting te geven aan de passende technische en organisatorische maatregelen. Als gemeente beschikken we over veel (persoons)gegevens. Om te bepalen welke gegevens in meer of mindere mate beschermd moeten worden, kun je de gegevens classificeren. Binnen de BIO wordt de controle 'classificatie van informatie' genoemd (8.2). De overheidsmaatregel die binnen deze controle valt (8.2.1.1) vereist dat alle informatie (BBN1) in alle informatiesystemen door middel van een expliciete risicoafweging is geclassificeerd.
Zo moet je zeer gevoelige gegevens (zoals persoonsgegevens) beter beschermen dan reeds bekende gegevens (zoals openbare jaarrapporten). Kortom, een hogere classificatie betekent meer technische en/ of organisatorische maatregelen.

5. **Tijdverlies**

Bij een beveiligingsincident zijn vaak meerdere teams betrokken om de schade te herstellen. Diverse medewerkers van verschillende teams en bestuurders zijn druk met het oplossen van een beveiligingsincident. Dit tijdverlies kan beter proactief worden gebruikt om een gedegen datakwalificatie uit te voeren.

Bijlage 1: Gegevensbeschermingseffectbeoordeling

1. Wat is een gegevensbeschermingseffectbeoordeling (DPIA)

Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt. Betrokkenen kunnen ervan uitgaan dat persoonsgegevens, door het nemen van passende technische en organisatorische maatregelen, op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is. En dat zij daarmee onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige gegevensverwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

- Een DPIA is een belangrijk verantwoordingsinstrument. Het helpt verwerkingsverantwoordelijken om aan de eisen van de AVG te voldoen, en om aan te tonen dat passende maatregelen zijn genomen om ervoor te zorgen dat de AVG wordt nageleefd. Met andere woorden: een DPIA is een proces voor het realiseren en aantonen van naleving.
- Een DPIA moet voorafgaand aan de verwerking en bij bestaande verwerkingen, waar sprake is van een gegevensverwerking die een hoog privacyrisico oplevert voor de betrokkenen. Tevens heeft de AP nog een lijst samengesteld voor verwerkingen waarbij een DPIA altijd verplicht is. Zie hieronder punt 3. (Specifieke lijst van verwerkingen)
- Een DPIA wordt doorgaans uitgevoerd door de product/proces/project eigenaar met ondersteuning van de PO.
- Of er sprake is van een hoog privacyrisico, toetst de gemeente aan de hand van een Business Impact Assessment (BIA). De BIA wordt uitgevoerd op het moment dat een van de BIV-classificaties 2 of hoger scoort. Dus naast de Vertrouwelijkheid, waar privacy geraakt wordt, ook op Beschikbaarheid en Integriteit.
- Op grond van de AVG is verder in ieder geval sprake van een hoog privacyrisico als de gemeente:
  a. Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
  b. Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied. (Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;

- Een DPIA moet in ieder geval het volgende bevatten:
  a. Een systematische beschrijving van de beoogde gegevensverwerkingen.
  b. Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen.
  c. Een beoordeling van de privacyrisico's voor de betrokkenen.
  d. De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat aan de AVG wordt voldaan.

- Na afronding van de DPIA moet de beschreven verwerking worden opgenomen in het Register van Verwerking.
- De opdrachtgever voor een DPIA moet dit weloverwogen te doen in verband met kosten, uitvoering , inhuur, etc.

Als niet aan de eisen van de DPIA wordt voldaan, kan dat onder de AVG tot gevolg hebben dat de bevoegde toezichthoudende autoriteit boetes oplegt. Als geen DPIA wordt uitgevoerd terwijl dat voor de gegevensverwerking wel verplicht is, als een DPIA niet correct wordt uitgevoerd, of als de Autoriteit Persoonsgegevens (AP) niet wordt geraadpleegd terwijl dat wel vereist is, kan dat leiden tot een administratieve boete van maximaal 10 miljoen euro.

2. Richtsnoer

De European Data Protection Board heeft op 4 oktober 2017 de Richtsnoeren voor gegevensbeschermingseffectbeoordeling (DPIA) en Bepaling of een verwerking die waarschijnlijk een hoog risico inhoudt, vastgesteld. In deze Richtsnoeren staan negen criteria vermeld die in aanmerking moeten worden genomen bij de beoordeling of een DPIA moet worden uitgevoerd, te weten in het geval dat sprake is van:

1. Evaluatie of scoretoekenning
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg
3. Stelselmatige monitoring
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard
5. Op grote schaal verwerkte gegevens
6. Matching of samenvoeging van datasets
7. Gegevens met betrekking tot kwetsbare betrokkenen

8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen
9. De situatie waarin als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst

3. **Specifieke lijst van verwerkingen**

Op basis van bovenstaande Richtsnoeren heeft de Nederlandse Autoriteit Persoonsgegevens (AP) een lijst met omschrijvingen van soorten verwerkingen samengesteld waarbij het uitgangspunt is dat de verwerkingsverantwoordelijke verplicht is een DPIA uit te voeren voordat met de verwerking van persoonsgegevens wordt begonnen. **Hierbij is aangegeven welk criterium uit de bovenstaande richtsnoer in aanmerking is genomen**:

1. **Heimelijk onderzoek**

Grootschalige verwerkingen van persoonsgegevens en/ of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen (bijvoorbeeld: heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten). Een DPIA is ook verplicht in geval van heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een DPIA te worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever)). **[3], [5], [7]**

2. **Zwarte lijsten**

Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden (artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene Verordening Gegevensbescherming) (zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus). **[4], [6], [7], [8]**

3. **Fraudebestrijding**

Grootschalige verwerkingen van (bijzondere) persoonsgegevens en-of stelselmatige monitoring in het kader van fraudebestrijding (bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars). **[3], [4], [5], [9]**

4. **Creditscores**

Grootschalige gegevensverwerkingen en/ of stelselmatige monitoring die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore. **[1], [2], [3], [4], [5], [9]**

5. **Financiële situatie**

Grootschalige verwerkingen en/ of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden (bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen). **[3], [4], [5]**

6. **Genetische persoonsgegevens**

Grootschalige verwerkingen en/ of stelselmatige monitoring van genetische persoonsgegevens (bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, Bio databanken). **[3], [4], [5]**

7. **Gezondheidsgegevens**

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid (let wel: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de Algemene Verordening Gegevensbescherming

uitgezonderd van de verplichting een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren). **[4], [5], [7]**

8. **Samenwerkingsverbanden**

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen, bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten. **[6], [7], [8]**

9. **Cameratoezicht**

Grootschalige en/ of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones. **[3], [5]**

10. **Flexibel camera toezicht**

Grootschalig en/ of stelselmatig gebruik van flexibel cameratoezicht (camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten). **[3], [5]**

11. **Controle werknemers**

Grootschalige verwerking van persoonsgegevens en/ of stelselmatig monitoring van activiteiten van werknemers (bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding). **[3], [5], [7]**

12. **Locatiegegevens**

Grootschalige verwerking en/ of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen (bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer). **[3], [5]**

13. **Communicatiegegevens**

Grootschalige verwerking en/ of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker. **[3], [5]**

14. **Internet of things**

Grootschalige verwerkingen en/ of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen ('internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etcetera). **[3], [5], [8]**

15. **Profilering**

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag. **[1], [3]**

16. **Observatie en beïnvloeding van gedrag**

Grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd of beïnvloed, dan wel gegevens daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld. **[1], [5]**

17. **Biometrische gegevens**

Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren. Op grond van de Algemene Verordening Gegevensbescherming

is de verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijk persoon, in beginsel verboden. In Nederland zijn aanvullende voorwaarden gesteld in artikel 29 van de Uitvoeringswet Algemene Verordening Gegevensbescherming. Enkel als de verwerking strikt noodzakelijk is voor authenticatie of beveiligingsdoeleinden, is de verwerking van biometrische gegevens toegestaan. **[3], [5], [8]**

Bijlage 2: Rollen en verantwoordelijkheden

1. College van burgemeester en wethouders

Net zoals het college jaarlijks aan de gemeenteraad verantwoording aflegt over de gemeentelijke uitgaven en inkomsten, legt het college ook jaarlijks aan de raad verantwoording af over de uitvoering en realisatie van beleid. Naast deze jaarlijkse verantwoording, hebben het college en de burgemeester op grond van de artikelen 169 en 180, tweede lid van de Gemeentewet de algemene informatieplicht om de raad te informeren over bijzonderheden (incidenten) bij gegevensverwerkingen.

Het college van burgemeester en wethouders heeft de volgende rollen en verantwoordelijkheden:

- Bestuurlijk eindverantwoordelijk voor de naleving van alle privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt verantwoording af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacy cultuur.

2. Controle door de raad

De gemeenteraad moet controleren of het college 'in control' is bij de uitvoering van de AVG. De gemeenteraad kan daarvoor de volgende vragen stellen:

- Zijn er bij de start van een nieuw traject risico's ten aanzien van de gegevensbescherming voldoende maatregelen genomen?
- Is privacy geborgd in alle gemeentelijke processen? Zo ja, kan het college dat ook aantonen?
- Worden de instrumenten ook daadwerkelijk ingezet, zodat risico's die verbonden zijn aan de verwerking van persoonsgegevens niet hoog zijn?
- Gebruikt de gemeente het Borgingsproduct van de VNG om te monitoren wat de stand van zaken is bij de gegevensbescherming?
- Komt de FG jaarlijks langs om een toelichting op zijn jaarverslag te geven?
- Welke gegevensbeschermingsincidenten hebben zich het afgelopen jaar voorgedaan en wat heeft de gemeente daarvan geleerd?

De gemeenteraad is als bestuursorgaan een verwerkingsverantwoordelijke op grond van artikel 4, zevende lid AVG. Dit betekent dat de raad zelf verwerkingsverantwoordelijke is voor taken die specifiek bij de raad liggen en dus moet kunnen aantonen dat de verwerkingen die hij doet, voldoen aan de AVG. Daarnaast dient de raad onder andere een register van verwerkingsactiviteiten bij te houden, technische en organisatorische maatregelen te nemen om persoonsgegevens te beschermen en zal de raad wanneer er persoonsgegevens verstrekt worden aan andere partijen specifieke afspraken moeten maken.

3. Gemeentesecretaris, Domein Directeuren en Teammanagers

De gemeentesecretaris/ algemeen directeur, is als hoofd, eindverantwoordelijk voor de ambtelijke organisatie. De domein directeuren zijn eindverantwoordelijk voor hun domein.

De teammanagers zijn verantwoordelijk voor hun teams. Specifiek:
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen het eigen team;
- Informeert de FG op welke manier het eigen team compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door medewerkers binnen het eigen team;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het Register van Verwerking voor zover dit betrekking heeft op de eigen processen;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy ambassadeur, voor zover benoemd binnen het eigen team;
- Bevordert duurzame privacy cultuur;
- Betrekt PO en/ of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens (Privacy by Design).

4. Functionaris Gegevensbescherming (FG)

De FG is de vertegenwoordiger van het belang van de betrokkene. De FG heeft een adviserende taak, maar is primair degene die de organisatie tegen de AVG-meetlat moet houden. Dan past het niet om al te ver mee te denken en de belangen van de organisatie te stevig mee te laten wegen. De AVG geeft ook aan dat de FG best andere taken mag uitvoeren in de organisatie, maar dat deze niet mogen leiden

tot belangenverstrengeling. Zo is het opstellen van beleid dat ziet op de AVG of gegevensverwerkingen niet een taak die bij de FG moet worden belegd.

De taken van de FG:

- De organisatie informeren en adviseren over de AVG en Wpg verplichtingen;
- Als interne toezichthouder de naleving van de AVG en Wpg controleren, maar ook en vooral op het privacybeleid van de verwerkingsverantwoordelijke. In dit privacybeleid moet huiselijk gezegd iets staan over governance, awareness, training en audits.
- (Verplicht) adviseren bij een DPIA:
  - Adviseren over de noodzaak van een DPIA
  - Beoordelen van de DPIA
  - Toezicht houden op de uitvoering
  - Waarborgen van naleving

- Met de Autoriteit Persoonsgegevens samenwerken en optreden als hun contactpunt.
- Betrokkenen moeten in contact kunnen komen met de FG. De FG krijgt alle verzoeken binnen en coördineert de beantwoording.

