centrum informatiebeveiliging en privacybescherming

Grip op Privacy

De Privacy Baseline

De AVG ontrafeld voor toepassing in organisaties

- Versie 3.4

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan echter voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie.

© Centrum Informatiebeveiliging en Privacybescherming.
Voor dit werk geldt een Creative Commons Naamsvermelding GelijkDelen 4.0 licentie, verleend door het CIP. Zie https://creativecommons.org/licenses/by-sa/4.0/

Titel	De Privacy Baseline - De *AVG ontrafeld voor toepassing in organisaties*
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Versie 3.4 Becommentarieerde praktijk (zie: https://cip-overheid.nl/totstandkoming/)
Auteur	CIP-kernteamleden
Bijdragen en review	Leden van de CIP Domeingroep Privacy
Datum	16 mei 2024 NB: logboek van kleine wijzigingen toegevoegd op 27 okt 2020 (bijlage)
WIKI-versie	https://www.noraonline.nl/wiki/De_Privacy_Baseline zie ook: https://www.noraonline.nl/wiki/Privacy

Considerans

CIP-producten steunen op kennis van mensen uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Algemene opmerkingen kan je stellen door te mailen naar: cip@cip-overheid.nl of contact op te nemen via https://www.cip-overheid.nl/contact/.

Specifiek inhoudelijk of redactioneel commentaar bij deze uitgave kun je als voorstel aanbrengen in de WIKI: https://www.noraonline.nl/wiki/De_Privacy_Baseline.

De WIKI versie is, op datum van verschijnen van deze traditionele versie, inhoudelijk gelijk aan deze publicatie. Het benutten van de specifieke WIKI-mogelijkheden staat echter nog in de kinderschoenen. Wij stellen suggesties en ideeën voor de doorontwikkeling zeer op prijs.

Inhoudsopgave

Voorwoord 5
Leeswijzer bij deze versie 5
1 Inleiding 9
1.1 Informationele privacy als uitgangspunt 9
1.2 De doelstelling van de Privacy Baseline 9
1.3 Voor wie is de Privacy Baseline geschreven 10
1.4 Sectorspecifieke wet- en regelgeving 10
2 De Privacy Baseline 11
2.1 Het beleidsdomein 13
2.1.1 B.01 Privacybeleid 13
2.1.2 B.02 Organieke inbedding 17
2.1.3 B.03 Risicomanagement, Privacy by Design en de DPIA 20
2.2 Het uitvoeringsdomein 27
2.2.1 U.01 Doelbinding gegevensverwerking 27
2.2.2 U.02 Register van verwerkingsactiviteiten 50
2.2.3 U.03 Kwaliteitsmanagement 53
2.2.4 U.04 Beveiligen van de verwerking van persoonsgegevens 58
2.2.5 U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens 63
2.2.6 U.06 Bewaren van persoonsgegevens 69
2.2.7 U.07 Doorgifte persoonsgegevens 71
2.3 Het Control- of Beheerdomein 80
2.3.1 C.01 Intern toezicht 80
2.3.2 C.02 Toegang gegevensverwerking voor betrokkenen 82
2.3.3 C.03 Meldplicht Datalekken 86
3 Aanvullende informatie 92
3.1 Werken met persoonsgegevens 92
3.1.1 Verwerking van persoonsgegevens 92
3.1.2 Zelf persoonsgegevens verwerken of uitbesteden 92
3.1.3 Verwerkingsverantwoordelijke en verwerker 93

3.1.4 Verwerkersovereenkomst 93
3.1.5 Persoonsgegevens en bijzondere categorieën persoonsgegevens 94
3.1.6 Strafrechtelijke gegevens en het BSN 95
3.2 De ACT-doelen van privacybescherming 95
3.3 Risico's bij niet voldoen aan de AVG 99
3.4 Grip op privacy 99
3.5 Privacyvolwassenheid 101
Bijlage: De SIVA-methode, korte uitleg 102
Bijlage: Logboek kleine wijzigingen 108

Voorwoord

Het kan voor organisaties een uitdaging zijn om op een juiste manier met persoonsgegevens om te gaan. Wat, waar, door wie en op welke wijze zaken geregeld moeten worden om privacy op een juiste wijze te waarborgen is voor (medewerkers van) organisaties niet altijd duidelijk. Dit is waarom de Privacy Baseline is ontwikkeld: de Privacy Baseline geeft organisaties concrete handvatten om persoonsgegevens op een juiste manier te beschermen. In de Privacy Baseline zijn de eisen van de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) vertaald naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om in overeenstemming met de wet de privacy van de betrokkenen te waarborgen. Het niet naleven van de AVG kan verregaande (negatieve) consequenties hebben; zie hiervoor: 3.3 Risico's bij niet voldoen aan de AVG.

De samenstellers zijn uitgegaan van wat bij het schrijven van de teksten praktisch en volgens de vigerende inzichten en beschikbare kennisbronnen geacht werd juist te zijn. Zij voelen zich daarbij gesteund door de reviews in het kennisnetwerk van CIP, de Domeingroep Privacy in het bijzonder. Maar in géén geval is de Privacy Baseline een vervanger voor de privacywetgeving zelf.

Een woord van dank aan diegenen, die in de afgelopen jaren verbeteringen hebben voorgesteld. Wij hopen dat zij kritisch zullen blijven en suggesties zullen aanbrengen in de wiki-versie[1].

Leeswijzer bij deze versie

Het uitgangspunt voor deze editie van de Privacy Baseline is de versie 3.3 (gepubliceerd oktober van 2020) en de bijgewerkte digitale versie in de wiki van Noraonline (voltooid in juni 2020).

Reden voor de 3.2 versie was de aanpassing op grond van de in het voorjaar van 2018 van kracht geworden Uitvoeringswet (UAVG). Omdat de omzetting van de papieren editie naar de wiki anno 2020 ook weer (lichte) redactionele wijzigingen met zich meebrengt, resulteert dat nu in een versie 3.3 voor zowel de wiki als het 'traditionele' document.

Diverse kleine actualiseringen hebben geleid tot deze 3.4 versie.

Het uitgangspunt van de wetgever voor de UAVG is nadrukkelijk geweest de toenmalige Nederlandse wetgeving (de WBP - Wet bescherming persoonsgegevens) zoveel mogelijk 'beleidsneutraal' over te nemen in de UAVG, daar waar de AVG dat toelaat of om invulling vraagt.

Zonder volledigheid te claimen geven wij hier de volgende voorbeelden:

- De handhaving van de leeftijdsgrens van 16 jaar voor de verwerking van de persoonsgegevens van kinderen op grond van toestemming, waar de AVG de mogelijkheid van 13 jaar geeft. [2]

[1] https://www.noraonline.nl/wiki/De_Privacy_Baseline.
[2] Artikel 5 lid 4 UAVG.

- De handhaving (ex WBP) van enkele specifieke uitzonderingen voor de verwerking van bijzondere gegevens[3]. NB: wees erop verdacht dat in Nederland specifieke uitzonderingen kunnen gelden die andere EU-lidstaten niet kennen.
- De UAVG breidt de reikwijdte van het toepassingsgebied van de AVG uit naar (ook) activiteiten die buiten de werkingssfeer van het Unirecht vallen[4]. Dit betekent dat in Nederland de AVG eigenlijk altijd geldt buiten de uitzonderingen die nog overeind zijn gebleven. Alleen gegevensverwerkingen op terreinen die in hun geheel zijn uitgezonderd van de werking van Europees recht vallen buiten de materiële werkingssfeer van de verordening. Dit zijn uitsluitend verwerkingen in het kader van nationale veiligheid en verwerkingen door de krijgsmacht, en verwerkingen waarop de Gegevensbeschermingsrichtlijn opsporing en vervolging van strafbare feiten van toepassing is[5].
- De UAVG[6] heft het verbod om mensen te onderwerpen aan geautomatiseerde besluitvorming (met aanmerkelijke gevolgen voor betrokkenen) op, indien de wet dat verplicht stelt. De UAVG vult hiermee AVG Art. 22 lid 2b in.
- Verwerking van biometrische gegevens is toegestaan voor authenticatie en beveiligingsdoeleinden[7].
- De uitzondering voor financiële ondernemingen om een datalek niet te hoeven te melden bij de betrokkene blijft bestaan. Zij moeten het datalek wel melden bij de Autoriteit Persoonsgegevens (AP) en de financiële toezichthouders[8]. De financiële sector heeft eigen wetgeving die de zorgplicht jegens betrokkenen regelt.
- Ook overheidsorganisaties kunnen boetes krijgen van maximaal 10 respectievelijk 20 miljoen Euro.[9]

Als direct gevolg van de UAVG is ook de Privacy Baseline aangepast. Met name het criterium U.01 Doelbinding gegevensverwerking is grondig gereviseerd met betrekking - maar niet beperkt - tot bijzondere categorieën persoonsgegevens; waar nodig zijn ook de overeenkomstige toelichtingen bij dit criterium en de indicatoren aangepast.

Veel artikelen in de AVG/UAVG gaan direct of indirect over de Autoriteit Persoonsgegevens. De bevoegdheden van de Nationale toezichthouder - de AP - en de eisen die de wet aan de AP stelt vallen buiten de scope van de Privacy Baseline. Het betreft Hoofdstuk 2 van de UAVG en de hoofdstukken VI en VII, en X en XI van de AVG. De bepalingen in deze hoofdstukken zijn voor de

---

[3] UAVG Art. 22 lid 2, Art. 23-29, Art. 30 lid 5 & 6.

[4] UAVG Art. 3.

[5] RICHTLIJN (EU) 2016/680 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
Bekijk via deze link de richtlijn.

[6] UAVG Art. 40.

[7] UAVG Art. 29

[8] Artikel 42 UAVG.

[9] UAVG Art. 18.

toepassing van de Baseline niet direct van belang. Hoofdstuk VIII en zeker hoofdstuk IX daarentegen ('Beroep, aansprakelijkheid en sancties' resp. 'Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking') kunnen voor organisaties c.q. verwerkingsverantwoordelijke en verwerkers nog wel degelijk relevant zijn. Dat kan ook gelden voor de artikelen 15-20 van de UAVG (waaronder het al genoemde Art. 18: "Bestuurlijke boete aan overheden").

Over de AP nog dit: de AVG spreekt consequent over "de bevoegde toezichthoudende autoriteit". Dat moet zo, omdat het kan voorkomen dat de toezichthouder die een overtreding behandelt niet altijd de toezichthouder voor het land is waar de overtreding is geconstateerd. Tenzij de context anders vereist spreken wij hierna van 'de AP' als de bevoegde toezichthoudende autoriteit.