Voorwaarden:

- Onafhankelijke positie: De onafhankelijkheid is vastgelegd in de wet: de AVG geeft in artikel 38 sub 3 aan dat de FG geen instructies ontvangt over de uitvoering van zijn taken.
- Hij brengt rechtstreeks verslag (jaarlijks) uit aan het college van burgemeester en wethouders. Hij kan niet én verantwoordelijk zijn voor het bedenken en uitvoeren van compliance activiteiten én onafhankelijk toezicht houden op die uitvoering.
- Omdat de FG direct aan het college van burgemeester en wethouders rapporteert is deze, anders dan Chief Information Security Officer (CISO) en PO, onafhankelijk ten opzichte van de rest van de gemeente en haar verwerkers.
- De FG kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Dat wil zeggen dat:
  - De FG geen rollen kan vervullen waarbij de FG doelen en middelen van verwerkingen bepaalt.
  - De FG geen verantwoordelijkheid kan nemen voor de naleving van de AVG en/ of de Wpg. Dat betekent -mede- dat de FG geen uitvoerende rol heeft, onder het mom van ‘de slager keurt niet zijn eigen vlees’.
  - Het betekent ook dat de verantwoordelijkheid voor de correcte naleving bij de verantwoordelijke teammanagers ligt en de ambtelijke eindverantwoordelijkheid bij de gemeentesecretaris/ algemeen directeur voor het geheel en de domein directeuren voor het eigen domein. De uiteindelijk bestuurlijke eindverantwoordelijkheid ligt bij het college van burgemeester en wethouders.

- De FG wordt regelmatig uitgenodigd om vergaderingen van de directie en de teammanagers bij te wonen, zeker wanneer beslissingen worden genomen die gevolgen hebben voor de Privacy.
- Het is belangrijk dat de FG als een gesprekspartner binnen de organisatie wordt gezien en dat hij/zij deel uitmaakt van de relevante werkgroepen die zich met gegevensverwerking binnen de organisatie bezighouden.
- De organisatie moet zorgen dat de FG "naar behoren en tijdig (lees: zo vroeg mogelijk) wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens". Het is in ieder geval verplicht om dit bij de volgende aangelegenheden te doen: bij de uitvoering van een DPIA moet altijd verplicht advies worden gevraagd aan de FG. Daarnaast moet de FG meteen geconsulteerd worden zodra zich een beveiligingsincident voordoet dat leidt of kan leiden tot een datalek.
- Alle relevante informatie moet tijdig aan de FG worden bezorgd, zodat hij passend advies kan geven.
- De mening van de FG wordt naar behoren in overweging genomen. Bij onenigheid is het een goede praktijk om de redenen voor het niet volgen van het advies van de FG duidelijk te motiveren en dit vast te leggen.

5. Privacy Officer (PO)

De PO is verantwoordelijk voor het vormgeven, bewaken en -deels- uitvoeren van het privacybeleid binnen de gemeente. Daarnaast kan de PO ondersteunen bij het in kaart brengen van de risico’s door bijvoorbeeld een Data Protection Impact Assessment (DPIA) uit te laten voeren. Ook speelt de PO een belangrijke rol op de werkvloer, zo heeft hij net als de CISO een adviserende rol richting de vakinhoudelijke teams en kan hij vragen beantwoorden zoals: “hoe moeten we deze gegevens delen?”; “Aan welke regels moeten we ons houden?”; “Welke maatregelen moeten we de externe partij opleggen?”. De PO heeft ook een belangrijke rol in het creëren van bewustwording en het (laten) verzorgen van trainingen. De Privacy Officer is niet per definitie een juridische specialist, voor complexe en/of speci-

fieke juridische vraagstukken kan deze eventueel een beroep doen op de juridisch adviseurs binnen de organisatie.

Samenwerking met de FG
In tegenstelling tot de FG, (die de vertegenwoordiger is van het belang van de betrokkene), moet de Privacy Officer daarentegen samenwerken met de 'business' om een werkbaar compromis voor elkaar te krijgen tussen de belangen van de verwerkingsverantwoordelijke en de belangen van de betrokkene. De FG en de PO zijn uiteraard bondgenoten, omdat zij een gezamenlijk doel hebben voor de organisatie: AVG-compliance en een goede bescherming van de persoonlijke levenssfeer van betrokkenen.

Taken van de PO:
- Verantwoordelijk voor privacy gerelateerd concernbeleid en documentatie (beleid, reglementen, onderwijs- en communicatieplan, factsheets), inclusief beoordelen domein en team specifieke reglementen en beleid, o.a. gedragscodes.
- Zorgen voor privacy bewustwording en bewustzijn (onderwijs, kennissessies, trainingen en communicatie).
- Bewaken voortgang data-inventarisaties, risicoanalyses en DPIA's. Adviseren en vragen beantwoorden, zodat de lijnverantwoordelijken de juiste input kunnen leveren voor deze privacy-producten.
- Beantwoordt ad hoc vragen.
- Behandelt de inzage-, correctie- en verwijderingsverzoeken van inwoners.
- Adviseert de diverse domeinen en teams.
- Begeleidt de diverse domeinen en teams en Privacy Ambassadeurs bij het uitvoeren van hun data-inventarisaties, DPIA's en risicoanalyses.
- Coördinerende rol richting de Privacy Ambassadeurs.
- Opzetten regulier overleg (voor kennisdeling en verantwoording over voortgang) tussen de Privacy Ambassadeurs en de PO. Maandelijks (desgewenst vaker) worden de FG en de CISO hierbij uitgenodigd.
- Beoordeelt convenanten en verwerkersovereenkomsten.
- Driewekelijks voortgangsoverleg met de CIO, de CISO en FG.
- Periodiek voortgangsoverleg met de teammanager en de directeur Bedrijfsvoering en dienstverlening.

Voorwaarden:
- Een zekere mate van ondersteuning bij het maken van afspraken en het inplannen van trainingen.
- Een budget waarmee met name het bewustwordingsplan gefinancierd kan worden. Uiteraard moet dat plan dan wel goedgekeurd worden door de directeur Bedrijfsvoering en Dienstverlening.
- Voldoende borging dat de Privacy Ambassadeurs de ruimte krijgen om samen te werken met de PO om deeltaken op te pakken. Ieder domein/ team is namelijk zelf verantwoordelijk voor het AVG en Wpg compliant krijgen van (het eigen onderdeel van) de organisatie.

6. **Privacy ambassadeurs (PA)**

Het is belangrijk dat er in de 3 domeinen plus in het team Concerncontrol, mensen zijn die de ogen en oren van de centrale Privacy Officer kunnen zijn. Zij kunnen de eenvoudige vragen beantwoorden en zij kunnen in een vroeg stadium signaleren wanneer er privacy vraagstukken opspelen. Daarnaast hebben zij een rol om het privacy- en informatiebewustzijn van collega's te vergroten. Zij moeten hier wel voor worden toegerust. Dat betekent naast tijd ook aandacht en opleiding. Dat wil zeggen dat het nodig is om een netwerk te creëren waarin deze mensen elkaar regelmatig ontmoeten om ervaringen te delen en vragen te stellen.

De PA biedt advies en ondersteuning vanuit de teams aan de organisatie op het gebied van privacy en gegevensbescherming, en werkt nauw samen met de PO. De PA is meewerkend voorman en ondersteunt de vakinhoudelijke teams en teammanagers bij de naleving van de AVG en andere privacywetgeving.

Taken van de PA:
- Advies en ondersteuning: adviseert teams en teammanagers op het gebied van privacy en de AVG, en beantwoordt (ad hoc) vragen van collega's.
- Data-inventarisaties en DPIA's: ondersteunt bij data-inventarisaties, risicoanalyses en Data Protection Impact Assessments (DPIA's).
- Privacy bewustzijn: zorgt voor privacy bewustwording binnen de organisatie door middel van trainingen en communicatie.
- Verzoekbehandeling: behandelt inzage-, correctie- en verwijderingsverzoeken van inwoners.
- Verwerkersovereenkomsten: beoordeelt en stelt verwerkersovereenkomsten op, op basis van het bestaande model, en zorgt voor naleving hiervan.

- Datalekbeheer: verantwoordelijk voor de afhandeling van datalekken en andere privacy-incidenten.

Deze verantwoordelijkheden zorgen ervoor dat de PA dicht bij de operationele werkzaamheden staat en speelt daarmee een belangrijke rol in het ondersteunen van de naleving van de AVG en andere privacywetgeving binnen het domein/ team, en draagt daardoor direct bij aan de bescherming van persoonsgegevens. De PA is ook aan te spreken door de Privacy Officer op de taken die ze op het privacygebied uitvoeren. Maar zitten functioneel in de lijn, dus leggen verantwoording af aan hun specifieke domein Directeur. Dus:

- Privacy ambassadeur domein Bedrijfsvoering en Dienstverlening
- Privacy ambassadeur domein Ruimte en Economie
- Privacy ambassadeur domein Sociaal Domein
- Privacy ambassadeur team Concerncontrol

7. **Chief Information Security Officer (CISO)**

De CISO moet het complete spectrum aan informatiebeveiliging overzien en coördineren. De CISO heeft een organisatie-brede kijk op beveiliging. Doel van de functie is het, op basis van de algemeen aanvaarde standaard (de BIO), zorgdragen voor een samenhangend pakket van technische en organisatorische maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de gemeente. Risicoanalyses, oog voor de bedrijfsvoering en inachtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

Voor een gedetailleerde beschrijving van de CISO rol, taken, verantwoordelijkheden en positionering in de informatiebeveiliging, zie de ‘Governance van de Informatiebeveiliging 2024’.

8. **Overige rollen en verantwoordelijkheden**

Team	**Betrokkenheid**
Juridische Zaken	Algemeen adviseren op juridisch gebied en eventueel adviseren bij privacy-gerelateerde vraagstukken.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden de communicatie-adviseurs betrokken.
Audit / concern control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
PenO: Leren en ontwikkelen	Faciliteert en ontwikkelt leermethodes/ materiaal/ workshops/ trainingen.

Bijlage 3: Wet- en regelgeving

1. Grondwet artikelen 10 en 13

In artikel 10 van de Grondwet staat dat iedereen het recht heeft om in de beslotenheid van zijn persoonlijke levenssfeer met rust te worden gelaten en om bijvoorbeeld niet te worden afgeluisterd.

De persoonlijke levenssfeer omvat onder meer:
- het huis
- de briefwisseling
- de communicatie via telefoon en andere communicatiemiddelen
- het recht om niet te worden bespied of afgeluisterd
- het recht op zorgvuldige behandeling van persoonlijke gegevens
- het recht op eerbiediging van het innerlijk leven
- het recht op eerbiediging van de lichamelijke integriteit

De wet kan in bepaalde gevallen dit recht beperken, bijvoorbeeld bij de opsporing van misdaden. Ook maakt de wetgever regels voor het gebruik van privacygevoelige gegevens.

Artikel 13 van de Grondwet omschrijft wat onder het briefgeheim verstaan wordt. Het vormt samen met de artikelen 10, 11 en 12 van de Grondwet, wat je bij wijze van spreken de 'harde kern' van onze grondrechten zou kunnen noemen. Van deze vier is artikel 10 een soort kapstokartikel. Het artikel is zo geformuleerd dat het in de praktijk mogelijk maakt om op nieuwe ontwikkelingen in te spelen. Denk aan mobiele telefoons, internet, cameratoezicht en het mogen fouilleren van inwoners.

2. Europees Verdrag tot bescherming van de rechten van de mens

In artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens (EVRM) wordt (vergelijkbaar met artikel 10 van de Grondwet) het Recht op eerbiediging van privé-, familie- en gezinsleven beschreven.

1. Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Artikel 8 van het EVRM is ook van toepassing op digitale gegevens die inzicht geven in privé leven, zoals bestanden op computers, smartphones en gegevensdragers.

3. Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) is al van kracht sinds 2016. Sinds 25 mei 2018 geldt de AVG in de plaats van de Wet bescherming persoonsgegevens (Wbp). In beginsel zijn 'de eisen voor verwerking van persoonsgegevens' niet veranderd. De verwerking moet proportioneel en niet eenvoudiger op andere wijze uitvoerbaar zijn. Iedere verwerkingsverantwoordelijke moet beschrijven waarom en hoe de gegevens worden verwerkt. Betrokkenen moeten, net als onder de Wbp, op de hoogte gesteld worden. De boetes bij het niet naleven zijn hoog en kunnen oplopen tot 20 miljoen euro. Zulke hoge boetes worden echter enkel opgelegd als de organisatie ernstig in gebreke is gebleven.

AVG en Archiefwet
Hoe in de praktijk van alledag om te gaan met AVG in samenhang met de Archiefwet. Anders dan vaak wordt gedacht, spreken Archiefwet en AVG elkaar niet tegen, maar zijn ze prima met elkaar te combineren. Belangrijk is hierbij dat er een intensieve samenwerking is tussen deskundigen op het gebied van privacy en die op het gebied van de Archiefwet. Alleen dan kan het beschermen van persoonsgegevens samengaan met belangen als authenticiteit en integriteit van informatie, goede bedrijfsvoering en geheugenfunctie volgens de Archiefwet. Sterker nog: een goede uitvoering van de AVG kan niet zonder ook de Archiefwet goed uit te voeren en andersom.

Wat regelt de AVG
Wie is er binnen de gemeente verantwoordelijk voor de uitvoering van de AVG? Hoe kan de gemeenteraad controle uitoefenen op de gegevensbescherming binnen de gemeente?
De AVG is een set open normen en heeft 2 doelen:
- Het mogelijk maken van het vrije verkeer van persoonsgegevens binnen de EU

- De bescherming van persoonsgegevens

Daarom moet het gemeentebestuur bij het verwerken van persoonsgegevens voortdurend een afweging maken tussen de belangen van de personen van wie de gemeente persoonsgegevens verwerkt (betrokkenen) en de belangen van het gemeentebestuur (het uitvoeren van gemeentelijke taken). Bij het verwerken van persoonsgegevens moet de gemeente zich dus de hele tijd de vraag stellen: wat is onze taak, wat is het doel, is er een grondslag en is er een noodzaak?

Het gemeentebestuur is op grond van de AVG verplicht om verantwoording af te leggen over de verwerking van persoonsgegevens: welke maatregelen heeft de gemeente genomen om de gegevens van de betrokkenen te beschermen? Het gemeentebestuur moet ook transparant zijn over welke persoonsgegevens ze verwerkt en waarom. Ter ondersteuning van de verantwoordingsplicht heeft de AVG een aantal (verplicht voorgeschreven) instrumenten:

- het opzetten en bijhouden van een Register van Verwerking
- het uitvoeren van DPIA's
- het toepassen van Privacy by Design/Default principe
- het zorgen voor een effectieve informatiebeveiliging
- de verplichting om datalekken te melden
- het aanwijzen van een Functionaris Gegevensbescherming

Daarnaast hebben inwoners op grond van de AVG rechten, zoals:
- Het recht op inzage
- Het recht op rectificatie en aanvulling
- Het recht op vergetelheid
- Het recht op dataportabiliteit (ook wel gegevensoverdraagbaarheid)
- Het recht op beperking van de verwerking
- Het recht om bezwaar te maken

Het invoeren van de hiervoor genoemde instrumenten gebeurt - in de ideale situatie - in de vorm van een proces waarbij de hele ambtelijke organisatie wordt betrokken (een situatie waarin alleen een FG of team Informatisering en Automatisering/ Informatiemanagement met de implementatie bezig is, is verre van ideaal). Het hele proces is in feite een privacy bewustwordingsproces.

Wat daarbij belangrijk om te weten is, dat de maatregelen die elke gemeente hoort te nemen risicogebaseerd zijn: hoe groter de privacyrisico's (de kans dat de gemeente een verwerking niet transparant, onbehoorlijk of onrechtmatig uitvoert), hoe meer maatregelen de AVG van de gemeente verwacht om zo de risico's voor de betrokkenen terug te brengen tot een aanvaardbaar niveau.

Het borgen van privacy is zodoende een continu proces. Het gaat niet om het eenmalig treffen van een aantal privacymaatregelen. Verwerkingen van gegevens, doelgroepen, technische mogelijkheden, privacyregels, en maatschappelijke opvattingen kunnen veranderen. De effectiviteit van de maatregelen moet daarom regelmatig worden beoordeeld en waar nodig aangepast.

4. **Uitvoeringswet van de Algemene Verordening Gegevensbescherming (UAVG)**

Lidstaten van de EU hebben op bepaalde punten ruimte gekregen om (meer specifieke) nationale wetgeving aan te nemen en de UAVG regelt dit. Daarnaast wordt de AP middels de UAVG opgericht.

Reikwijdte UAVG
De Nederlandse wetgever heeft in de UAVG bepaald dat deze van toepassing is op organisaties die een vestiging hebben in Nederland en op organisaties die geen vestiging in de Europese Unie hebben, maar hier wel diensten en goederen aanbieden. Het gevolg hiervan is dat er mogelijk toch verschillende UAVG's van toepassing zijn op dezelfde verwerking door een organisatie. Dit terwijl het voorkomen van een lappendeken een van de belangrijkste speerpunten van de AVG was.

Bijzondere persoonsgegevens
Naast de uitzonderingen op het algemene verbod om bijzondere persoonsgegevens te verwerken in de AVG, biedt het wel de mogelijkheid om in het kader van het algemeen belang nadere wetgeving te kunnen aannemen. De Nederlandse wetgever maakt hier ruim gebruik van in artikelen 22 – 30 UAVG. In de praktijk betekent dit dat de uitzonderingen in de oude Wet bescherming persoonsgegevens (Wbp) grotendeels ongewijzigd zijn overgenomen. Ook voor strafrechtelijke gegevens heeft de Nederlandse wetgever de huidige uitzonderingen gehandhaafd in de UAVG.

Toestemming wettelijk vertegenwoordiger vereist

Volgens artikel 5 UAVG is in plaats van toestemming van de betrokkene toestemming van zijn wettelijk vertegenwoordiger vereist indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt.

5. Wpg en Wjsg

Naast de AVG hebben onze Boa's, maar soms ook de medewerkers binnen het Sociaal domein te maken met de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze wetten vloeien voort uit de Europese Richtlijn gegevensbescherming bij rechtshandhaving. Aan welke privacywet Boa's en de medewerkers binnen het Sociaal domein zich bij hun werk moeten houden, hangt af van de taak die ze uitvoeren.

Bij specifieke taken voor opsporing en vervolging moeten boa's zich aan de Wpg houden. Deze wetten gelden ook bij:
- het uitvoeren van opgelegde straffen;
- taken om de openbare veiligheid te bewaken;
- taken om strafbare feiten te voorkomen.

Bij andere taken van politie en justitie is de AVG van toepassing. Bijvoorbeeld bij de verwerking van persoonsgegevens van het eigen personeel.

Medewerkers binnen het Sociaal domein van de gemeente kunnen, onder bepaalde voorwaarden (zoals een wettelijke grondslag), ook justitiële en strafvorderlijke gegevens verwerken bij aanvraag en/ of handhaving van een uitkering.

Voor gegevens die onder de Wjsg of de Wpg worden verwerkt, gelden andere regels dan onder de AVG het geval zou zijn geweest. Bijvoorbeeld andere bewaartermijnen, of andere eisen die gelden bij het onderling delen van gegevens. Het is daarom van belang dat de gegevensverwerkingen die onder de Wjsg of de Wpg vallen, andere kenmerken krijgen dan de gegevensverwerkingen die onder de AVG vallen. Om vast te kunnen stellen dat de gemeente dit bij de verwerkingen conform de wettelijke eisen hebben toegepast, wordt de audit Wet politiegegevens uitgevoerd.

Auditing voor de Wpg
Conform de Wpg dient 'de verwerkingsverantwoordelijke' (dit is meestal de werkgever) twee jaren na inwerkingtreding van de wet en vervolgens eenmaal in de vier jaren een externe privacy audit uit te voeren. Nieuw vanaf september 2024 is dat nu de hercontrole op basis van de Regeling Periodieke Audits plaats moet vinden binnen één jaar na rapportdatum van de externe audit. Over de 1e helft van dit jaar blijft de hercontrole beperkt tot het beoordelen van de opzet en het bestaan. Echter, gedurende de 2e helft van dit jaar wordt niet alleen de opzet en het bestaan maar ook de effectieve werking van de beheersingsmaatregelen voortaan beoordeeld bij die beheersingsmaatregelen die bij de externe audit 2024 als 'voldoet niet' of 'voldoet deels' zijn beoordeeld; die interne audit is te vergelijken met een zelfevaluatie. De interne audit (opzet, bestaan en werking) heeft betrekking op enkele onderdelen van de wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven.

Welke rollen zijn er bij het uitvoeren van de interne audit?
Hieronder volgt een overzicht van de verschillende rollen, wie die (kunnen) vervullen en wat de daarbij behorende taken zijn. Per gemeente kan het verschillen door wie de interne audit in de praktijk wordt uitgevoerd. Er moet worden gezorgd voor een helder auditplan, waarin is vastgelegd wanneer wordt gestart met de (voorbereidingen op) de verschillende audits, wie daarvoor het initiatief neemt/ nemen, wie de audit uitvoeren, wie op de uitvoering toeziet, wat de doorlooptijd is en hoe de benodigde informatie (beveiligd) wordt opgeslagen. Hierin worden zowel de jaarlijkse interne audit, als de vierjaarlijkse externe audit verwerkt.

Rol	Naam	Taken/verantwoordelijkheden

Verwerkingsverantwoordelijke	Werkgever van de boa (College van burgemeester en wethouders)	• Verantwoordelijkheid voor het voldoen aan de wettelijke vereisten
Opdrachtgever	Portefeuillehouder	• Bestuurlijk eindverantwoordelijk voor het audit proces • Zorgt voor eventuele financiële middelen voor de uitvoering van het audit proces • Bewaakt de voortgang van het audit proces op strategisch niveau
Gedelegeerd opdrachtgever	Gemeentesecretaris/ domein directeuren/ teammanagers	• Is ambtelijk verantwoordelijk voor de uitvoering van de audit • Stuurt coördinator aan
Opdrachtnemer, coördinator	Projectleider	• Zorgt voor dagelijkse uitvoering van de audit
Domeindeskundigen	PO / PA / Informatiebeveiliger/ FG / CISO / Buitengewoon opsporingsambtenaren	• Leveren advies voor het invullen van de vragenlijst

Het verschil tussen de interne en de externe audit
De jaarlijkse interne audit heeft betrekking op één dan wel een aantal onderdelen van de wet. De interne audit heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven.

Denk bijvoorbeeld aan de verschillende domeinen waarbinnen politiegegevens voor de opsporingstaak verwerkt kunnen worden, maar ook aan verschillende applicaties die daarvoor worden ingezet. Voor een algemeen overzicht van processen die in aanmerking komen voor de audit wordt verwezen naar bijlage 5 bij het Privacybeleid gemeente Zutphen 2024.