Wij verwijzen naar de Uitvoeringswet plus de Memorie van toelichting als: 'de Uitvoeringswet' of: 'de UAVG'. Wanneer we zonder verdere specificatie spreken van 'de AVG' of 'de privacywetgeving', dan bedoelen we daarmee de combinatie van de AVG en de UAVG.

De AVG (in verschillende talen, inclusief Nederlands) is te vinden op de website van Eur-Lex. Bij onduidelijkheid over de betekenis van de teksten in een andere taal dan het Engels is de Engelstalige versie de maatstaf.

De UAVG is via deze link te raadplegen. De Memorie van toelichting bij de UAVG is via deze link te bereiken.

Draagvlak door brede inbreng uit het CIP-netwerk

De Privacy Baseline is het hart van de documentenreeks 'Grip op Privacy': een verzameling gerelateerde documenten over de pragmatiek van Privacy in organisaties. Het doel van deze documenten is praktische handvatten bieden aan organisaties die privacy in beleid en uitvoering controleerbaar willen implementeren, verbeteren en op orde houden.

Alle documenten zijn tot stand gekomen in en vanuit de CIP-community. Het brede palet van organisaties dat daarbij betrokken is geweest geeft de auteurs het vertrouwen dat de methode 'Grip op privacy' draagvlak heeft voor een brede toepassing en verdere ontwikkeling.

Over CIP

CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het is opgericht voor informatie-uitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening en heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waarin ook gespecialiseerde marktorganisaties als kennispartners deelnemen. Kennis die in de aangesloten organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt. Voldragen producten worden op de publieke site van het CIP gepubliceerd.

Door meer samen te doen en zo mogelijk te uniformeren draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen. De publicaties van het CIP worden in principe om niet ter beschikking gesteld en kunnen, met inachtneming van de voorwaarden van Creative Commons Naamsvermelding/Gelijk Delen, vrijelijk gebruikt worden, zie:
https://creativecommons.org/licenses/by-sa/3.0/nl/

1 Inleiding

Eind 2014 werd in de CIP-community de vraag gesteld "hoe dat nou moet, met die privacy". De vraag was niet voortgekomen uit naïviteit, maar uit de wirwar van informatie en opvattingen over privacy op dat moment. Het antwoord hebben we gezocht in de pragmatiek: pak privacy bij de kop zoals organisaties en bedrijven ermee moeten werken. Daarvoor gelden immers wetten en voorschriften en wat je er ook van vindt, daaraan heb je als bedrijf of organisatie te voldoen.-en wat je er ook van vindt, daaraan heb je als bedrijf of organisatie te voldoen[10].

1.1 Informationele privacy als uitgangspunt

Organisaties kunnen ervoor kiezen om 'slechts' te voldoen aan de wet, een lastige hinderpaal. Maar door verantwoord en efficiënt om te gaan met privacy en de balans te vinden tussen wetgeving, de doelstelling van de organisatie en respect voor de persoonlijke levenssfeer van betrokkenen, is 'privacy' ook als een kwaliteitskenmerk ten voordele te benutten.

In dat verband is het zeker nuttig om ook naar de niet-wettelijke aspecten van privacy te kijken en te weten hoe klanten 'privacy' ervaren. In de andere documenten van Grip op privacy besteden we daar ook aandacht aan. Maar als een organisatie transparant en concreet wil zijn over het privacybeleid en ook netjes wil voldoen aan de wettelijke vereisten om boetes, imagoschade en schadeclaims te voorkomen, dan moet zij proactief werk maken van het type privacy dat 'informationele privacy' wordt genoemd.

Informationele privacy gaat over het "beschermen van personen in relatie tot informatie die van of over hen bekend is en/of ten aanzien van hen wordt toegepast" (S. Nouwt 2005, *Privacy voor doe-het-zelvers*), nu veelal begrepen als 'bescherming van persoonsgegevens' (of 'gegevensbescherming').

Het centrale uitgangspunt van de AVG 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. De Privacy Baseline bevat dertien principes (ook wel: normen of criteria) die moeten worden gerespecteerd om dat als organisatie goed te doen. De Privacy Baseline is van toepassing op organisaties die met persoonsgegevens werken.

1.2 De doelstelling van de Privacy Baseline

De ACT doelen

De Privacy Baseline biedt concrete handvatten voor een juiste omgang met persoonsgegevens. Voor organisaties die met persoonsgegevens werken bieden de AVG en de UAVG een harde maatstaf om concreet, effectief en controleerbaar privacybeleid te voeren, volgens de drie doelstellingen

[10] Bedrijven en organisaties: wij hanteren 'organisatie' voor beide aanduidingen in de publieke en private sectoren.

Afscherming, *Corrigeerbaarheid* en *Transparantie* (ACT)[11]. Deze zijn vergelijkbaar met de BIV-doelstellingen bij informatiebeveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid.

ACT beoogt expliciet de betrokkene te beschermen. De AVG zegt met dezelfde bedoeling dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene "rechtmatig, behoorlijk en transparant" is. Met enige lenigheid is deze trits gemakkelijk te verzoenen met het ACT-trio.

De ACT doelen helpen bij het adequaat borgen van de informationele privacy van betrokkenen en helpen de organisatie bij het voorkomen van rode kaarten, bindende aanwijzingen en/of boetes vanuit de Autoriteit Persoonsgegeven. Meer hierover zie: 3.2 De ACT-doelen van privacybescherming.

Accountability

Deze baseline is bij uitstek ook het hulpmiddel dat organisaties in staat stelt te voldoen aan de vereisten voor 'accountability', in de Nederlandstalige AVG 'verantwoordingsplicht' genoemd, die inhoudt dat naleving van de wet moet kunnen worden aangetoond. Verantwoordingsplicht impliceert documentatieplicht en ook die vereiste is concreet in de Baseline verwerkt.

1.3 Voor wie is de Privacy Baseline geschreven

Het format van de Privacy Baseline is dat van de normenkaders zoals die al jaren in het domein van informatiebeveiliging worden gebruikt. Het is een naslagwerk waarmee je kunt controleren in hoeverre de organisatie aan privacy wet- en regelgeving voldoet en waarmee je afwegingen kunt maken bij die zaken die daarvoor - volgens de Baseline - nog te doen staan. De Privacy Baseline is een document voor professionals die hands-on in de organisatie werken aan privacymaatregelen en de borging van en de controle op die maatregelen.

De Privacy Baseline vertaalt de privacywetgeving naar concrete, hanteerbare en ondubbelzinnige normen die aangeven *wat een organisatie moet doen* om te kunnen voldoen aan de privacywetgeving: moet je regelen in het privacybeleid, de uitvoering en de controle erop.

De Baseline is *een gids voor omgang met persoonsgegevens*, maar kan niet als vervanger van de wet worden beschouwd. Nauwkeurige naleving van de Baseline brengt een organisatie echter wel naar een privacyvolwassenheidsniveau dat doorgaans voldoende is om een basale compliancy-toets te doorstaan.

1.4 Sectorspecifieke wet- en regelgeving

Organisaties die persoonsgegevens verwerken moeten in sommige gevallen (ook) voldoen aan sectorspecifieke wetgeving. Denk aan de Telecommunicatiewet, de Gezondheidszorg of de voorschriften voor financiële ondernemingen. Zoals de AVG naar specifieke lidstatelijke wet- en regelgeving verwijst maar niet feitelijk behandelt, zo houdt ook de Privacy Baseline géén rekening met eventueel van toepassing zijnde sectorspecifieke wet- en regelgeving.

[11] De ACT-privacydoelstellingen zijn gebaseerd de Privacy Protection Goals van ENISA: Unlinkability, Transparency, Intervenability. (ENISA dec 2014, Privacy and data protection by design. From policy to engineering).

2 De Privacy Baseline

De Privacy Baseline is verdeeld in de volgende drie hoofdstukken:

1. Het Privacybeleid van organisaties (2.1 Het beleidsdomein);
2. De eisen aan de uitvoering van de AVG (2.2 Het uitvoeringsdomein), en:
3. Het beheer en de controle van het privacybeleid (2.3 Het Control- of Beheerdomein).

Het geheel beschrijft welke concrete eisen worden gesteld aan organisaties bij de omgang met persoonsgegevens.

Baseline format

De eisen aan de uitvoering van de privacywetgeving zijn weergegeven in de vorm van een normenkader. Dit normenkader is gebaseerd op de SIVA-methode[12]. De eisen worden gestructureerd op basis van een template waarin de elementen wie, wat en waarom geadresseerd worden, zodat antwoord wordt gegeven op de vraag: "wie doet wat en waarom?".

Onderwerp van de norm						
Criterium (wie en wat)	Wat (xxxxxx) <werkwoord> xxxxx trefwoorden xxxxx					
Doelstelling (waarom)	De reden waarom de norm gehanteerd wordt.					
Risico	Het risico dat de aanleiding vormt om de norm te hanteren.					
Referentie	Bron 1	Bron 2	...			
Conformiteitsindicatoren en maatregelen						
Conformiteitsindicator (trefwoord)						
/01	Maatregel 01					
/02	Maatregel 02.					
...	...					

Figuur 1: De SIVA-schrijfwijze

[12] W.N.B. Tewarie, SIVA, Methodiek voor de ontwikkeling van auditreferentiekaders, VU University Press, Amsterdam 2014.

Een *conformiteitsindicator* is een (sub)norm waaraan voldaan moet worden om aan het criterium (de hoofdnorm) te kunnen voldoen. Conformiteitsindicatoren hebben in de tekst van de hoofdnorm een anker in de vorm van een *trefwoord* dat de subnorm aanduidt. Je kunt stellen dat ieder onderstreept trefwoord gedefinieerd en uitgewerkt wordt in de vorm van maatregelen.

Per conformiteitsindicator worden een of meer maatregelen (/01, /02, etc.) geformuleerd, op basis waarvan een uitspraak mogelijk is over de desbetreffende conformiteitsindicator.

In veel gevallen volgt een nadere uitleg van de maatregelen in toelichtingen onder het kader.

Dit maakt de Baseline niet alleen een heldere verzameling van instructies die je stapsgewijs vertellen hoe je privacy in de organisatie kunt bewerkstelligen, hij biedt ook het kader waartegen je gedetailleerd kunt toetsen hoe de organisatie ervoor staat.

Voor een meer uitgebreide toelichting zie Bijlage: De SIVA-methode, korte uitleg en https://www.noraonline.nl/wiki/SIVA-methode

2.1 Het beleidsdomein

Inleiding

In dit hoofdstuk zijn richtlijnen opgenomen voor het algemeen beleid rondom privacy. Met dit beleid geeft de organisatie zowel de eigen afdelingen als andere partijen duidelijkheid over de kaders waarbinnen de verwerkingen van persoonsgegevens plaatsvinden. Dit beleid beschrijft ook aan welke voorwaarden processen en systemen moeten voldoen en hoe dit beleid op naleving wordt gecontroleerd.

Doelstelling

De doelstelling van het beleidsdomein is ervoor te zorgen dat op strategisch niveau afdoende randvoorwaarden en condities aanwezig zijn om de persoonsgegevens verantwoord te verwerken en opdat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.

Risico's

Door het ontbreken van een door het management uitgevaardigd beleid ontstaat het risico dat onvoldoende sturing wordt gegeven aan het verwerken van de persoonsgegevens. Doorgaans zal dit een negatieve impact hebben op het realiseren van organisatiedoelstellingen (en het voldoen aan de eisen van de AVG).

2.1.1 B.01 Privacybeleid

Privacybeleid geeft op organisatie - en strategisch niveau duidelijkheid en daarmee sturing aan de inrichting van privacy.

Inhoud

Het privacybeleid geeft aan op welke wijze - door het treffen van maatregelen - voldaan wordt aan de van toepassing zijnde wet- en regelgeving. Omdat de wet- en regelgeving externe factoren zijn die kunnen veranderen, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Maar ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde missie of visie, kunnen het nodig maken om te komen tot aanpassing van het beleid. Het volstaat dus niet om eenmalig beleid op te stellen en niet meer aan te passen. Door het beleidsproces cyclisch in te richten kan het beleid op de ontwikkelingen en de uitvoering afgestemd blijven.

Proces

De ontwikkeling van de organisatie tot een organisatie die aantoonbaar aan wet- en regelgeving voldoet (ofwel: 'compliant' is aan wet- en regelgeving), vraagt om een cyclisch proces. Dit houdt in dat er sprake is van een terugkoppelmechanisme waarbij - door inzicht in de uitvoering - het beleid kan worden bijgestuurd en gecorrigeerd. De Privacy Baseline is als cyclisch proces (Beleid, Uitvoering en Control) opgezet. Afspraken over hoe dit cyclische proces vormgegeven wordt maken onderdeel uit van het beleid.

B.01 Privacybeleid				
Criterium	De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen. [13]			
Doelstelling	Privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt.			
Risico	Het ontbreken van een privacybeleid leidt ertoe dat de organisatie geen duidelijkheid heeft wat precies wordt verwacht, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden verwerkt (waaronder verzamelen, bewerken, inzien et cetera).			
Referentie	AVG	UAVG		
	Art. 5, 24, 40	Art. 2, 4		
Indicatoren en maatregelen				
/01 Privacybeleid				
/01.01	Het beleid geeft duidelijkheid over hoe de verantwoordelijken hun verantwoordelijkheid voor de naleving van de beginselen en de rechtsgrondslagen invullen en dit kunnen aantonen ("verantwoordingsplicht")[14].			
/01.02	Het privacybeleid is tot stand gekomen langs een cyclisch proces dat voldoet aan een gestandaardiseerd patroon met daarin de elementen: voorbereiden, ontwikkelen, goedkeuren, communiceren, uitvoeren, implementeren en evalueren.			
/01.03	Het topmanagement van de organisatie heeft het privacybeleid vastgelegd, bekrachtigd en gecommuniceerd binnen de organisatie, met daarin de visie op privacybescherming en richtlijnen voor het - in overeenstemming met de wet - rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens.			
/01.04	De organisatie heeft vastgesteld en vastgelegd welke wet- en regelgevingen gelden.			
/01.05	In het beleid is vastgelegd en bekrachtigd op welke wijze invulling wordt gegeven aan de eisen van de sectorspecifieke wetgeving.			
/01.06	In het beleid is vastgelegd of een gedragscode wordt gehanteerd waarin de uitvoering van de AVG nader wordt geconcretiseerd voor de eigen organisatie of branche, en met welke frequentie deze gedragscode en de naleving ervan worden gecontroleerd en geëvalueerd door de verantwoordelijke en - indien aangesteld - de Functionaris voor Gegevensbescherming (FG)[15].			
/02 Invulling gegeven aan de wettelijke beginselen				
/02.01	Beschreven is hoe gewaarborgd wordt dat verantwoordelijken vooraf aantoonbaar maatregelen hebben genomen door het conform B.03 toepassen van Privacy by Design, het uitvoeren van DPIA's en het gebruik van standaard instellingen.			

[13] AVG Art. 5 lid 1 Beginselen inzake verwerking van persoonsgegevens.
[14] AVG Art. 5 lid 2.
[15] AVG Art. 25 en Art. 64 lid 2.

B.01 Privacybeleid	
/02.02	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens, conform U.01, voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.
/02.03	Beschreven is hoe gewaarborgd wordt dat, conform U.01, de verwerking toereikend, ter zake dienend en beperkt is tot "minimale gegevensverwerking"; tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt.
/02.04	Beschreven is hoe gewaarborgd wordt dat, conform U.03, de persoonsgegevens juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens die onjuist zijn, gelet op de doeleinden waarvoor zij worden verwerkt, onverwijld te wissen of te rectificeren.
/02.05	Beschreven is hoe gewaarborgd wordt dat, conform U.04, passende technische en organisatorische beveiligingsmaatregelen worden getroffen, zoals pseudonimisering van persoonsgegevens, zodat duidelijk is hoe een veilige verwerking wordt gewaarborgd en hoe de persoonsgegevens onder meer worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
/02.06	Beschreven is hoe gewaarborgd wordt dat, conform U.05 en C.02, de persoonsgegevens op een wijze worden verwerkt die voor het publiek en de betrokkene transparant is en het de betrokkene mogelijk maakt zijn rechten uit te oefenen. Hierbij is specifiek aandacht voor de bescherming van kinderen.
/02.07	Beschreven is hoe gewaarborgd wordt dat, conform U.06, persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij worden verwerkt en in welke vorm de opslag moet plaatsvinden zodanig dat na deze periode de betrokkenen niet langer zijn te identificeren.
/02.08	Beschreven is hoe gewaarborgd wordt dat, conform U.07, persoonsgegevens slechts worden doorgegeven wanneer formeel afdoende garanties zijn vastgelegd, zodat aangetoond kan worden dat ook bij de doorgifte aan de AVG wordt voldaan en dat aangegeven kan worden wat in verwerkersovereenkomsten en samenwerkingsovereenkomsten moet worden vastgelegd.
/02.09	Beschreven is hoe gewaarborgd wordt hoe verantwoordelijken, conform C.01, aantonen dat - gedurende en na de verwerking - de verwerking ten aanzien van de betrokkene behoorlijk is en hoe dit door middel van het bijhouden van een register, conform U.02, en een dossier kan worden aangetoond.
/02.10	Beschreven is hoe gewaarborgd wordt dat, conform C.03, bij een inbreuk in verband met persoonsgegevens (datalek of 'personal data breach') de betrokkenen en de AP worden geïnformeerd als deze inbreuk waarschijnlijk een risico inhoudt voor de rechten en/of vrijheden van natuurlijke personen.

Toelichting /01 Privacybeleid

/01.02 De ontwikkeling van het beleid komt cyclisch tot stand, zodat het beleid kan worden bijgestuurd en gecorrigeerd. Bekende voorbeelden van cyclische processen zijn Plan-Do-Check-Act (PDCA) of Observe-Orient-Do-Act (OODA).

/01.02 Het tot stand komen van het beleid langs een cyclisch proces betekent vooral dat de effectiviteit van het beleid gemeten wordt. Wanneer de maatregelen die uit het beleid voortvloeien onvoldoende blijken bij te dragen aan de doelstellingen van het beleid, dan worden zowel de getroffen maatregelen als het beleid zelf onderzocht op hiaten Zo worden mogelijke aanvullingen en correcties geïdentificeerd, die na validatie worden opgenomen. Daarmee is het beleid en/of de onderliggende uitvoering aangepast.

/01.03 Door het vaststellen van het privacybeleid door het topmanagement worden het privacybeleid en de verantwoordelijkheden op strategisch en uitvoeringsniveau geborgd.

/01.03 Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Voor natuurlijke personen dient het duidelijk te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins worden verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt.
Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijke en eenvoudige taal worden gebruikt. Dat beginsel betreft met name het informeren van de betrokkenen over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de natuurlijke personen in kwestie en hun recht om bevestiging en mededeling te krijgen van de verwerking van hun persoonsgegevens. Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot deze verwerking kunnen uitoefenen.

/01.03 De specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt dienen expliciet en gerechtvaardigd te zijn en te zijn vastgesteld nog voordat de persoonsgegevens worden verwerkt .De persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

/01.04 De organisatie bepaalt aan de hand van een analyse of zij de passende maatregelen kan nemen die vanuit de van toepassing zijnde wet- en regelgeving worden vereist.

/01.05 In het beleid is vastgesteld en bekrachtigd op welke wijze sectorspecifieke wetgeving wordt uitgevoerd. Verschillende sectorspecifieke wetten stellen nadere regels aan de gegevensverwerkingen in specifieke sectoren, bijvoorbeeld de Telecommunicatiewet en Wet BRP.

/01.05 Bij overlapping gaan de bijzondere regels van de sectorspecifieke regels vóór op de algemene regels van de (U)AVG. Als in sectorspecifieke wetgeving niets is bepaald, dan gelden de algemene regels van de (U)AVG.

1. /01.06 De organisatie kan ervoor kiezen om een Gedragscode[16] op te stellen. In een Gedragscode worden de eisen van de AVG voor een specifieke branche of organisatie uitgewerkt tot concreet te nemen maatregelen om aan de AVG te voldoen. Een dergelijke Gedragscode moet voldoen aan eisen:

1. Elke bepaling heeft een toelichting waarom die is opgenomen;
2. Als de bepaling een uitwerking is van de wet, is aangegeven waarom de wet op die specifieke manier is vertaald;
3. De aanvrager van de gedragscode is voldoende representatief voor de betrokken sector en de betrokken sector is voldoende nauwkeurig omschreven in de Gedragscode;
4. De Gedragscode is concreter dan de AVG;
5. De Gedragscode vormt een juiste uitwerking van de AVG of van andere wettelijke bepalingen voor de verwerking van persoonsgegevens;
6. Als een bepaling uit de Gedragscode uit een gedeelte of een parafrasering van een wettelijke bepaling bestaat, dan is deze afwijking gemotiveerd;
7. De AP of (indien aangesteld) de FG kan verzocht worden om de gedragscode op juistheid te controleren.

/01.06 Als een Gedragscode voorziet in het beslechten van geschillen over de naleving ervan, dan kan de AP de verklaring slechts afgeven als er waarborgen zijn voor de onafhankelijkheid van de geschilbeslechting.