Vervolgens vindt een beoordeling plaats van de volgende aspecten binnen de organisatie:
- **Opzet**: De opzet van beheersmaatregelen staat voor ontwerp, bijvoorbeeld te vinden in beleid, zoals informatiebeveiligingsbeleid, privacybeleid, een business case of een projectplan. Als het ontwerp aanwezig is, blijkt dat er een afgewogen keuze is gemaakt. De auditor zal het ontwerp bijvoorbeeld toetsen aan volledigheid. Omdat er van het ontwerp verwacht wordt dat het een formele positie heeft binnen de organisatie (het geeft de kaders voor het treffen en toetsen van de maatregelen) zal er verwacht worden dat het een formele aftekening of goedkeuring heeft gekregen. Denk hierbij aan de handtekening van een directie of MT, of een vastlegging van accordering in een formeel overleg.
- **Bestaan**: Het bestaan zegt zoveel als dat de maatregelen feitelijk zijn getroffen. Voor feitelijke maatregelen (het ophangen en aanzetten van brandmelders) is dat eenvoudig vast te stellen. Voorbeelden van bestaan bij minder concrete maatregelen zijn hoe het ontwerp (de opzet) zich heeft vertaald in procedures, processen en werkwijzen.
- **Werking**: De werking gaat over de effectiviteit van de getroffen maatregelen. Doen deze wel hoe ze bedoeld zijn? Hierbij wordt het ontwerp naast de getroffen maatregel gelegd en wordt het effect getoetst. Als voorbeeld: in het ontwerp staat dat er in iedere ruimte een rookmelder is geplaatst, vanwege een wettelijke plicht. Het ontwerp is gelezen en blijkt volledig. Check. Dan is er een rondgang in het gebouw en in de genoemde ruimten is er een rookmelder aanwezig. Maar dan weten we nog niet of ze het ook feitelijk doen. In dit (korte) voorbeeld zijn zowel opzet als bestaan getoetst. Als de rookmelders getest worden en ze gaan af op het juiste moment (zoals beschreven in het ontwerp, wat getoetst was), dan is ook de werking vastgesteld.

Maak bij het uitvoeren van de interne audit gebruik van reeds opgestelde documenten, zoals DPIA's, het Register van Verwerking, eerder uitgevoerde audits zoals de ENSIA en werkinstructies. De bevindingen en aanbevelingen worden in een rapportage opgenomen en verstrekt aan de intern verantwoordelijke(n).

De vierjaarlijkse externe audit bestaat uit toetsing op alle onderwerpen. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegevens. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen

van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de Autoriteit Persoonsgegevens (uiterlijk 1 jaar na het uitvoeren van de externe audit). Voor het uitvoeren van de externe audit (een volledige audit op opzet, bestaan en werking) wordt ook verwezen naar de NOREA Handreiking 'Privacy audit Wpg voor boa's' (versie 3 september 2024).

Niet iedereen kan/ mag zomaar de interne audit uitvoeren. Een interne auditor moet voldoen aan de volgende eisen:

- De interne auditor stelt zich onafhankelijk op ten opzichte van de auditee;
- De interne auditor beschikt over voldoende kennis en vaardigheden op het gebied van:
  - geautomatiseerde informatiesystemen en methoden en technieken rond IT auditing;
  - de Boa-organisatie;
  - de informatievoorziening en processen van verwerking van politiegegevens;
  - de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens, het Besluit politiegegevens en de Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming.

Beschikt de gemeente niet over iemand die voldoet aan bovenstaande eisen? Dan zal bij het uitvoeren van de audits mogelijk een externe auditor ingeschakeld moeten worden. In theorie zou het inschakelen van een auditor die in dienst is van een dienstverleningsorganisatie in een samenwerkingsverband van gemeenten ook mogelijk moeten zijn.

6. Aankomende wet- en regelgeving voor gemeenten

Privacy & Data Protection	Cybersecurity	Data & Information Exchange	Artificial Intelligence
• GDPR • E-Privacy Verordening	• Cybersecurity Act • NIS Directive 2 • Cyber Resilience Act	• Single Digital Gateway • Open Data Directive • Data Governance Act • Data Act • European Data Spaces	• Ai act

Electronic Identification (E-IDAS)	Urban Air Mobility	Consumer Protection & Regulation of Platforms	
• E-IDAS 2.0	• Regulations on UAS and on the rules to operate with them. • Regulations on the U-Space	• Digital Services & Digital Market Acts.	

Voor een uitgebreid overzicht van aankomende wet- en regelgeving voor gemeenten, zie bijlage 4.

Bijlage 4: Aankomende wet- en regelgeving

De digitale ontwikkeling is binnen onze samenleving niet meer weg te denken. Digitale technologieën en de integratie van data en informatie raken alle aspecten van gemeentelijk bestuur. Deze ontwikkeling heeft ervoor gezorgd dat de EU een datastrategie heeft geformuleerd met als gevolg dat er veel nieuwe wetgeving op gemeenten afkomt. **Tot en met 2026 zullen er in totaal 14 nieuwe wetten van kracht worden op het gebied van digitalisering**.

Gemeenten hebben een rijke bron aan persoonsgegevens die van belang zijn voor openbare diensten, stadsplanning en beleidsvorming. Gemeenten interacteren met inwoners op vele digitale fronten en zijn een centraal punt binnen onze samenleving. Het is dan ook cruciaal dat gemeenten de nieuwe regels in scope hebben voor de interne organisatie en de impact die dit met zich meebrengt voor organisaties waarmee zij samenwerken. Aansluitend dienen de nieuwe regels geïmplementeerd te worden en dient hierop een aantoonbaar controlemechanisme ingericht te zijn.

De Digital Decade biedt gemeenten de kans om te transformeren om zo hun dienstverlening te moderniseren, de betrokkenheid van inwoners te vergroten teneinde vertrouwen te realiseren en innovatie te omarmen. Hierdoor kunnen gemeenten de uitdagingen van de 21e eeuw aangaan waar (online)privacy en ethiek cruciaal zijn.

De verplichtingen uit de Digital Decade geven antwoord op de uitdagende digitale veranderde wereld waar innovatie, data privacy en inwoners centraal staan. Deze ontwikkelingen zijn groots en staan garant voor vele veranderingen. Met de juiste aanpak en implementatie van de Digital Decade komt de gemeente op een hoger niveau van digitale weerbaarheid.

1. ePrivacy Verordening

De ePrivacy Verordening staat op het punt een cruciale rol te spelen in het beschermen van de privacy van inwoners en het reguleren van elektronische communicatie binnen gemeenten en andere organisaties. Deze nieuwe verordening is de opvolger van de huidige ePrivacy richtlijn en een aanvulling op de Algemene Verordening Gegevensbescherming (AVG).

De verordening richt zich op het reguleren van onder andere cookies, vertrouwelijkheid van elektronische communicatie, spam en marketing communicatie.

De ePrivacy Verordening zal in de loop van het jaar 2024 of 2025 van kracht worden. Momenteel is deze nog in ontwikkeling.

De verplichtingen op een rij (dit kan inhoudelijk nog gewijzigd worden):

- **Toestemming voor cookies**: websites dienen toestemming te ontvangen van gebruikers voordat zij niet-essentiële cookies plaatsen of toegang krijgen tot informatie die al is opgeslagen op de apparaten van gebruikers. Een cookiemuur (cookiewall) waarin geen vrije keuze gemaakt kan worden door de betrokkene, is niet toegestaan. De cookiebanner, waarin toestemming wordt gevraagd, zijn aan voorwaarden verbonden zoals het opsplitsen van functionele cookies en andere cookies zoals marketing en analytische.
- **Vertrouwelijkheid van elektronische communicatie**: elektronische communicatie, zoals e-mail en chatberichten, moet vertrouwelijk blijven en mag niet onrechtmatig worden onderschept of afgeluisterd.
- **Spam bescherming**: ongevraagde commerciële communicatie (spam) zal worden voorkomen door opgestelde anti-spamregels, dit helpt de mailboxen van zowel gemeenteambtenaren als inwoners vrij te houden van ongewenste berichten.
- **Recht op privacy van telecommunicatie**: informatie uit elektronische communicatie zoals e-mail berichten, WhatsApp berichten, video calls, sms berichten, bezochte websites en locatiegegevens mag alleen gebruikt worden voor een noodzakelijk doel. Anders dient er toestemming te zijn van de betrokkene om de privacy te beschermen.
- **Toestemming voor direct marketing**: het is van belang dat gemeenten voorafgaand aan het gebruik van elektronische communicatie voor direct marketing doeleinden toestemming hiervoor hebben ontvangen van de betrokkene.
- **Datalekken**: wanneer er sprake is van een inbreuk op persoonsgegevens (een datalek) met mogelijke gevolgen voor de betrokkene, dan is het noodzakelijk dat dit incident wordt geregistreerd en gemeld bij de Autoriteit Persoonsgegevens (AP) en in sommige gevallen ook wordt gemeld aan de betrokkenen.

- **Geheimhoudingsplicht voor communicatieproviders**: telecommunicatieproviders zijn verplicht om de vertrouwelijkheid van de communicatie te waarborgen en mogen de informatie via de communicatie kanalen niet onrechtmatig verwerken.
- **Bescherming van locatiegegevens**: het verzamelen en verwerken van locatiegegevens van gebruikers mag niet zomaar en vereist doorgaans de toestemming van de betrokkene.
- **Opt -in voor telemarketing**: betrokkenen dienen zich actief aan te melden voor telemarketing gesprekken en moet de mogelijkheid worden geboden om zich af te melden.
- **Beveiligingsmaatregelen**: om de beveiliging van elektronische communicatiesystemen te kunnen waarborgen, is het van belang dat telecommunicatieproviders passende technische en organisatorische maatregelen nemen.

2. **Cyber Security Act**

De Cyber Security Act heeft als doel om cyberbeveiliging in Europa te versterken en de digitale weerbaarheid te verbeteren. Hierdoor draagt het bij aan de bescherming van digitale systemen en persoonsgegevens op alle bestuursniveaus, inclusief de gemeentelijke overheden. Deze wet, oftewel de Cyberbeveiligingsverordening, is sinds 2019 van kracht en in april 2022 heeft de Europese upgrade plaatsgevonden.

Gemeenten zullen mogelijk hun beleid en aanbieders inzake cyberbeveiliging moeten herzien en upgraden om aan de nieuwe vereisten te voldoen om zo de digitale infrastructuur van hun gemeente te beschermen tegen cyberdreigingen.

De belangrijkste verplichtingen op een rij:

- **Meldingsplicht**: de autoriteiten verplichten gemeenten om ernstige cybersecurity incidenten te melden zodat zij dit op hun beurt kunnen delen met het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA). Dit zal bijdragen aan de identificatie en aanpak van grootschalige cyberdreigingen.
- **Risicobeoordeling**: het regelmatig uitvoeren van risicobeoordelingen is een vereiste om kwetsbaarheden in digitale systemen te identificeren en passende maatregelen te treffen om deze risico's te verminderen.
- **Bescherming van kritieke diensten**: gemeentelijke digitale diensten die als kritiek worden beschouwd vereisen dat er specifieke beveiligingsmaatregelen worden geïmplementeerd. Daarnaast hebben zij een meldingsplicht voor incidenten waarbij er sprake is van impact op de beschikbaarheid en integriteit van deze diensten.
- **Certificering van beveiligingsmaatregelen**: om aan te tonen dat de digitale diensten voldoen aan bepaalde beveiligingsnormen kunnen gemeenten de diensten laten certificeren.
- **Beveiligingsmaatregelen**: de wet vereist specifieke technische en organisatorische beveiligingsmaatregelen, zoals het gebruik van firewalls, antivirussoftware, toegangscontrolemechanismen en versleuteling.
- **Samenwerking en informatie-uitwisseling**: het wordt aangeraden om samen te werken met andere overheden, instanties of organisaties om informatie over cyberdreigingen en -incidenten te delen, zodat er gezamenlijk actie kan worden ondernomen op beveiligingsuitdagingen.
- **Continuïteitsplanning**: het ontwikkelen van plannen voor bedrijfscontinuïteit en incidentrespons is een vereiste, zodat de gemeentelijke dienstverlening kan worden voortgezet in geval van een cyberaanval en niet geheel stil komt te liggen.
- **Gegevensbescherming**: het is van belang dat de bescherming van persoonsgegevens wordt gewaarborgd in overeenstemming met de relevante privacywetten zoals de Algemene Verordening Gegevensbescherming (AVG).
- **Training en bewustwording**: het is vereist om medewerkers op te leiden en daarbij bewustwording te creëren over cybersecurity en procedures voor incidentrespons.
- **Gegevensretentie en archivering**: het is van belang om een beleid te implementeren voor gegevensretentie en -archivering voor onderzoek en analyse over beveiligingsincidenten.

3. **Network & Information Systems (NIS) Directive 2**

Deze richtlijn heeft als doel de beveiliging van netwerk- en informatiesystemen binnen de EU-lidstaten te verbeteren en gaat over kritieke infrastructuursectoren en digitale dienstaanbieders. De vele datalekken en hacks laten zien dat de cyberdreiging flink is verhoogd waardoor de NIS-richtlijn opnieuw is bekeken en een upgrade heeft gekregen. NIS Directive 2 geeft maatregelen om een hoog niveau van cyberbeveiliging te waarborgen. De deadline om aan de verplichtingen te voldoen is 17 oktober 2024.

De belangrijkste verplichtingen op een rij:

- **Bestuurlijke verantwoordelijkheid**: het bestuur van een organisatie dient cyberbeveiligingstrainingen te volgen en intern streng toezicht te houden.
- **Beveiligingsmaatregelen**: gemeenten zullen strengere beveiligingsmaatregelen moeten implementeren voor hun netwerk- en informatiesystemen. Ook zullen zij passende risicobeoordelingen en beveiligingsplannen opstellen.
- **Minimale beveiligingseisen**: gemeenten dienen minimaal te voldoen aan de basis beveiligingseisen zoals het beheer van risico's van derden om zwakke schakels in de toeleveringsketen te elimineren.
- **Security certificering**: gemeenten dienen aan te tonen dat zij voldoen aan de minimale (cyber)beveiligingseisen aan de hand van een (cyber)beveiligingscertificaat.
- **Meldplicht voor beveiligingsincidenten**: ernstige beveiligingsincidenten dienen binnen 24 uur gemeld te worden aan de nationale autoriteiten waardoor een betere coördinatie en respons op cyberincidenten mogelijk wordt.
- **Security team**: een Computer Security Incident Response Team (CSIRT) dient opgezet te worden zodat dit team hulp kan verlenen bij een dreiging of incident in het netwerk- en/ of informatiesysteem.
- **Samenwerking en informatie-uitwisseling**: een samenwerking en informatie-uitwisseling tussen publieke en private organisaties zal ervoor moeten zorgen dat gemeenten meer betrokken kunnen worden bij bredere samenwerkingsinspanningen.
- **Toezicht en handhaving**: om ervoor te zorgen dat gemeenten voldoen aan de beveiligingsvereisten zullen zij worden onderworpen aan toezicht en handhaving. Zo zullen er security audits worden uitgevoerd, welke kunnen leiden tot boetes wanneer blijkt dat zij niet of onvoldoende voldoen aan de wet-en regelgeving.
- **Boetes**: organisaties die de regels niet naleven lopen het risico op het krijgen van een boete van minimaal 10 miljoen euro of 2% van de totale wereldwijde omzet.
- **Ethische hackers**: ethische hackers krijgen de gelegenheid om kwetsbaarheden in de netwerk- en informatiesystemen te vinden met het doel om deze kwetsbaarheden op te lossen.

4. **Cyber Resilience Act (CRA)**

De Cyber Resilience Act is een cruciale wetgeving die specifiek gericht is om kosten van het afhandelen van cyberincidenten en reputatieschade te verlagen. Cyberdreigingen blijven stijgen en cybercriminelen worden steeds sluwer. Het doel van deze wet is om een "appropriate level of cybersecurity based on the risks" te hebben wat ook aansluit bij de AVG.

De CRA verplicht dat fabrikanten van producten met digitale elementen 'security by design' dienen te hanteren. Dit betekent dat de beveiliging van de digitale producten op orde moet zijn, er een samenhangend cyberbeveiligingskader is en dat er transparante beveiligingskenmerken zijn zodat bedrijven en inwoners een veilig digitaal product kunnen gebruiken.

De verwachting is dat deze wet eind 2024 van kracht wordt en dat iedereen zich hier vanaf 2027 aan moet houden. De belangrijkste verplichtingen voor gemeenten op een rij:

- **Risicoanalyse**: risicoanalyses dienen met regelmaat uitgevoerd te worden om de kwetsbaarheden en bedreigingen voor de gemeentelijke systemen te identificeren.
- **Beleid en procedures**: gemeenten dienen duidelijke beleidslijnen en procedures te ontwikkelen voor de bescherming van persoonsgegevens en systemen tegen cyberaanvallen inclusief handhaving.
- **Cyberbeveiligingstraining**: het is van belang dat medewerkers worden getraind over de basisprincipes van cyberbeveiliging, zodat zij ook bewust zijn wat het allemaal betekent.
- **Netwerkbeveiliging**: het is vereist om een firewall en intrusion detection systeem te hebben om ongeautoriseerde toegang te voorkomen.
- **Gegevensversleuteling**: gevoelige gegevens zullen moeten worden versleuteld om te voorkomen dat ze worden gestolen of worden gelekt.
- **Incident responsplan**: het opstellen van een gedetailleerd incident responsplan is een vereiste om snel te reageren op mogelijke cyberaanvallen.
- **Patchbeheer**: om bekende kwetsbaarheden te dichten is het van belang dat software en systemen tijdig worden bijgewerkt en updates worden uitgevoerd, dit om privacy risico's zoals datalekken te beperken.
- **Toegangscontrole**: het beheer van toegangsrechten is cruciaal om ervoor te zorgen dat alleen geautoriseerd personeel toegang heeft tot bepaalde systemen en gegevens.
- **Back-up en herstel**: er dienen regelmatig back-ups van gegevens gemaakt te worden en de herstelprocedures dienen regelmatig getest te worden.
- **Samenwerking en informatie-uitwisseling**: het wordt aangeraden dat gemeenten samenwerken met andere overheidsinstanties en organisaties om informatie en best practices over cyberbevei-

liging te delen. Ook is het raadzaam om samen te werken met experts in cyberbeveiliging om de organisatie te beschermen tegen cyberdreigingen.

5. **Single Digital Gateway**

De Single Digital Gateway heeft als doel het creëren van één enkel digitaal portaal waar inwoners en bedrijven toegang kunnen krijgen tot informatie en diensten van overheidsinstanties in de hele Europese Unie. Het is in oktober 2018 aangenomen en vanaf eind 2023 van kracht.

Voor gemeenten betekent dit dat ze de mogelijkheid hebben om informatie en diensten efficiënter en gebruiksvriendelijker aan te bieden aan hun inwoners en lokale organisaties. Hierdoor wordt bureaucratie verminderd met als gevolg een betere dienstverlening. Deze digitale transformatie is nodig zodat diensten bij gemeenten strakker digitaal worden ingericht en/ of worden geoptimaliseerd.

De belangrijkste verplichtingen op een rij:

- **Informatieverplichting**: het geven van accurate en actuele informatie over rechten, plichten en procedures die van belang zijn voor inwoners en organisaties is een vereiste voor overheidsinstanties.
- **Toegang tot online formulieren**: inwoners en organisaties zullen de mogelijkheid hebben om digitale formulieren in te kunnen vullen en te kunnen indienen voor administratieve procedures, vergunningen, aanvragen etc.
- **Eenvoudige toegang tot regelgeving**: alle relevante nationale en Europese wet- en regelgeving dient eenvoudig toegankelijk te zijn voor alle inwoners en organisaties.
- **Contactmogelijkheden**: overheidsinstanties dienen duidelijke contactgegevens en communicatiemogelijkheden aan te bieden wanneer inwoners of organisaties vragen hebben.
- **Online dienstverlening**: diensten die het aanvragen van documenten, vergunningen of certificaten mogelijk maken, zullen online beschikbaar worden gesteld.
- **Informatie over deadlines en kosten**: inwoners en organisaties zullen worden geïnformeerd over de geschatte kosten, verwerkingstijden en deadlines voor verschillende procedures.
- **Beschikbaarheid in meerdere talen**: informatie en diensten zullen in meerdere officiële Europese talen worden aangeboden om de toegankelijkheid te vergroten.
- **Informatie over klachtenprocedures**: er zal informatie worden gedeeld over hoe inwoners en organisaties klachten kunnen indienen in het geval van een probleem of ontevredenheid.
- **Elektronische identificatie en authenticatie**: de elektronische identificatie en authenticatie die nodig is voor online transacties en dienstverlening wordt mogelijk gemaakt.
- **Koppeling met andere overheidsinstanties**: het faciliteren van gegevensuitwisseling met verschillende overheidsinstanties om de coördinatie en efficiëntie te verbeteren.

6. **European Data Spaces**

De European Data Spaces is het speerpunt van de Europese data strategie die in 2020 is voorgesteld met als uitvoering meerdere wetten zoals de Data Governance Act, Data Act en Open Data Directive.

De open data spaces biedt gemeenten de wettelijke ruimte om gegevens te delen, te innoveren en de kwaliteit van hun dienstverlening te verbeteren en te moderniseren. Het is van essentieel belang dat gemeenten zorgvuldig overwegen hoe ze hieraan deel willen nemen en welke gegevens zij op vrijwillige basis delen, en niet te vergeten de bijkomende privacy- en beveiligingsaspecten.

De belangrijkste verplichtingen op een rij:

- **Gegevensuitwisseling**: het kan gemeenten helpen bij het delen van relevante gegevens met andere overheidsinstanties, het bedrijfsleven en onderzoeksinstanties. De verbeterde gegevensuitwisseling draagt bij aan een gedegen besluitvorming en beleidsontwikkeling.
- **Interoperabiliteit**: een belangrijk aspect van de European Data Spaces is het bevorderen van interoperabiliteit, wat betekent dat gegevens gemakkelijk kunnen worden gedeeld tussen verschillende systemen en organisaties. Gemeenten kunnen profiteren van gestandaardiseerde gegevensformats en protocollen, waardoor ze gegevens effectiever kunnen delen en gebruiken.
- **Data-eigenaarschap en verantwoordelijkheid**: er zullen duidelijke regels en verantwoordelijkheden moeten worden vastgesteld met betrekking tot het eigendom en gegevensbeheer.
- **Toestemming**: betrokkenen moeten controle hebben over hun eigen gegevens en dienen expliciet toestemming te geven voor het delen en gebruiken hiervan binnen de Data Spaces.
- **Innovatie**: via de European Data Spaces is er toegang tot een breder scala aan gegevensbronnen die innovatie stimuleren. Gemeenten kunnen deze gegevens gebruiken voor nieuwe diensten, toepassingen en oplossingen die de kwaliteit van leven in hun gemeenschap verbeteren.

- **Efficiëntere openbare diensten**: door gegevensuitwisseling en deze te gebruiken kunnen gemeenten de efficiëntie van openbare diensten verbeteren. Dit kan leiden tot kostenbesparingen, betere planning en een verhoogde tevredenheid van inwoners.
- **Europese samenwerking**: gemeenten kunnen via de European Data Spaces deel uitmaken van bredere Europese samenwerkingsinitiatieven. Hierdoor kunnen gemeenten elkaar helpen via best practices en het uitwisselen van ervaringen met andere steden en regio's, en daarnaast deelnemen aan Europese projecten.
- **Gegevensbescherming**: gemeenten zullen zorgvuldig na moeten denken over gegevensbeheer en beveiliging bij deelname aan European Data Spaces. Het waarborgen van de privacy en beveiliging van gegevens is essentieel, aangezien persoonsgegevens worden gedeeld en toegankelijk zijn voor verschillende partijen. Hier dienen gemeenten extra zorgvuldig mee om te gaan.
- **Privacy bescherming**: er dienen mechanismen te zijn ingericht om de privacy van betrokkenen te beschermen, inclusief naleving van de relevante gegevensbeschermingswetgeving zoals de AVG.
- **Inclusiviteit**: door deze European Data Spaces worden verschillende organisaties en gemeenten erbij betrokken. Discrimineren op basis van bijvoorbeeld grootte van de organisatie of technische capaciteiten is niet toegestaan.