2.1.2 B.02 Organieke inbedding

Het waarborgen van de privacy ligt niet bij één persoon. Een veelheid van personen binnen een organisatie is betrokken om aan de vereisten van de wet- en regelgeving te kunnen voldoen.

B.02 Organieke inbedding				
Criterium	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.			
Doel	Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG.			
Risico	Door het ontbreken van een goede en inzichtelijke taakverdeling en de daarvoor benodigde middelen en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de AVG, de sectorspecifieke wetgeving en het privacybeleid niet effectief worden ingevuld.			
Referentie	AVG	UAVG		
	Art. 5, 37, 38, 39	Art. 39		

[16] AVG Art. 40.
Zie ook: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-gedragscode ;
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-gedragscode#aan-welke-eisen-moet-een-gedragscode-voldoen-6576

B.02 Organieke inbedding	
Indicatoren en maatregelen	
/01 Verdeling taken en verantwoordelijkheden	
/01.01	De eindverantwoordelijke voor een gegevensverwerking is degene die het doel en de middelen van de gegevensverwerking heeft vastgesteld; het is te allen tijde duidelijk wie deze verantwoordelijke is.
/01.02	De verwerkingsverantwoordelijke en de verwerker hebben (de beschikking over) een Functionaris gegevensbescherming, als ten minste één van de volgende situaties aan de orde is: • *Het betreft een overheidsinstantie of overheidsorgaan*: de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken; • *Een stelselmatige observatie op grote schaal is vereist*: een verwerkingsverantwoordelijke of de verwerker is hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; • *De gegevens betreffen bijzondere categorieën persoonsgegevens, strafrechtelijke veroordelingen of strafbare feiten*: de verwerkingsverantwoordelijke of de verwerker is hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, conform U.01/04 of AVG Art. 9, en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, conform U.01/05 of AVG Art. 10. In overige situaties kunnen of moeten, indien wettelijk verplicht, de verwerkingsverantwoordelijke of de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een FG hebben aangewezen.
/01.03	Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken om de rechtmatigheid van de gegevensverwerking te garanderen schriftelijk vastgesteld en vastgelegd in een overeenkomst.
/01.04	De taken, verantwoordelijkheden en bevoegdheden zijn duidelijk belegd in een TVB-matrix (Taken, Verantwoordelijkheden, Bevoegdheden) waarbij ook de onderlinge relaties tussen de verschillende verantwoordelijken en verwerkers inzichtelijk zijn gemaakt.
/02 Benodigde middelen	
/02.01	Gekoppeld aan het privacybeleid voorziet de organisatie voldoende en aantoonbaar in de benodigde middelen voor de uitvoering ervan.
/03 Rapporteringslijnen	
/03.01	De rapportage- en verantwoordingslijnen tussen de betrokken verantwoordelijken, verwerkers en - indien aangesteld - de FG zijn vastgesteld en vastgelegd.

Toelichting /01 Verdeling taken en verantwoordelijkheden

/01.02 De AP houdt een register bij van FG's.

/01.02 Eisen aan de FG:

a. *Bereikbaarheid*. Een concern kan één FG benoemen, op voorwaarde dat de FG vanuit elke vestiging makkelijk te contacteren is. Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan met inachtneming van hun organisatiestructuren en omvang één FG worden aangewezen voor verschillende dergelijke instanties of organen.

b. *Voor een of meerdere organisaties*. De FG kan optreden voor verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.

c. *Professionele kwaliteiten*. De FG wordt aangewezen op grond van zijn professionele kwaliteiten en in het bijzonder zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming.
Hij moet bijvoorbeeld over toereikende kennis beschikken van de organisatie, van de gegevensverwerkingen die zich binnen de organisatie afspelen, van de belangen die daarbij betrokken zijn en uiteraard kennis van de privacywetgeving die op de verwerkingen binnen zijn organisatie van toepassing is. Hij moet betrouwbaar zijn en het vermogen hebben alle bij de verwerkingen betrokken belangen op een onafhankelijke wijze tegen elkaar te kunnen afwegen. Hij moet met name de volgende taken kunnen vervullen:
   - Informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken over hun verplichtingen uit hoofde van de AVG en andere wettelijke gegevensbeschermingsbepalingen;
   - Toezien op het naleven van de AVG, van andere wettelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
   - Desgevraagd verstrekken van advies met betrekking tot de DPIA en het toezien op de uitvoering daarvan;
   - Samenwerken met de AP;
   - Optreden als contactpunt voor de AP inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging ten behoeve van de gegevensbeschermingseffectbeoordeling (DPIA - zie B.03 Risicomanagement, Privacy by Design en de DPIA) en waar passend, overleg plegen over enige andere aangelegenheid.
   - Naar behoren rekening houden met de aan verwerkingen verbonden risico's en met de aard, de omvang, de context en de verwerkingsdoeleinden.

d. *Positie*. De FG kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of de taken op grond van een dienstverleningsovereenkomst verrichten. De FG vervult zijn taken in onafhankelijkheid waarbij de verwerkingsverantwoordelijke de FG ondersteunt om de taken naar behoren uit te

kunnen voeren. Dit betekent onder meer dat hem daartoe de benodigde menskracht en middelen ter beschikking worden gesteld. De FG geniet ontslagbescherming voor de wijze waarop hij invulling geeft aan de taakuitvoering.
De FG is in het algemeen met betrekking tot de uitvoering van zijn taken binnen de geldende wetgeving gehouden tot geheimhouding of vertrouwelijkheid. Hij heeft in het bijzonder ook een geheimhoudingsplicht ten aanzien van hetgeen hem of haar op grond van een klacht of een verzoek van een betrokkene is bekend geworden, tenzij de betrokkene toestemt in bekendmaking. [17]

e. *Andere taken*. De FG kan andere taken en plichten vervullen. Deze taken of plichten mogen niet tot een belangenconflict leiden.

/01.04 De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de FG zijn taken kan uitvoeren:

a. *Het naar behoren en tijdig betrekken*. De FG wordt naar behoren en tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
b. *Het verschaffen van toegang*. De FG heeft voor het vervullen van zijn taken en het in stand houden van zijn deskundigheid toegang tot persoonsgegevens en verwerkingsactiviteiten en de daarvoor benodigde middelen.
c. *Het niet ontvangen van instructies*. De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.
d. *Het bieden van contactmogelijkheden*. Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de AVG.
e. *Bekendmaking*. De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de FG bekend en deelt die mee aan de AP.

Toelichting /02 Benodigde middelen

/02.01 Gekoppeld aan het privacybeleid voorziet de organisatie voldoende en aantoonbaar in de benodigde middelen om te kunnen voldoen aan het privacybeleid; waaronder:

- De middelen voor interne bewustwording en doelgroepgerichte training van medewerkers op privacybestendig werken;
- De middelen voor het faciliteren van transparantie voor betrokkenen (zoals inzage);
- De (technische) mogelijkheid om persoonsgegevens te kunnen corrigeren;
- De (technische) mogelijkheid om persoonsgegevens te anonimiseren of verwijderen;
- De middelen voor (publieks)voorlichting;
- De middelen voor adequaat en onafhankelijk toezicht, bijvoorbeeld door de toewijzing van een FG.

2.1.3 B.03 Risicomanagement, Privacy by Design en de DPIA

[17] UAVG Art. 39.

Risicomanagement is een continu proces dat de privacyrisico's signaleert, beoordeelt en een passende behandeling daarvan bewaakt. Privacy-risicomanagement richt zich op het beheersen van privacyrisico's bij het verwerken, waaronder verzamelen, opslaan en doorgeven van persoonsgegevens. Door middel van privacy-risicomanagement worden, bij de ontwikkeling, de inrichting en de inzet van de gegevensverwerking voor de organisatie de privacyrisico's in lijn gebracht met het privacybeleid (zie: B.01). Zo wordt voldaan aan de wet- en regelgeving en worden de belangen van de betrokkenen gewaarborgd.

B.03 Risicomanagement, Privacy by Design en de DPIA				
Criterium	De verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen.			
Doelstelling	Beoordeling van de privacyrisico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht.			
Risico	Privacyrisico's worden niet of niet tijdig gesignaleerd, waardoor de verwerking van de persoonsgegevens niet aan de AVG voldoet en een grote(re) kans loopt op inbreuken op de beveiliging; dit kan leiden tot schade voor natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.			
Referentie	AVG	UAVG		
	Art. 24, 25, 35, 36, 42			
/01 Het beoordelen van de privacyrisico's				
/01.01	Wanneer waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen bestaat, in het bijzonder wanneer gelet op de aard, de omvang, de context en de doeleinden nieuwe technologieën worden gebruik, wordt voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd. [18]			
/01.02	Wanneer een Functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een DPIA diens advies in.			
/01.03	Ten minste wanneer sprake is van een verandering van het risico dat een verwerking inhoudt, verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de gewijzigde verwerking overeenkomstig de DPIA wordt uitgevoerd. [19]			
/01.04	Wanneer uit een DPIA blijkt dat de verwerking een hoog risico kan opleveren (als de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken), dan raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de AP hierover. [20]			
/02 Passende maatregelen				
/02.01	De maatregelen bestaan uit technische en organisatorische maatregelen.			

[18] AVG Art. 35 lid 1.
[19] AVG Art. 35 lid 11.
[20] AVG Art. 36.

B.03 Risicomanagement, Privacy by Design en de DPIA	
/02.02	Passende maatregelen zijn genomen door bij het ontwerp de principes van gegevensbescherming te hanteren (privacy by design) en door het hanteren van standaardinstellingen (privacy by default).[21]
/02.03	De maatregelen zijn blijvend passend door het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's).
/02.04	De resultaten van de DPIA worden gebruikt om de organisatie (beter) bewust te maken van het belang om aan privacybescherming te doen.
/03 Aantonen	
/03.01	Van alle verwerkingen waarop een DPIA is uitgevoerd is een DPIA-rapportage beschikbaar, waardoor bekend is welke risico's bestaan en welke maatregelen genomen (moeten) worden.
/03.02	Een procesbeschrijving is aanwezig voor het uitvoeren van DPIA's en voor het opvolgen van de uitkomsten.
/03.03	De risicomanagement aanpak wordt aantoonbaar toegepast, bijvoorbeeld door in de vorm van een plan van aanpak aantoonbaar opvolging te geven aan de aanbevelingen/verbetervoorstellen uit de DPIA's.
/03.04	Een tot standaard verheven DPIA toetsmodel wordt toegepast; dit model voldoet aan de in de AVG gestelde eisen.
/03.05	Privacy by Design en de DPIA maken onderdeel uit van een tot standaard verheven risicomanagement aanpak.

Toelichting /01 Het beoordelen van de privacyrisico's

/01 Een DPIA wordt in een zo vroeg mogelijk stadium uitgevoerd; in ieder geval voordat wordt overgegaan tot de verwerking van persoonsgegevens. Zo kunnen gegevensbeschermingsmaatregelen vooraf al in het ontwerp worden meegenomen. Dit voorkomt dat achteraf blijkt dat de gegevensverwerking niet voldoet aan de verplichtingen die volgen uit de AVG inzake het treffen van passende technische en organisatorische maatregelen om onrechtmatige gegevensverwerkingen te voorkomen. Op deze manier kunnen ook kosten worden bespaard: het meenemen van beveiligingsmaatregelen bij de ontwikkeling van een ICT-systeem is goedkoper dan het achteraf aanpassen ervan. Bovendien kunnen schadevergoedingen worden vermeden, omdat adequate maatregelen zijn genomen om te voorkomen dat voorzienbare risico's zich daadwerkelijk voordoen.

/01 Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

/01 De DPIA bevat ten minste:

1. Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

[21] AVG Art. 25.

2. Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
3. Een beoordeling van de hierboven genoemde risico's, en:
4. De beoogde maatregelen om de risico's aan te pakken; waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

/01.01 Een DPIA in verband met een hoog risico is met name vereist in de volgende gevallen c.q. bij de volgende risico's[22]:

1. Een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
2. Grootschalige verwerking van bijzondere categorieën persoonsgegevens (U.01/04 of AVG Art. 9, lid 1) of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (U.04/05 of AVG Art. 10), of:
3. Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

/01.01 Dit dient met name te gelden voor grootschalige verwerkingen die bedoeld zijn voor de verwerking van een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of supranationaal niveau, waarvan een groot aantal betrokkenen gevolgen kan ondervinden en die bijvoorbeeld vanwege hun gevoelige aard een hoog risico met zich kunnen brengen wanneer conform het bereikte niveau van technologische kennis een nieuwe technologie op grote schaal wordt gebruikt, alsmede voor andere verwerkingen die een groot risico voor de rechten en/of vrijheden van de betrokkenen inhouden, met name wanneer betrokkenen als gevolg van die verwerkingen hun rechten moeilijker kunnen uitoefenen.[23]

/01.01 Een DPIA dient ook te worden uitgevoerd wanneer persoonsgegevens worden verwerkt met het oog op het nemen van besluiten met betrekking tot specifieke natuurlijke personen na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen die is gebaseerd op de profilering van deze gegevens of na de verwerking van bijzondere categorieën persoonsgegevens, biometrische gegevens of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.[24]

/01.01 Een DPIA is ook nodig voor de grootschalige bewaking van openbaar toegankelijke ruimten, met name wanneer optisch elektronische apparatuur wordt gebruikt of voor alle andere verwerkingen waarover de AP oordeelt dat zij waarschijnlijk een groot risico inhouden voor de rechten en vrijheden van betrokkenen, met name omdat betrokkenen als gevolg van deze verwerkingen een recht niet kunnen uitoefenen of geen beroep kunnen doen op een

[22] AVG Art. 35 lid 3.
[23] Grond 91 AVG.
[24] Grond 91 AVG.

dienst of een overeenkomst of omdat deze verwerkingen systematisch op grote schaal worden uitgevoerd.[25]

/01.01 De verwerking van persoonsgegevens mag niet als een grootschalige verwerking worden beschouwd als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat. In die gevallen mag een DPIA niet verplicht worden gesteld.[26]

/01.04 Wanneer de verwerkingsverantwoordelijke de AP raadpleegt, verstrekt hij informatie over[27]:

1. Voor zover van toepassing: de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijke, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerking binnen een concern;
2. De doeleinden en de middelen van de voorgenomen verwerking;
3. De maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG;
4. Voor zover van toepassing: de contactgegevens van de FG;
5. De DPIA, en:
6. Alle andere informatie waar de AP om verzoekt.

[25] Grond 91 AVG.
[26] Grond 91 AVG.
[27] AVG Art. 36 lid 3.

Toelichting /02 Passende maatregelen

/02 De maatregelen zijn passend voor de waarschijnlijkheid en ernst van de risico's voor de rechten en vrijheden van natuurlijke personen. Hierbij wordt rekening houdend met[28]:

- De aard;
- De omvang;
- De context, en:
- Het doel van de verwerking.

/02 Bij het bepalen van wat passend is wordt rekening gehouden met de waarschijnlijkheid en de ernst van de risico's, met name waar de verwerking[29] kan leiden tot:

- Discriminatie;
- Identiteitsdiefstal of -fraude;
- Financiële verliezen;
- Reputatieschade;
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- Het ongeoorloofd ongedaan maken van pseudonimisering, of:
- Enig ander aanzienlijk economisch of maatschappelijk nadeel;

of wanneer:

- Betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- Persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen of vakbondslidmaatschap blijkt en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- Persoonlijke aspecten worden geëvalueerd om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen teneinde persoonlijke profielen op te stellen of te gebruiken;
- Persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt;
- De verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

/02.02 Hierbij wordt gekeken naar de verwerkingsmiddelen en de verwerking.

/02.02 Zie ook de (toekomstige) lijst van de AP waarvoor dit wel en waarvoor dit niet geldt.[30] Uitzondering hierop[31] zijn verwerkingen uit hoofde van een wettelijke verplichting of voor de invulling van algemeen belang (zie U.01).

[28] AVG Art. 24 lid 1.
[29] AVG overweging 75.
[30] Zie lijst verplichte DPIA's van de AP
[31] AVG Art. 35 lid 10.

/02.02 Privacy by design en by default betekent feitelijk dat de verwerkingsverantwoordelijke vanaf het begin privacyoverwegingen betrekt bij het opstellen van nieuw beleid en het ontwerp van nieuwe verwerkingen van persoonsgegevens. [32]

/02.02 Privacy by design voorkomt dure reparatie achteraf.

/02.02 De privacy by design en privacy by default verplichting geldt voor:

- De hoeveelheid verzamelde persoonsgegevens;
- De mate waarin zij worden verwerkt;
- De termijn waarvoor zij worden opgeslagen, en:
- De toegankelijkheid daarvan.

Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. Denk hierbij bijvoorbeeld aan pseudonimisering (zie ook U.04) en *minimale gegevensverwerking* (alleen verwerken wat nodig is).

Toelichting /03 Aantonen

/03.01 De risicomanagementrapportage is niet alleen sturend op uitvoeringsniveau, maar ook op organisatieniveau.

/03.01 Wanneer de rapportage een overzicht bevat van waar privacyrisico's het grootst zijn (risico = kans x impact), dan is dit ondersteunend aan het prioriteren van de verwerkingen waarvan de bescherming en de privacy op niveau moeten worden gebracht. Overigens is (risico = kans x impact) wel een theoretische definitie; in praktijk zal het vaak gaan om de kans dat een incident zich voordoet, of om de kans van optreden van een activiteit waarop het risico berust, in relatie met de potentiële impact die dit incident heeft.

/03.02 Risicomanagement ondersteunt het gehele proces van signaleren tot wegwerken van de gesignaleerde risico's en is als cyclisch proces ingericht.

/03.03 T.b.v. het aantonen van het passend zijn van de maatregelen kan gebruik gemaakt worden van een goedgekeurde gedragscode. [33]

/03.03 Het beschikken over passende maatregelen kan worden aangetoond met behulp van certificering van de verwerking.[34]

[32] Kamerstukken II 2017/18, 34851, nr. 3, paragraaf 5.2.1 (MvT).
[33] AVG Art. 24 lid 3.
[34] AVG Art. 42.

2.2 Het uitvoeringsdomein

Inleiding

In dit hoofdstuk zijn de eisen opgenomen voor de uitvoering van de gegevensverwerking. Het beleid dat op de beleidslaag vanuit het hogere managementniveau is ontwikkeld en bekrachtigd, is leidend voor de invulling van de specifieke aspecten van de gegevensverwerking.

Doelstelling

In het uitvoeringsdomein worden persoonsgegevens daadwerkelijk verwerkt. De verantwoordelijke voor de verwerking moet hier de verwerking realiseren onder de condities en randvoorwaarden die in het beleidsdomein zijn gedefinieerd. Personen waarvan de persoonsgegevens worden verwerkt (betrokkenen) moeten de zekerheid kunnen krijgen dat de verwerking conform de wet- en regelgeving gebeurt.

Risico's

Wanneer richtlijnen voor de specifieke aspecten van de gegevensverwerking ontbreken dan bestaat het risico dat onvoldoende sturing wordt gegeven aan de specifieke aspecten bij de verwerking van persoonlijke gegevens. Dit geeft onduidelijkheid bij de technische en organisatorische inrichting van de gegevensverwerkingen.

2.2.1 U.01 Doelbinding gegevensverwerking

Het uitgangspunt van doelbinding is, dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doel. 'Welbepaald en uitdrukkelijk omschreven' houdt in dat men geen gegevens mag verzamelen *zonder* een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat.

'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. 'Uitdrukkelijk omschreven' houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt moet hebben omschreven.

3.2.1 U.01 Doelbinding gegevensverwerking	
Criterium	De verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven: • De doeleinden, en: • De rechtvaardigingsgronden voor: a. De *verdere verwerking* op grond van de verenigbaarheid met de oorspronkelijke gerechtvaardigde doeleinden; b. De *geautomatiseerde besluitvorming*; c. De *bijzondere categorieën persoonsgegevens*; d. De persoonsgegevens betreffende *strafrechtelijke veroordelingen en strafbare feiten*; e. Het *nationaal identificerend nummer*;

3.2.1 U.01 Doelbinding gegevensverwerking				
	f. De persoonsgegevens ten behoeve van *wetenschappelijk of historisch onderzoek met een statistisch oogmerk en archivering in het algemeen belang*.			
Doelstelling	Het doel van 'Doelbinding gegevensverwerking' is om te waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden.			
Risico	Het ongeoorloofd en onrechtmatig verzamelen en (verder) verwerken van persoonsgegevens.			
Referentie	AVG	UAVG		
	Art. 5, 6, 9, 10, 22, 23	Art. 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 40, 46		
Indicatoren en maatregelen				
/01 Tijdig, welbepaald en uitdrukkelijk omschreven				
/01.01	Het doel is welbepaald en uitdrukkelijk omschreven nog vóórdat de gegevensverwerking begint en wordt niet tijdens het verzamelproces of het verwerkingsproces vastgesteld of gewijzigd. [35]			
/01.02	Van alle gegevens zijn de rechtmatige gronden en de doeleinden van de verzameling en verwerking welbepaald en uitdrukkelijk omschreven en gerechtvaardigd. [36]			
/01.03	Het doel is zodanig vastgelegd (welbepaald) dat het een kader biedt waaraan getoetst kan worden of de gegevens noodzakelijk zijn voor het doel en bij verdere verwerking of de verwerking verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verstrekt. [37]			
/01.04	Het doel is uitdrukkelijk omschreven, dus niet te vaag of te ruim, maar nauwkeurig, specifiek, meetbaar, acceptabel, realistisch en tijdgebonden.			
/02 Doeleinden				
/02.01	De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking, ook wel dataminimalisatie genoemd).			
/02.02	De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan[38]: 1. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden 2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;			

[35] AVG Art. 5 lid 1 en overweging 50.
[36] AVG Art. 5 lid 1b.
[37] AVG Art. 6 lid 4.
[38] AVG Art. 6 lid 1.