7. Open Data Directive

De Open Data Directive is bedoeld om af te dwingen dat overheidsinstanties bepaalde gegevens zoals gegevens over milieu, vervoer en overheidsdiensten die worden verzameld en beheerd, openbaar beschikbaar stellen en hergebruiken. Dit met het doel om de digitale transformatie te stimuleren. De toegang tot overheidsinformatie wordt hierdoor verbeterd en daardoor kan de data worden hergebruikt voor innovatie, economische groei en maatschappelijke doelen.

Deze richtlijn is in het begin van 2019 vastgesteld en in het jaar 2021 in werking getreden. Ons land loopt hierop wel achter en heeft deze richtlijn nog niet omgezet in nationale wetgeving. Hierdoor zal Nederland verantwoording afleggen aan het Hof van Justitie.

De belangrijkste verplichtingen op een rij:

- **Principe van hergebruik**: overheidsinstanties dienen ervoor te zorgen dat de overheidsinformatie beschikbaar is voor hergebruik. Het omvat informatie in digitale vorm en informatie die eventueel digitaal beschikbaar gesteld kan worden.
- **Geen exclusieve rechten**: exclusieve rechten, zoals auteursrechten, kunnen het hergebruik van overheidsinformatie belemmeren, dus zorg ervoor dat er geen exclusieve rechten zijn.
- **Toepassing van standaarden**: overheidsinformatie dient zoveel mogelijk te worden gepubliceerd in machinaal leesbare formaten en onder open standaarden.
- **Communicatie binnen systemen**: streef bij het delen van informatie naar interoperabiliteit van overheidsinformatie waarbij systemen laagdrempelig data met elkaar kunnen uitwisselen, zodat deze gemakkelijk kan worden gecombineerd en hergebruikt.
- **Geen beperkingen**: leg geen beperkingen op aan hergebruik van overheidsinformatie op basis van nationaliteit of vestigingsplaats.
- **Transparante en redelijke kosten**: kosten die in rekening worden gebracht voor het hergebruik van overheidsinformatie moeten transparant zijn, redelijk en gebaseerd zijn op kostenoriëntatie.
- **Gemeenschappelijke toegangsrechten**: gemeenschappelijke toegangsrechten tot overheidsinformatie inclusief de voorwaarden voor hergebruik moeten worden vastgesteld.
- **Uitsluitingen en beperkingen**: in sommige gevallen, bij specifieke belangen zoals bij privacy en veiligheid, is het noodzakelijk om uitsluitingen en beperkingen vast te stellen voor het hergebruik van overheidsinformatie.
- **Toezicht en rapportage**: lidstaten dienen toezicht te houden of de wet wordt nageleefd en zullen regelmatig rapporteren aan de Europese Commissie over de voortgang.
- **Promotie en bewustwording**: lidstaten moeten maatregelen nemen om het bewustzijn over de beschikbaarheid van overheidsinformatie voor hergebruik te vergroten en het gebruik ervan te bevorderen.

8. Data Governance Act (DGA)

De Data Governance Act richt zich op de processen en structuren van data. De wet heeft als doel het stimuleren van gegevensverdeling, het bevorderen van concurrentievermogen en innovatie én het waarborgen van een veilige en verantwoorde omgang met gegevens.

De DGA is op 23 juni 2022 in werking getreden, echter pas van toepassing per september 2023. De DGA is van belang voor gemeenten om te helpen bij het verbeteren van hun omgang met gegevens wat leidt tot betere dienstverlening en innovatie.

De belangrijkste verplichtingen op een rij:

- **Toegang tot publieke gegevens**: er dienen voorwaarden gesteld te worden voor toegang tot publieke gegevens, met name gegevens die worden beheerd door overheidsinstanties zoals gemeenten. Installeer mechanismen om toegang tot gegevens te reguleren.
- **Rechten van gegevensproducenten**: de rechten van gegevensproducenten dienen beschermd te worden, waaronder eigendomsrechten en het recht op gegevensportabiliteit (het overdragen van gegevens).
- **Toegankelijkheid gegevens**: de Data Governance Act beoogt de toegang tot gegevens te vergemakkelijken voor innovatie, met inbegrip van de toegang tot bedrijfsgegevens voor hergebruik.
- **Gegevensintermediairs**: de oprichting en werking van gegevensintermediairs, die dienen als tussenpersonen voor gegevensdiensten, dienen te worden vastgelegd.
- **Gegevensbeschikbaarheid en vertrouwelijkheid**: er dienen maatregelen genomen te worden om de beschikbaarheid en vertrouwelijkheid van gegevens te kunnen waarborgen.
- **Gegevensportabiliteit**: de wet streeft naar het vergemakkelijken van gegevensportabiliteit, waardoor het gemakkelijker wordt voor organisaties en individuen om gegevens van de ene dienst naar de andere over te dragen.
- **Bevordering van databeheerdiensten**: er wordt een kader vastgesteld om de ontwikkeling en bevordering van databeheerdiensten te ondersteunen.
- **Onafhankelijke controleorganen**: om toezicht te houden op de naleving van de regels en voorschriften uit de DGA kunnen er onafhankelijke controleorganen worden opgericht.
- **Certificeringen**: om organisaties te helpen voldoen aan de vereisten vanuit de DGA worden er certificeringen opgesteld.
- **Toegang en hergebruik van gegevens**: de wetgeving bevat bepalingen voor de toegang en het hergebruik van gegevens voor het algemeen belang, zoals voor onderzoek, milieu en het verbeteren van de levering van overheidsdiensten.

9. **Data Act**

De Data Act is een veelbesproken en impactvolle wet, deze wet zal op 12 september 2025 van kracht worden. Deze wet is bedoeld om regels te hebben voor toegang tot en het gebruik van gegevens die door slimme apparaten worden uitgewisseld. Deze slimme apparaten zoals slimme meters, een smart TV, medische apparatuur, deurbellen en connected cars verzamelen veel unieke informatie die vooral bij de fabrikanten in beheer blijft. Via de Data Act zullen betrokkenen makkelijker toegang hebben en inzicht krijgen tot de informatie.

De belangrijkste verplichtingen op een rij:

- **Transparantie**: gemeenten dienen transparant te zijn over het verzamelen en beheren van data. Inwoners moeten duidelijkheid krijgen over welke data er van hen wordt verzameld en zullen toegang krijgen tot hun data op verzoek zonder bijkomende kosten.
- **Clouddiensten**: gemeenten maken gebruik van clouddiensten. Het overstappen is vereenvoudigt. Voor de eerste 3 jaar nadat de Data Act actief is mogen de cloud-aanbieders een vergoeding vragen aan gebruikers, hierna is de cloud overstap gratis.
- **Overheid en data**: overheidsinstanties hebben toegang tot data wanneer zij voldoen aan de voorwaarden, namelijk; bij een noodsituatie, bij het voorkomen van een noodsituatie en wanneer zij een noodzakelijk belang hebben bij het uitvoeren van hun taken in het algemeen belang oftewel op basis van één van de zes AVG-grondslagen, namelijk het algemeen belang.
- **Contracten**: er zijn verschillende bepalingen in contracten die worden verplicht of juist worden verboden. Zo wordt de mogelijkheid tot cloud overstap verplicht. Contracten die tegen goede trouw en eerlijke handel zijn (zoals het sluiten van een paragraaf over grove nalatigheid en aansprakelijkheid) worden verboden.
- **Gegevensuitwisseling**: deze Act bevat regels en voorwaarden bij de gegevensuitwisseling tussen organisaties onderling en dat het onder een eerlijke, redelijke, transparante en niet-discriminerende manier wordt uitgewisseld.
- **Gegevenswaarborging**: er dient te worden gewaarborgd dat er geen onrechtmatige gegevens worden overgedragen zonder een mededeling vooraf, bijvoorbeeld aan derde landen die toegang willen tot bepaalde data.
- **Gegevensbescherming**: de fabrikanten dienen passende technische en organisatorische maatregelen te nemen om de gegevens adequaat te beschermen. Voor gemeenten een aspect om rekening mee te houden.
- **Bijzonderheid**: de European Data Protection Supervisor heeft aangegeven dat de Data Act geen afbreuk mag doen aan de bescherming van persoonsgegevens en dus de AVG een hogere prioriteit heeft.

- **Internationale doorgifte**: de AVG biedt al verplichtingen over internationale doorgifte van persoonsgegevens en de Data Act heeft strikte regels voor de doorgifte van niet-persoonsgebonden gegevens aan landen buiten de EU, in het bijzonder bij informatieverzoeken van buitenlandse autoriteiten.
- **Toezicht en handhaving**: de Data Act bepaalt dat elk land zijn eigen toezichthouder krijgt en daarnaast een sanctiebeleid opstelt. Hierbij dient rekening te worden gehouden met verschillende factoren zoals de ernst van de inbreuk en de jaaromzet van de overtreder.

10. **Artificial Intelligence Act (AI Act)**

De AI Act heeft als doel om een balans te hebben voor de bevordering van innovatie door het gebruik van AI, algoritmes en machine learning en aan de andere kant de bescherming van de rechten, de veiligheid en het welzijn van Europese inwoners en de maatschappij.

De verordening volgt een risico gebaseerde benadering en stelt verplichtingen voor aanbieders en gebruikers. Dit afhankelijk van het risiconiveau dat een AI-systeem met zich meebrengt.

De AI Act is op 9 december 2023 aangenomen en definitief per maart 2024 van kracht geworden.

De belangrijkste verplichtingen op een rij:

- **Verboden AI-praktijken**: de AI Act verbiedt een aantal praktijken zoals emotieherkenning op de werkvloer of het categoriseren van mensen op basis van biometrische kenmerken (ras, seksuele geaardheid of religie). Dit is omdat deze een te groot risico vormen voor de fundamentele rechten van personen.
- **Duidelijkheid**: het moet duidelijk zijn voor gebruikers dat zij met een AI-robot communiceren.
- **AI-systemen met hoog risico**: voor vijf categorieën zoals overheidsinstanties geldt dat zij verplicht een Fundamental Rights Impact Assessment (FRIA) uit dienen te voeren bij hoog risico AI-systemen. Dit om risico's in kaart te brengen voor de zes onderwerpen namelijk: procesbeschrijving, periode en frequentie, categorieën betrokkenen, specifieke risico's, implementatie maatregelen en beheersmaatregelen.
- **Transparantie en aansprakelijkheid**: de AI Act bevat regels voor transparantie en aansprakelijkheid voor AI-systemen, algoritmes en machine learning, zodat gebruikers inzicht hebben in de logs (die 6 maanden worden bewaard) en hoe beslissingen zijn gemaakt. Daarbij wie er verantwoordelijk is voor eventuele schade.
- **Gegevensgebruik en privacy**: de act kijkt ook naar het gegevensgebruik in verband met AI en benadrukt het belang van privacy en beveiliging.
- **Conformiteitsbeoordeling**: ook introduceert het een systeem voor conformiteitsbeoordeling met een CE-logo die organisaties krijgen toegewezen wanneer zij compliant zijn volgens de AI Act.
- **Systeem inregelen**: organisaties dienen een systeem in te richten om in de praktijk zorg te dragen voor data kwaliteit en een systeem in te regelen voor risico beheersing.
- **Menselijk toezicht**: hiermee wordt bedoeld dat er een adequaat getraind persoon vanuit de organisatie is, die onderdeel is van de besluitvorming (in-the-loop) of minstens nauw toezicht (in-command) houdt, bij AI-praktijken.
- **Toezicht en handhaving**: de AI Act bepaalt dat elk land zijn eigen toezichthouder krijgt die er zorg voor draagt dat de AI Act wordt gevolgd en toegang heeft tot de documentatie, bindende aanwijzingen kan geven, bevelen om AI te stoppen bij risico's en boetes kan opleggen.
- **Boetes**: mochten organisaties zich onvoldoende houden aan de AI Act dan kunnen zij een boete verwachten van 7,5 miljoen, 15 miljoen of 35 miljoen euro afhankelijk van de zwaarte van de overtreding. In percentages is dit 1,5%, 3% en 7% van de wereldwijde omzet. Voor mkb en startups zullen de boetes lager uitvallen.