3.2.1 U.01 Doelbinding gegevensverwerking	
	3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Deze rechtsgrond moet zijn vastgesteld bij het Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is[39]; 4. De verwerking is noodzakelijk om vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; 5. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze rechtsgrond moet zijn vastgesteld bij het Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is[40]; 6. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Dit onderdeel (punt 6) geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun wettelijke taken.
/02.03	Persoonsgegevens moeten ten opzichte van de betrokkene behoorlijk en transparant worden verwerkt[41] [42]. Hiertoe moet/moeten: a. De gegevensverwerking transparant te zijn (U.02 en U.05). b. De gegevens juist te zijn en zo nodig te worden bijgewerkt (U.03). c. De gegevens passend te worden beveiligd (U.04). d. De gegevens niet langer dan noodzakelijk te worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren is (U.06).
/03 Rechtvaardiging verdere verwerking	
/03.01	De verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, is alleen mogelijk wanneer: 1. De verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld en de verwerkingsverantwoordelijke bij de beoordeling van de verenigbaarheid onder meer rekening houdt met[43]: a. Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking; b. Het kader waarin de persoonsgegevens zijn verzameld, met name wat betreft de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke;

[39] AVG Art. 6 lid 3.
[40] AVG Art. 6 lid 3.
[41] AVG Art. 5.
[42] De AVG is niet van toepassing op de persoonsgegevens van overleden personen (AVG overweging 27).
[43] AVG Art. 6 lid 4.

3.2.1 U.01 Doelbinding gegevensverwerking	
	c. De aard van de persoonsgegevens, met name of bijzondere categorieën persoonsgegevens worden verwerkt[44] en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt[45]; d. De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; e. Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering; of: 2. De verdere verwerking plaatsvindt op basis van de toestemming van betrokkene; of: 3. Wanneer de verdere verwerking berust op een wettelijke bepaling waarbij een specifieke uitzondering geldt.
/03.02	Wanneer de verwerkingsverantwoordelijke zich een verdere verwerking voorneemt dan moet de verwerkingsverantwoordelijke de betrokkene nog vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken (zie U.05). Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld, omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt. [46]
/04 Rechtvaardiging bijzondere categorieën persoonsgegevens	
/04.01	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden[47]. Hierbij is nagegaan of in het Unierecht of lidstatelijk is bepaald of betrokkene het verbod mag opheffen. [48]
/04.02	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt. [49] Tevens geldt hierbij dat het verbod om gegevens over gezondheid te verwerken niet van toepassing is indien de verwerking geschiedt door bestuursorganen, pensioenfondsen,

[44] AVG Art. 9.
[45] AVG Art. 10.
[46] AVG overweging 61.
[47] UAVG Art. 22 lid 2a is de invulling van AVG Art. 9 lid 2a.
[48] Voorbeeld BSN: in Nederland kan een persoon niet zelf alsnog toestemming geven voor de verwerking van het BSN bij het ontbreken van een wettelijke grondslag.
[49] AVG Art. 9 lid 2b.

3.2.1 U.01 Doelbinding gegevensverwerking	
	werkgevers of instellingen die te hunnen behoeve werkzaam zijn, en voor zover de verwerking noodzakelijk is voor: [50] • Een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of • De re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid. Hierbij worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die bevoegd zijn tot verwerking daarvan[51] [52].
/04.03	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven. [53]
/04.04	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking verricht wordt door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt. [54]
/04.05	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. [55]
/04.06	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid. [56]
/04.07	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht:

[50] Artikel 30 lid 1 a en b UAVG
[51] UAVG art 30 lid 1, Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld (UAVG art 30 lid 6).
[52] UAVG Art. 30 lid 4.
[53] UAVG Art.22 lid 2b; AVG Art. 9 lid 2c.
[54] UAVG Art.22 lid 2c, ofwel AVG Art. 9 lid 2d.
[55] UAVG Art.22 lid 2d, ofwel AVG Art. 9 lid 2e.
[56] UAVG Art.22 lid 2e, ofwel AVG Art. 9 lid 2f.

3.2.1 U.01 Doelbinding gegevensverwerking	
	1. Nationaalrechtelijke algemene uitzonderingen[57]: a. De verwerking is noodzakelijk ter voldoening aan een volkenrechtelijke verplichting; b. De gegevens worden verwerkt door de Autoriteit persoonsgegevens of een ombudsman als bedoeld in Art. 9:17 van de Algemene wet bestuursrecht (AWB), en voor zover de verwerking noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken, onder voorwaarde dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of c. De verwerking is noodzakelijk in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt. 2. Uitzonderingen inzake verwerking van persoonsgegevens waaruit ras of etnische afkomst blijkt[58] : a. Verwerking met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is; of b. Verwerking met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen teneinde feitelijke nadelen, verband houdende met de grond ras of etnische afkomst, op te heffen of te verminderen, en slechts voor zover: • De verwerking voor dat doel noodzakelijk is; • De gegevens betrekking hebben op het geboorteland van de betrokkene, diens ouders of diens grootouders, dan wel op andere, bij wet vastgestelde criteria op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een bepaalde etnische of culturele minderheidsgroep behoort; en • De betrokkene tegen de verwerking geen schriftelijk bezwaar heeft gemaakt. 3. De verwerking van persoonsgegevens waaruit politieke opvattingen blijken voor vervulling openbare functies: de verwerking geschiedt met het oog op de eisen die met betrekking tot politieke opvattingen in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges. [59] 4. De verwerking van persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken voor geestelijke verzorging[60]: a. De verwerking geschiedt door andere instellingen dan de instellingen, bedoeld in artikel 22, tweede lid, onderdeel c, en voor zover de verwerking

[57] UAVG Art. 23.
[58] UAVG Art. 25.
[59] UAVG Art. 26.
[60] UAVG Art. 27.

3.2.1 U.01 Doelbinding gegevensverwerking	
	noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar heeft gemaakt. b. Hierbij worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene. 5. De verwerking van genetische gegevens[61]: a. De verwerking vindt plaats met betrekking tot de betrokkene bij wie de desbetreffende gegevens zijn verkregen. b. Hierbij is het verbod om genetische gegevens te verwerken uitsluitend niet van toepassing, indien: • Een zwaarwegend geneeskundig belang prevaleert; of • De verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek dat een algemeen belang dient of ten behoeve van statistiek, indien: • De betrokkene uitdrukkelijke toestemming heeft gegeven; en • Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Deze toestemming is niet vereist, indien het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt. 6. De verwerking van biometrische gegevens[62]: de verwerking vindt plaats ten behoeve van de unieke identificatie van een persoon, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Voor al deze verwerkingen is bepaald dat de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.
/04.08	De verwerking van gegevens over gezondheid vindt niet plaats, tenzij de verwerking geschiedt door[63]: 1. Scholen, voor zover de verwerking met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is; 2. Een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming, de gecertificeerde instelling, bedoeld in artikel 1.1 van de Jeugdwet, of de rechtspersoon, bedoeld in artikel 256, eerste lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover de verwerking noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken; of:

[61] UAVG Art. 28.
[62] UAVG Art. 29.
[63] UAVG Art. 30 lid 2.

3.2.1 U.01 Doelbinding gegevensverwerking	
	3. Onze Minister en Onze Minister van Justitie en Veiligheid voor zover de verwerking in verband met de tenuitvoerlegging van vrijheidsbenemende maatregelen noodzakelijk is. Hierbij worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die bevoegd zijn tot verwerking daarvan[64].
/04.09	De verwerking van bijzondere categorieën persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van zorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker.[65] De verwerking geschiedt door[66]: a. Hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk. Hierbij geldt dat het verbod om andere bijzondere categorieën persoonsgegevens te verwerken niet van toepassing is, indien de verwerking noodzakelijk is in aanvulling op deze verwerking met het oog op een goede behandeling of verzorging van de betrokkene[67]; of b. Verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover de verwerking noodzakelijk is voor: • De beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of • De uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering. Hierbij worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een

[64] UAVG Art. 30 lid 4.
[65] AVG Art. 9 lid 2h.
[66] UAVG Art. 30 lid 3.
[67] UAVG Art. 30 lid 5.

3.2.1 U.01 Doelbinding gegevensverwerking	
	geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die bevoegd zijn tot verwerking daarvan.[68] Als voorwaarde en waarborg geldt dat: a. De gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of b. Door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden. [69]
/04.10	De verwerking van bijzondere categorieën van persoonsgegevens vindt niet plaats, tenzij de verwerking plaatsvindt vanuit het algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.[70]
/04.11	De verwerking van bijzondere categorieën van persoonsgegevens vindt niet plaats, tenzij de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden[71, 72], waarbij[73]: a. Het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en b. Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. [74]
/05 Rechtvaardiging strafrechtelijke veroordelingen en strafbare feiten	
/05.01	Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt[75] indien: a. De betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden; b. De verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

[68] UAVG Art. 30 lid 4.
[69] AVG Art. 9 lid 3 Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld (UAVG art 30 lid 6).
[70] AVG Art. 9 lid 2i.
[71] Doeleinden overeenkomstig AVG Art. 89, lid 1.
[72] AVG Art. 9 lid 2j.
[73] UAVG Art. 24.
[74] De definitie van 'wetenschappelijk of historisch onderzoek' is te vinden in AVG overweging 159.
[75] UAVG Art. 32.