11. **Electronic Identities and Trust Services (eIDAS 2.0)**

De Europese Unie wil met de eIDAS 2.0 een Europees kader voor digitale identiteit creëren, zodat het makkelijker wordt om binnen Europa zaken online te regelen en dat inwoners veilig kunnen inloggen. Vooral organisaties die DigiD en eHerkenning leveren komen in aanraking met de eIDAS 2.0 verordening. De overheid geeft aan dat deze elektronische vertrouwensdiensten diensten zijn die het vertrouwen in online transacties bij bedrijven en consumenten vergroten.

De verwachting is dat het voor gemeenten verplicht wordt om zich vanaf het jaar 2025 aan de eIDAS 2.0 verordening te houden.

De belangrijkste verplichtingen op een rij:

- **Erkenning van eID -middelen**: gemeenten dienen eID-middelen (elektronische identificatie en authenticatie middelen) uit andere EU-lidstaten te erkennen en te accepteren, zodat EU-inwoners met hun digitale identiteit toegang krijgen tot andere lokale overheidsdiensten.
- **Implementatie van eIDAS -conforme eID -oplossingen**: om deel te kunnen nemen aan het eIDAS-netwerk is het van belang dat gemeenten eID-oplossingen implementeren die voldoen aan de technische en juridische vereisten van de eIDAS.
- **Veilige digitale handtekeningen**: het is een vereiste dat gemeenten de mogelijkheid bieden om digitale handtekeningen te gebruiken bij digitale transacties. eIDAS definieert drie niveaus in digitale handtekeningen, zoals een ingescande handgeschreven handtekening of een handtekening met een code die extra beveiligd is.
- **Juridische elektronische handtekeningen**: de elektronische handtekeningen dienen juridisch gelijkwaardig te zijn aan handgeschreven handtekeningen voor relevante transacties.
- **Gegevensbescherming**: het waarborgen van de privacy en gegevensbescherming van inwoners zal voor gemeenten voorop moeten staan bij het gebruik van eID-middelen en andere diensten.
- **Veilige toegang tot e-diensten**: het is van belang dat gemeenten ervoor zorgen dat inwoners veilig toegang krijgen tot elektronische diensten door gebruik te maken van eIDAS-conforme identificatiemiddelen.
- **Tijdstempels**: gemeenten zullen tijdstempels ondersteunen om de integriteit en authenticiteit van elektronische documenten te waarborgen.
- **Beveiligde elektronische bezorging**: het is een vereiste dat gemeenten elektronische bezorgingsdiensten aanbieden die bewijs leveren van de verzending en ontvangst van documenten.
- **Informatievoorziening**: inwoners dienen geïnformeerd te worden over het gebruik van eIDAS-conforme vertrouwensdiensten en de rechten en verplichtingen die hiermee samenhangen.
- **Samenwerking met andere overheidsinstanties**: de samenwerking met andere overheidsinstanties, zowel nationaal als internationaal, is vereist om de uitwisseling van eID-gegevens en vertrouwensdiensten te vergemakkelijken en te coördineren.

12. **Regulations on the U-Space**

U-Space staat voor "Unmanned Aircraft Systems (UAS)" en de regulations zijn een reeks voorschriften en regels die gaan over het beheer van het luchtruim voor onbemande vliegtuigen – zoals drones – in stedelijke en dichtbevolkte gebieden. In Nederland is deze regeling per 26 januari 2023 van kracht.

Het helpt gemeenten bij het reguleren van drone-activiteiten binnen hun jurisdicties, het handhaven van de veiligheid, het waarborgen van de privacy van hun inwoners én natuurlijk het bijhorende beleid en procedures.

De belangrijkste verplichtingen op een rij:

- **Registratieplicht**: drone operators dienen verplicht hun drone te registreren bij de gemeente en moeten hierbij relevante informatie verstrekken, zoals de gebruiker en het serienummer van de drone.
- **Toestemming voor vluchten**: drone operators zullen toestemming moeten vragen bij de gemeentelijke autoriteiten voor het uitvoeren van dronevluchten binnen de stadsgrenzen.
- **No- fly zones**: bepaalde gebieden kunnen door gemeenten worden aangeduid als 'no-fly zones', hier zijn dronevluchten dus verboden. Denk bijvoorbeeld aan gebieden rondom luchthavens, openbare evenementen of op locaties met een gevoelige infrastructuur.
- **Veiligheidsafstanden**: gemeenten kunnen eisen stellen aan de minimale afstanden die drones moeten bewaren ten opzichte van personen, gebouwen en voertuigen om de veiligheid te waarborgen.
- **Vlieghoogte eisen**: maximale vlieghoogtes kunnen door gemeenten worden vastgesteld om conflicten met bemande luchtvaartuigen en privacy kwesties te voorkomen.
- **Privacybescherming**: om de privacy van inwoners te beschermen kunnen gemeenten speciale regels opleggen, bijvoorbeeld het beperken van het gebruik van camera's of gegevensverzameling.
- **Geluidsnormen**: gemeenten hebben ook de optie om regels op te leggen voor het geluidsniveau dat drones mogen maken om overlast voor omwonenden te beperken.
- **Verzekeringseisen**: drone operators worden verplicht voor het hebben van een aansprakelijkheidsverzekering om eventuele schade te dekken in geval van ongevallen.
- **Veiligheidstraining**: gemeenten hebben de mogelijkheid tot het vorderen van training en certificering voor drone operators om ervoor te zorgen dat ze de nodige kennis en vaardigheden hebben om veilig te opereren.
- **Handhaving en boetes**: handhavingsmechanismes en boetes dienen door de gemeenten te worden vastgesteld voor overtredingen van de regelgeving om ervoor te zorgen dat de voorschriften worden nageleefd.

13. Digital Services Act (DSA)

Deze wet zal de huidige e-commerce wet uit 2000 gaan vervangen. De DSA gaat over transparantie in het digitaal adverteren, zodat tussenhandelsdiensten, search engines en grote online platforms verantwoordelijk digitaal adverteren. De Deense Christel Schaldemose die verantwoordelijk is voor het wetsontwerp heeft met deze wet de intentie om alles wat offline verboden is, ook online te verbieden.

Het gaat dus over modernisatie van digitale dienstverleners en de rechten en veiligheid van gebruikers in de digitale wereld. Gemeenten maken gebruik van deze digitale platforms waardoor deze wet ook voor hen relevant is.

De zeer grote online platforms en search engines oftewel de tech reuzen zijn ook aangewezen door de Europese Commissie op 25 april 2023. Voor de tech reuzen is de wet per 25 augustus 2023 van kracht, voor de tussenhandelsdiensten per 17 februari 2024.

De belangrijkste verplichtingen op een rij:

- **Transparantievereisten**: online platforms moeten transparante informatie verstrekken over hun algoritmen, de manier waarop ze inhoud aanbevelen en hun advertentiepraktijken. Dit zodat de gebruiker weet waarom juist deze advertentie wordt getoond en de gebruiker via een opt-out de mogelijkheid heeft om de online profilering te stoppen.
- **Bescherming van consumentenrechten**: gebruikers krijgen meer grip, naast bovengenoemde opt-out kunnen zij gemakkelijk illegale content rapporteren. Advertenties mogen niet op basis van bijzondere persoonsgegevens zoals achtergrond, politieke voorkeur of seksuele geaardheid getoond worden. Daarbij komt dat de voorwaarden van de platforms in begrijpelijke taal worden aangeboden.
- **Mogelijkheid om in beroep te gaan**: platforms moeten mechanismen bieden waarmee gebruikers en bedrijven beslissingen over inhoudsverwijdering kunnen aanvechten.
- **Verwijdering van illegale inhoud**: online platforms moeten zelf inspanningen leveren om illegale inhoud te verwijderen en de verspreiding ervan te voorkomen, inclusief haatdragende taal, terroristische propaganda en kindermisbruik materiaal.
- **Sterke bescherming voor minderjarigen**: platforms dienen een hoog niveau van privacy, informatiebeveiliging en veiligheid voor minderjarigen te hebben. Specifieke reclames richting minderjarigen is dus ook niet meer toegestaan.
- **Rapportage en samenwerking**: platforms moeten rapporteren over hun advertenties en transparante rapporten beschikbaar stellen over risicobeheersing. Hiernaast moeten ze samenwerken met rechtshandhavingsinstanties.
- **Niet-discriminatie en eerlijke behandeling**: platforms moeten alle bedrijven op hun platforms op een niet-discriminerende manier behandelen, inclusief kleinere concurrenten.
- **Onafhankelijke audit en naleving**: grote platforms moeten regelmatig onafhankelijke audits laten uitvoeren door de Commissie om hun naleving van de DSA te controleren.
- **Naleving van advertentieregels**: advertenties moeten voldoen aan specifieke regels en platforms moeten transparantie bieden over de herkomst van advertenties.
- **Coördinatie tussen lidstaten**: de DSA streeft naar betere coördinatie tussen EU-lidstaten bij het handhaven van de regels en het aanpakken van grensoverschrijdende uitdagingen. Per EU-lidstaat zal een digitale coördinator worden aangewezen.

14. Digital Market Act (DMA)

De Digital Market Act streeft naar een betere bescherming van consumentenbelangen. Gemeenten zijn betrokken bij consumentenzaken en kunnen profiteren van sterkere consumentenbescherming op digitale platforms. De Digital Market Act zoomt in op een aantal van de grootste digitale spelers in de markt, zoals grote online platforms en gatekeepers. Dit om eerlijke concurrentie te bevorderen, innovatie te stimuleren en de belangen van consumenten en zakelijke gebruikers te beschermen.

De gemeenten maken gebruik van digitale platforms en diensten waardoor de DMA ook impact voor hen heeft. Deze wet zorgt ervoor om eerlijke en transparante transacties via deze digitale platforms te waarborgen waardoor de digitale innovatie bij gemeenten zal gaan groeien. Deze wet is van kracht sinds 2023 en dus goed om onderstaande verplichtingen mee te nemen.

De belangrijkste verplichtingen op een rij:

- **Definitie van digitale poortwachters**: de DMA definieert digitale poortwachters als grote platforms met een aanzienlijke impact op de interne markt. Deze platforms hebben specifieke verplichtingen.

- **Niet-discriminatie en eerlijke behandeling**: digitale poortwachters moeten alle zakelijke gebruikers op hun platform op een niet-discriminerende en eerlijke manier behandelen. Ze mogen hun eigen diensten niet bevoordelen ten opzichte van concurrerende diensten.
- **Interoperabiliteit**: digitale poortwachters kunnen worden verplicht om de interoperabiliteit van hun diensten mogelijk te maken, zodat gebruikers gegevens en informatie gemakkelijk kunnen delen tussen verschillende platforms.
- **Toegang tot gegevens**: digitale poortwachters moeten mogelijk toegang verschaffen tot bepaalde gegevens aan concurrerende diensten, mits aan bepaalde voorwaarden wordt voldaan.
- **Verbod op zelfpreferentie**: digitale poortwachters mogen hun eigen diensten niet voortdurend bevoordelen in de zoekresultaten, rangschikkingen of aanbevelingen.
- **Transparantievereisten**: digitale poortwachters moeten transparantie bieden over hun rangschikkingscriteria en de manier waarop ze gegevens van gebruikers gebruiken.
- **Verbod op bepaalde praktijken**: de DMA verbiedt bepaalde oneerlijke praktijken, zoals het weigeren van toegang tot gegevens, het belemmeren van de overdraagbaarheid van gegevens en het ongerechtvaardigd blokkeren of verwijderen van content.
- **Onafhankelijke controle en handhaving**: de DMA voorziet in onafhankelijke autoriteiten die verantwoordelijk zijn voor de handhaving van de regels en de beoordeling van nalevingsmaatregelen.
- **Sancties**: mochten er digitale poortwachters zijn die deze regels overtreden dan zijn er reusachtige boetes.
- **Rapportageverplichtingen**: de DMA verplicht digitale poortwachters om regelmatig te rapporteren over hun naleving van de DMA.