3.2.1 U.01 Doelbinding gegevensverwerking	
	c. De verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; d. De verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.
/05.02	Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (inclusief een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag) of daarmee verband houdende veiligheidsmaatregelen mogen worden verwerkt[76] indien: a. De verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verwerkingsverantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens (WPG) of de Wet justitiële en strafvorderlijke gegevens (WJSG); b. De verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken, indien: • De verwerking noodzakelijk is voor de uitvoering van de taak van deze verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken; en • Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of: c. De verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in de UAVG Art. 30, derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene; d. Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt: • Ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren, of: • Ter bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn; e. Persoonsgegevens van strafrechtelijke aard over personeel in dienst van de verwerkingsverantwoordelijke mogen uitsluitend worden verwerkt, indien dit geschiedt overeenkomstig de regels die zijn vastgesteld in overeenstemming met de procedures in de Wet op de ondernemingsraden voor zover het persoonsgegevens van strafrechtelijke aard over personeel in dienst van de verwerkingsverantwoordelijke betreft;

[76] UAVG Art. 33.

3.2.1 U.01 Doelbinding gegevensverwerking	
	f. Persoonsgegevens van strafrechtelijke aard mogen ten behoeve van derden worden verwerkt, indien: • Door verwerkingsverantwoordelijken die optreden krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (WPBR); • Door een verwerkingsverantwoordelijke die tevens rechtspersoon is en in dezelfde groep is verbonden als bedoeld in artikel 2:24b van het Burgerlijk Wetboek, of: • Door een verwerkingsverantwoordelijke die hiervoor van de AP een vergunning heeft verkregen.
/06 Rechtvaardiging gebruik nationaal identificerend nummer	
/06.01	Het bepalen van een nummer dat ter identificatie van een persoon bij wet is voorgeschreven wordt slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden die bij de wet zijn bepaald[77]: • Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak[78] gebruik maken van het burgerservicenummer (BSN), zonder dat daarvoor nadere regelgeving vereist is. • Voor instellingen die geen beroep kunnen doen op Wabb Art. 10 dient het gebruik te zijn voorgeschreven in sectorale wetgeving. • De wet Digitale overheid (voorheen: Wet generieke digitale infrastructuur - GDI) maakt het noodzakelijk dat er ook voor private partijen een wettelijke grondslag komt voor het verwerken van het BSN in het kader van authenticatie[79].
/07 Rechtvaardiging geautomatiseerde besluitvorming	
/07.01	Een betrokkene wordt niet onderworpen aan een geautomatiseerde individuele besluitvorming, tenzij het besluit[80]: a. Noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke, of: b. Is toegestaan bij de wet- en regelgeving die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, of: c. Berust op de uitdrukkelijke toestemming van de betrokkene.
/07.02	Indien geautomatiseerde besluitvorming plaatsvindt heeft de verwerkingsverantwoordelijke passende maatregelen getroffen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op

[77] UAVG Art. 46.
[78] Dus met een specifieke wettelijke grondslag.
[79] https://wetten.overheid.nl/BWBR0048156/2023-07-01
[80] AVG Art. 22 lid 1.

3.2.1 U.01 Doelbinding gegevensverwerking	
	menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten. [81] Indien de verwerkingsverantwoordelijke geen bestuursorgaan is, dan zijn passende maatregelen in ieder geval getroffen indien het recht op menselijke tussenkomst, het recht voor betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten, zijn geborgd. [82]
/07.03	Indien geautomatiseerde besluitvorming plaatsvindt, waarbij bijzondere categorieën persoonsgegevens worden gebruikt, dan zijn daarbij passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene getroffen. [83]
/08 Rechtvaardiging wetenschappelijk of historisch onderzoek met een statistisch oogmerk en archivering in het algemeen belang	
/08.01	De verwerking van bijzondere categorieën persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek en archivering in het algemeen belang vindt plaats voor zover deze aan de vereisen uit /04.11 voldoen.[84]
/08.02	Verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of archivering vindt alleen plaats, als passende technische en organisatorische maatregelen zijn getroffen om de rechten en vrijheden van de betrokkene te beschermen door[85]: • Minimale gegevensverwerking te garanderen; • Ervoor te zorgen dat de betrokkene niet meer geïdentificeerd kan worden, bijvoorbeeld door middel van pseudonimisering of anonimisering.

Toelichting /01 Tijdig welbepaald en uitdrukkelijk omschreven

/01.04 Het verzamelen en verwerken van persoonsgegevens 'uitsluitend omdat dat in de toekomst misschien wel handig kan zijn', is als doel niet voldoende welbepaald en daarom onrechtmatig.

/01.04 Gegevens mogen voor meerdere doelen verzameld en verwerkt worden[86]. Voor al deze doelen afzonderlijk geldt dat ze tijdig moeten worden vastgesteld, gerechtvaardigd zijn en welbepaald en uitdrukkelijk zijn omschreven.

/01.04 Een voldoende SMART omschrijving houdt in:

1. Specifiek: de doelstelling is eenduidig;
2. Meetbaar: er zijn meetbare/observeerbare voorwaarden waardoor het doel bereikt kan worden;
3. Acceptabel: het doel is acceptabel voor de doelgroep en/of management en iemand neemt zijn verantwoordelijkheid voor het juist realiseren van dit doel;
4. Realistisch: de doelstelling is haalbaar;
5. Tijdgebonden: er is bepaald wanneer (in de tijd) het doel bereikt moet zijn.

[81] AVG Art. 22 lid 2.
[82] UAVG Art. 40.
[83] AVG Art. 22 lid 3.
[84] UAVG Art. 24; AVG Art. 9 lid 2j.
[85] AVG Art. 5 lid 1e.
[86] Handleiding Algemene Verordening Gegevensbescherming, Ministerie van Justitie en Veiligheid, 2018, pag. 35.

Toelichting /02 Gerechtvaardigde doelen

/02 Ook een verwerking die noodzakelijk is in het kader van een overeenkomst of een voorgenomen overeenkomst, dient rechtmatig te zijn[87] en daarmee aan de vereisten van /02 te voldoen.

/02.02 Voor de private sector zijn doorgaans de onderdelen 1, 2, 4 en 6 een basis voor verwerking van persoonsgegevens. Ook onderdeel 3 kan een basis zijn voor verwerking van persoonsgegevens in de private sector wanneer er sprake is van een wettelijke verplichting voor een private partij. [88]

/02.02 Voor de overheid is met name verwerking op basis van een wettelijke verplichting (onderdeel 3) en verwerking in het belang van uitvoering van een taak van algemeen belang (onderdeel 5) relevant. Deze beide rechtsgrondslagen voor de overheid moeten worden vastgesteld bij het wettelijke recht dat op de verwerkingsverantwoordelijke van toepassing is. [89]

Voorwaarde voor rechtmatige verwerking in het kader van een wettelijke verplichting is dat de verwerking noodzakelijk is om te voldoen aan de wettelijke verplichting. De wettelijke verplichting tot verstrekking van persoonsgegevens is doorgaans zeer precies vastgelegd in sectorspecifieke regelgeving. Dit is echter niet noodzakelijkerwijs het geval. Denkbaar is ook dat verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht. In dat geval heeft de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid inzake het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan de wettelijke verplichting. Op dit punt is het wettelijk kader, zoals dat gold onder de WBP, niet veranderd. [90]

/02.02 Met betrekking tot de rechtsgrond 'uitvoering van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag' (hierna ook kortweg: 'publieke taak') moet het doel van de verwerking noodzakelijk zijn voor de vervulling van die taak. Naar zijn aard is de publieke taak dynamisch en veranderlijk door de tijd heen. De grenzen van de publieke taak zijn niet altijd op voorhand scherp te trekken. De publieke taak zelf zal echter altijd moeten blijken uit de sectorspecifieke regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de sectorspecifieke regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Met de wettelijke grondslag voor de publieke taak[91] is tevens een grondslag gegeven voor de verwerking van persoonsgegevens. Het doel van de gegevensverwerking is daarbij naar zijn aard wel gebonden aan de uitoefening van die publieke taak en de ruimte voor gegevensverwerking vindt hierin zijn begrenzing. De publiekrechtelijke taak zelf zal moeten blijken uit de voor de verwerkingsverantwoordelijke relevante wettelijke bepalingen. [92]

---

[87] AVG overweging 44.
[88] AVG overweging 46.
[89] AVG Art. 6 lid 3.
[90] AVG overweging 46.
[91] AVG Art. 6 lid 1.
[92] AVG overweging 46.

/02.02 De publieke taak noch de gegevensverwerking hoeft uitputtend te zijn geregeld in een wet in formele zin. Voldoende is dat de hoofdlijnen kenbaar zijn uit de wet. Deze lezing strookt ook met het uitgangspunt van het EVRM[93] inzake beperking van grondrechten, waarbij de beperking van het privéleven voorzienbaar moet zijn bij wet[94]. Het begrip 'voorzienbaar bij wet' wordt hierbij opgevat als een materieel wetsbegrip, dat niet beperkt is tot wetten in formele zin[95]. In de kern gaat het er om dat voor het individu duidelijk moet zijn, dat zijn persoonsgegevens met betrekking tot een specifieke publieke taak worden verwerkt. Dit kan ook, zoals nu in sommige gevallen wordt aangenomen, volgen uit een samenstel van wettelijke regels die tezamen een publieke taak aanduiden. Het begrip publieke taak moet dus breed worden gelezen, mede in het licht van de overwegingen bij de AVG, maar die publieke taak moet wel voldoende duidelijk blijken uit nationaal recht. AVG Art. 6, lid 1e is geen zelfstandige rechtsbasis voor gegevensverwerking, gelet op het derde lid van deze bepaling.

/02.02 Als van het doel van de verwerking de rechtmatigheid wordt vastgesteld en als de verwerking betrekking heeft op het algemeen belang volgens punt 5): "noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke", dan kan die rechtsgrond specifieke bepalingen bevatten om de toepassing van de regels van de AVG aan te passen, met inbegrip van de algemene voorwaarden inzake[96]:

- De rechtmatigheid van verwerking door de verwerkingsverantwoordelijke;
- De types verwerkte gegevens;
- De betrokkenen;
- De entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt;
- De doelbinding;
- De opslagperioden, en:
- De verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX van de AVG.

/02.02 Met betrekking tot onderdelen 3 en 5 geldt dat het Nederlands recht moet beantwoorden aan een doelstelling van algemeen belang en evenredig moet zijn met het nagestreefde gerechtvaardigde doel. [97]

/02.02 Bij onderdeel 6 is voor de overheid van belang dat dit onderdeel niet geldt voor overheidsinstanties in het kader van de uitoefening van hun taak. Overheidsinstanties zullen bij het uitoefenen van hun taak geen gebruik kunnen maken van de grondslag 'gerechtvaardigd belang', maar zullen voor dit gebruik moeten kunnen aangeven dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Dit geldt niet voor zover de

[93] Link naar het verdrag.
[94] AVG Art. 8 lid 2.
[95] AVG overweging 41.
[96] Overweging 45 AVG.
[97] AVG Art. 6.

overheidsinstantie 'typisch bedrijfsmatige handelingen' verricht waarbij persoonsgegevens worden verwerkt, zoals de verwerking van persoonsgegevens die noodzakelijk is voor de beveiliging van overheidsgebouwen. Voor handelingen die buiten de uitoefening van de wettelijke taak vallen mag wel een grondslag worden aangenomen in het gerechtvaardigd belang van de organisatie. De overheid onderscheidt zich hierin niet wezenlijk van een private partij. [98]

Toelichting /03 Rechtvaardiging voor verdere verwerking

/03 'Verdere verwerking' ziet in de AVG op alle verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Dit kan verwerking door een en dezelfde verwerkingsverantwoordelijke zijn, maar kan ook de basis zijn voor verstrekking van gegevens aan een andere verwerkingsverantwoordelijke.