Bijlage 5: Uitgebreide RASCI Tabel

RASCI-tabel/ Verantwoordelijkheden-Rollen BIO Controles / Privacy controles																		
Datum	28-mei-24																	
Onderwerp	Controles	Rollen en verantwoordelijkheden																
		College	Directie	Teammanager	CISO	FG	PO	ISO	Controller	Contractmgt	Coördinator BCP	iProjectleider	iAdviseur	FAB	Beveiligingsbeheerder			
															ICT	Facilitair	HRM	alle beheerders
5 Informatiebeveiligingsbeleid		A	R	R	C	C	C	S	C									C
	5.1.1	A	R	R	S	C	C	S	C									C
	5.1.2	A	R	R	S	C	C	S	C			I	I					C
6 Informatiebeveiligingsorganisatie		A	R	R	S	C	C	S	C			S	C		C			C
	6.1.1	A	R	R	S	C	C	S	C									C
	6.1.2		A	R														
	6.1.3		A	R	S			S		C								C
	6.1.4	-	-	-	-	-	-	-		-	-	-		-	-	-	-	-
	6.1.5		A	R	C			C				S	C					
	6.2.1		A	R	S			S							C			
	6.2.2		A	R	S			S							C			
7 Veilig personeel			A	R	C			C									S	
	7.1.1		A	R	C			C									S	
	7.1.2		A	R	C			C									S	
	7.2.1		A	R	C			C									S	
	7.2.2		A	R	C			C									S	
	7.2.3		A	R	C			C									S	
	7.3.1		A	R	C			C									S	
8 Beheer van bedrijfsmiddelen			A	R	C			C							S			
	8.1.1		A	R	C			C							S			
	8.1.2		A	R	C			C							S			

	8.1.3		A	R	C			C									S	
	8.1.4		A	R	C			C							C	C	S	
	8.2.1		A	R	C			C					S					
	8.2.2		A	R	C			S										
	8.2.3		A	R	C			S							C			
	8.3.1		A	R	C			S							C			
	8.3.2		A	R	C			C							S			
	8.3.3		A	R	C			S							C			
9 Toegangsbeveiliging			A	R	C			S				I	I		C	C		
	9.1.1		A	R	C			S				I	I		C	C		
	9.1.2		A	R	C			S				I	I		C			
	9.2.1		A	R	C			S				I	I		C			
	9.2.2		A	R	C			S				I	I		C			
	9.2.3		A	R	C			S				I	I		S			
	9.2.4		A	R	C			S				I	I		S			
	9.2.5		A	R	C			S				I	I	S				
	9.2.6		A	R	C			S				I	I	S				
	9.3.1		A	R	C			S				I	I		C			
	9.4.1		A	R	C		C	S				I	I	S	C			
	9.4.2		A	R	C			S				I	I	S	S			
	9.4.3		A	R	C			S				I	I	S	S			
	9.4.4		A	R	C			S				I	I		S			
	9.4.5		A	R	C			S				I	I		S			
10 Cryptografie			A	R	C			S							C			
	10.1.1		A	R	C			S							C			
	10.1.2		A	R	C			S							S			
11 Fysieke beveiliging			A	R	C			S							S	S		
	11.1.1		A	R	C			S								S		
	11.1.2		A	R	C			S								S		
	11.1.3		A	R	C			S								S		
	11.1.4		A	R	C			S							S	S		
	11.1.5		A	R	C			S							S	S		
	11.1.6		A	R	C			S								S		
	11.2.1		A	R	C			S							S	S		
	11.2.2		A	R	C			S							S	S		
	11.2.3		A	R	C			S							S			
	11.2.4		A	R	C			S							S	S		
	11.2.5		A	R	C			S							C	C		
	11.2.6		A	R	C			S							S	S		
	11.2.7		A	R	C			S							S			
	11.2.8		A	R	C			S							S	S		
	11.2.9		A	R	C			S							S	S		

12 Beveiliging van bedrijfsvoering			A	R	C			S						S	S	S		
	12.1.1		A	R	C			S						S	S	S		
	12.1.2		A	R	C			S						S	S	S		
	12.1.3		A	R	C			S						S	S			
	12.1.4		A	R	C			S						S	S			
	12.2.1		A	R	C			S							S			
	12.3.1		A	R	C			S							S			
	12.4.1		A	R	C			S							S			
	12.4.2		A	R	C			S	C						S			
	12.4.3		A	R	C			S	S						C			
	12.4.4		A	R	C			S							S			
	12.5.1		A	R	C			S							S			
	12.6.1		A	R	C			S							S			
	12.6.2		A	R	C			S							S			
	12.7.1		A	R	C			S	C						C			
13 Communicatiebeveiliging			A	R	C			S							S			
	13.1.1		A	R	C			S							S			
	13.1.2		A	R	C			S							S			
	13.1.3		A	R	C			S							S			
	13.2.1		A	R	C			S							C			
	13.2.2		A	R	C			S							C			
	13.2.3		A	R	C			S							S			
	13.2.4		A	R	C			S							C			
14 Acquisitie, ontwikkeling en Onderhoud Informatiesystemen			A	R	C			S		C			S					
	14.1.1		A	R	C			S		C			S					
	14.1.2		A	R	C			S		C					S			
	14.1.3		A	R	C			S		C					S			
	14.2.1		A	R	C			S		C								
	14.2.2		A	R	C			S		C								
	14.2.3		A	R	C			S		C				S	S			
	14.2.5		A	R	C			S		C					C			

	14.2.6		A	R	C			S		C								
	14.2.7		A	R	C			S		C								
	14.2.8		A	R	C			S		C				S				
	14.2.9		A	R	C			S		C				S	S			
	14.3.1		A	R	C			S		C				S	S			
15 Leveranciersrelaties			A	R	C		C	S		S			S					
	15.1.1		A	R	C		C	S		S			S					
	15.1.2		A	R	C		C	S		S								
	15.1.3		A	R	C		C	S		S								
	15.2.1		A	R	C			S		S								
	15.2.2		A	R	C			S		S								
16 Beheer van beveiligingsincidenten			A	R	C	C		S										
	16.1.1		A	R	C	C		S						s	S	S	C	C
	16.1.2		A	R	C	C	C	S						S	S	S		
	16.1.3		A	R	C	C		S									C	
	16.1.4		A	R	C	C	C	S										
	16.1.5		A	R	C	C		S							S			
	16.1.6		A	R	C	C	C	S	C					C				C
	16.1.7		A	R	C	C		S						S	S			
17 Bedrijfscontinuïteitsbeheer			A	R	C			C			S							C
	17.1.1		A	R	C			C			S							C
	17.1.2		A	R	C			C			S							C
	17.1.3		A	R	C			C			S							C
	17.2.1		A	R	C			S							S			
18 Naleving			A	R	C			S					S					C
	18.1.1		A	R	C			S					S					C
	18.1.2		A	R	C			S		C								
	18.1.3		A	R	C			S					S					
	18.1.4		A	R	C	S	S	C										
	18.1.5		A	R	C			S							C			
	18.2.1		A	R	C			S	C									C
	18.2.2		A	R	S			C	C									C
	18.2.3		A	R	C			S							S			

20 Privacy uit borgingsproduct																		
Beleid	1	A	R	R	C	C	C	C	C					S				S
Er is beleid om beleid vast te stellen	1.1	A	R	R	C	C	C	C	C					S				S
Er is een algemeen privacybeleid en uitwerkingen daarvan	1.2	A	R	R	C	C	C	C	C					S				S
Verantwoordelijkheden op het niveau van het lijnmanagement zijn benoemd, belegd en vastgelegd. (TVB Matrix/RASCI Tabel)	1.3	A	R	R	C	C	C	C	C					S				S
Processen	2		A	R	C	C	C	C	C	S		S	S	S	S	S	S	
Beschrijving administratieve organisatie	2.1		A	R	C	C	C	C	C					S				
Register van Verwerking	2.2		A	R	C	C	C	C	C					S				
Pre-DPIA	2.3		A	R	C	C	C	C	C									
DPIA	2.4		A	R	C	C	C	C	C			S	S	S				S
Bewaar en vernietigingsbeleid	2.5		A	R	C	C	C	C	C	S								
Org Inbedding	3		A	R	C	C	C	C	C								S	
Privacy team	3.1		A	R	C		C		C								S	
Aanstelling FG	3.2		A	R	C	C	C	C	C			S	S	S			S	
Informeren OR	3.3		A	R	C	C	C	C	C								R	
Bewustwording	3.4		A	R	C	C	C	C	C								S	
Rechten van betrokkenen	4		A	R	C	C	C	C	C					S				
Recht op informatie	4.1		A	R	C	C	C	C	C					S				S
Processen rechten van betrokkene op orde	4.2		A	R	C	C	C	C	C					S				
Toestemming	4.3		A	R		C	C							S				
Geautomatiseerde individuele besluitvorming (algoritmes)	4.4		A	R		C	C						S	S	S			
Websites en applicaties	4.5		A	R		C	C						S	S	S			
Technische ondersteuning	4.6		A	R		C	C						S	S	S			

Samenwerking	5		A	R	C	C	C	C	C	S				S				
De organisatie heeft inzichtelijk welke AVG-rol externe partijen innemen en er worden afspraken gemaakt conform de AVG.	5.1		A	R		C	C		C									
Eenmalige gegevensverstrekkingen worden getoetst aan de relevante privacywet- en regelgeving.	5.2		A	R	C	C	C	C	C					S				
Gegevens-bescherming	6		A	R	C	C	C	C	C			S	S	S	S			
Risicomanagement	6.1		A	R	C	C	C	C	C			S	S	S	S			
Gegevens bescherming door ontwerp	6.2		A	R	C	C	C	C	C			S	S	S	S			
Gegevensbescherming door standaard instellingen	6.3		A	R	C	C	C	C	C			S	S	S	S			
Informatiebeveiliging	6.4	A	R	R	C	C	C	C	C			S	S	S	S			
De gemeente heeft inzicht in (potentiële) privacy-incidenten, zoals datalekken.	6.5		A	R	C	C	C	C	C					S	S			
Verantwoording	7		A	R	C	C	C	C	C					S				S
Evaluatie naleving AVG	7.1		A	R	C	C	C	C	C					S	S		S	
Evaluatie informatiebeveiliging	7.2		A	R	C	C	S	C	C				S	S				
Rapportage	7.3		A	R	C	C	R	C	C				S	S				

Definitie RASCI	**Accountable**	De functionaris die **eindverantwoordelijk** (bevoegd) is voor de juiste uitvoering van de taak en goedkeuring geeft aan het eindresultaat. Als het erom gaat, moet deze persoon het eindoordeel kunnen vellen, vetorecht hebben. Deze functionaris is geheel afhankelijk van het succes waarmee R de activiteit uitvoert. Vooral ook omdat A vaak voor het totaal van het proces eindverantwoordelijk is, als proceseigenaar. In veel gevallen is A iemand hoger in de hiërarchie dan R, maar dat hoeft niet per se.
	Responsible	De functionaris die **direct verantwoordelijk** is voor de juiste en tijdige uitvoering van de taak of degene die de activiteit zelf uitvoert. Hiervoor wordt verantwoording afgelegd aan de persoon die accountable is.

	Consultable	De functionaris die **vooraf** geraadpleegd moet worden of goedkeuring of input moet leveren bij een activiteit in het proces. Deze persoon kan daarmee dus het resultaat nog beïnvloeden.
	Supportive	De functionaris die **ondersteuning** verleent aan de uitvoering van de taak of de taak uitvoert. S is een ondersteunende rol waarop R een beroep kan doen. Kan alleen op verzoek van R support leveren. Deze persoon is een expert op zijn gebied. S is verantwoordelijk voor de kwaliteit en het resultaat van zijn support maar is niet direct verantwoordelijk voor de activiteit zelf.
	Informed	De functionaris die **achteraf** geïnformeerd moet worden over de beslissingen, over de voortgang of bereikte resultaten. Deze persoon kan het resultaat dus niet meer beïnvloeden.