/03 Om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer rekening houden met[99]:

- Een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking;
- Het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan;
- De aard van de persoonsgegevens;
- De gevolgen van de voorgenomen verdere verwerking voor de betrokkenen, en:
- Passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen.

/03 De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (doelbinding).

/03 Verdere verwerking voor zuiver commerciële doelstellingen, zoals het gericht kunnen aanbieden van reclame, kan niet hierop worden gebaseerd. Dat kan alleen met uitdrukkelijke toestemming van de betrokkene.

/03.01 Mogelijkheid #1 voor verdere verwerking is 'verenigbaarheid'. De verwerkingsverantwoordelijke mag gegevens verder verwerken voor een ander doel mits dat andere doel verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. [100] De verwerkingsverantwoordelijke moet dit zelf vaststellen. Ook verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden blijft mogelijk op voorwaarde dat passende waarborgen voor de bescherming van de persoonsgegevens van de betrokkenen, bijvoorbeeld pseudonimisering. [101.]

[98] AVG overweging 47.
[99] AVG overweging 50.
[100] AVG Art. 5 lid 1b.
[101] Over de scope van 'wetenschappelijk of historisch onderzoek' zie AVG overweging 159.

/03.01 Mogelijkheid #2 voor verdere verwerking is gebaseerd op de toestemming van de betrokkene, ook wanneer deze niet verenigbaar is met het doel van de oorspronkelijke verwerking van persoonsgegevens. De aanvaardbaarheid van verdere verwerking op basis van toestemming is in zekere zin een vanzelfsprekendheid. Met de toestemming komt immers tot uitdrukking dat betrokkene zelf de inbreuk op de persoonlijke levenssfeer, die plaatsvindt bij de verwerking van persoonsgegevens, niet bezwaarlijk acht. De toestemming dient wel expliciet en vrijelijk te worden gegeven. [102] De verwerkings-verantwoordelijke hoeft in geval van toestemming niet te toetsen aan het vereiste van verenigbaarheid.

/03.01 Mogelijkheid #3 voor verdere verwerking is gebaseerd op de wet- en regelgeving die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de bedoelde doelstellingen. De verdere verwerking hoeft ook in dat geval niet verenigbaar te zijn met het oorspronkelijke doel waarvoor de gegevens zijn verzameld en de verwerkingsverantwoordelijke hoeft dan ook niet te toetsen aan het vereiste van verenigbaarheid. [103] De verdere verwerking door de verwerkingsverantwoordelijke is dan gebaseerd op de lidstaatrechtelijke bepaling (een specifieke wettelijke bepaling dus). Gaat het om de nationale veiligheid? Dan valt volgens de MvT verder verwerken onder het regime van WPG/WJSG of de Wet op de inlichtingen en veiligheidsdiensten (WIV).
In andere gevallen moet de verwerkingsverantwoordelijke het verder verwerken toetsen (en motiveren/documenteren) aan de criteria om verenigbaarheid vast te stellen zoals weergegeven onder U.01/02.02.

/03.01 Als de verdere verwerking wordt verricht op basis van mogelijkheid 3, doordat de verwerkingsverantwoordelijke hiertoe wettelijk is verplicht of als de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag, dan dient de verwerking een grondslag te hebben in het wettelijke recht. De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen op grond van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of voor verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang, dan wel voor een taak in het kader van de uitoefening van het openbaar gezag.
Het moet ook het Nederlands recht zijn dat het doel van de verwerking bepaalt. Voorts zou dat recht een nadere omschrijving kunnen geven van de algemene voorwaarden van de AVG, waaraan de persoonsgegevensverwerking moet voldoen om rechtmatig te zijn, en van specificaties voor het bepalen van de verwerkingsverantwoordelijke, het type verwerkte persoonsgegevens, de betrokkenen, de entiteiten waaraan de persoonsgegevens mogen worden vrijgegeven, de doelbinding, de opslagperiode en andere maatregelen om te zorgen voor rechtmatige en behoorlijke verwerking. Ook dient in het wettelijke recht te worden vastgesteld of de verwerkingsverantwoordelijke, die is belast met een taak van algemeen belang dan wel met een taak in het kader van de uitoefening van het openbaar gezag, een overheidsinstantie of een andere publiekrechtelijke persoon moet zijn, of een

[102] AVG Art. 7 en 8.
[103] AVG Art. 6, tweede deel lid 4.

privaatrechtelijke persoon moet zijn, zoals een beroepsvereniging, indien zulks is gerechtvaardigd om redenen van algemeen belang, waaronder gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming en het beheer van gezondheidszorgdiensten. [104]

/03.01 De verwerking van persoonsgegevens dient ook als rechtmatig te worden beschouwd als zij noodzakelijk is voor de bescherming van een belang dat voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is. Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan als de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd. Sommige typen persoonsgegevensverwerking kunnen zowel gewichtige redenen van algemeen belang als de vitale belangen van de betrokkene dienen, bijvoorbeeld wanneer de verwerking noodzakelijk is voor humanitaire doeleinden, onder meer voor het monitoren van een epidemie en de verspreiding daarvan of in humanitaire noodsituaties, met name bij natuurrampen of door de mens veroorzaakte rampen. [105]

/03.01 Specifieke uitzonderingsgronden zijn de volgende:[106]

1. De nationale veiligheid;
2. Landsverdediging;
3. De openbare veiligheid;
4. De voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
5. Andere belangrijke doelstellingen van algemeen belang van de EU of van een lidstaat, met name een belangrijk economisch of financieel belang van de EU of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
6. De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
7. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
8. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen;
9. De bescherming van de betrokkene of van de rechten en vrijheden van anderen;
10. De inning van civielrechtelijke vorderingen.

Toelichting /04 Rechtvaardiging voor verwerking bijzondere categorieën persoonsgegevens

/04.04 Als het bij verkiezingsactiviteiten voor de goede werking van de democratie in een lidstaat vereist is dat politieke partijen persoonsgegevens over de politieke opvattingen van personen verzamelen, kan de verwerking van zulke gegevens op grond van een algemeen belang worden toegestaan mits passende waarborgen worden vastgesteld. [107]

[104] AVG overweging 45.
[105] AVG overweging 46.
[106] AVG Art. 23.
[107] AVG overweging 56.

/04.04 Bovendien vindt de verwerking van persoonsgegevens door overheidsinstanties ter verwezenlijking van in het constitutionele recht of in het volkenrecht vastgelegde doelstellingen van officieel erkende religieuze verenigingen plaats op grond van een algemeen belang. [108]

/04.07 Genetische gegevens moeten worden gedefinieerd als persoonsgegevens met betrekking tot de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die blijken uit een analyse van een biologisch monster van de persoon in kwestie, met name een chromosoomanalyse, een analyse van desoxyribonucleïnezuur (DNA) of van ribonucleïnezuur (RNA) of uit een analyse van andere elementen waarmee soortgelijke informatie kan worden verkregen. [109]

/04.07 Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens. [110]

/04.07 Foto's worden niet systematisch beschouwd als verwerking van bijzondere categorieën persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.[111]

/04.09 Persoonsgegevens over gezondheid zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven[112].

Deze gegevens hebben betrekking op de gezondheidstoestand van een betrokkene en die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst. Dit omvat informatie over de natuurlijke persoon die is verzameld in het kader van de registratie voor of de verlening van gezondheidszorgdiensten als bedoeld in Richtlijn 2011/24/EU van het Europees Parlement en de Raad aan die natuurlijke persoon; een aan een natuurlijke persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van die natuurlijke persoon geldt voor gezondheidsdoeleinden; informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van genetische gegevens en biologische monsters en informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron, zoals een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitro diagnostiek. [113]

/04.09 Bijzondere categorieën persoonsgegevens, die betere bescherming vergen, mogen alleen voor gezondheidsdoeleinden worden verwerkt als dat nodig is om die doeleinden te

[108] AVG overweging 55.
[109] AVG overweging 34.
[110] AVG Art. 4 lid 14.
[111] AVG overweging 51.
[112] AVG Art. 4 lid 15.
[113] AVG overweging 35.

verwezenlijken in het belang van natuurlijke personen en de samenleving als geheel. Dit geldt met name bij:

- Het beheer van gezondheidszorgdiensten en -stelsels of sociale diensten en stelsels van sociale diensten, met inbegrip van de verwerking door de beheer autoriteiten en de centrale nationale gezondheidsinstanties van die gegevens met het oog op kwaliteitscontrole, beheerinformatie en het algemeen nationaal en lokaal toezicht op:
  - Het gezondheidszorgstelsel, of:
  - Het stelsel van sociale diensten.
- Bij het waarborgen van de continuïteit van de gezondheidszorg of de sociale diensten en grensoverschrijdende gezondheidszorg.
- Voor doeleinden inzake gezondheidsbeveiliging, -bewaking en -waarschuwing, of:
- Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden op basis van het wettelijk recht die aan een doelstelling van algemeen belang moet voldoen, alsook:
- Voor studies van algemeen belang op het gebied van de volksgezondheid.

Derhalve moet de AVG voorzien in geharmoniseerde voorwaarden voor de verwerking van bijzondere categorieën persoonsgegevens over de gezondheid, in geval van specifieke behoeften, met name indien deze gegevens met het oog op bepaalde gezondheidsdoeleinden worden verwerkt door personen die wettelijk aan het beroepsgeheim gebonden zijn. Het wettelijke recht moet voorzien in specifieke en passende maatregelen voor de bescherming van de grondrechten en persoonsgegevens van natuurlijke personen.

Het moet de lidstaten worden toegestaan andere voorwaarden te handhaven of in te voeren, waaronder beperkingen met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid. Wanneer deze voorwaarden van toepassing zijn op de grensoverschrijdende verwerking van deze persoonsgegevens, dan mag dit evenwel geen belemmering vormen voor het vrije verkeer van gegevens binnen de Unie. [114]

/04.09 Het kan om redenen van algemeen belang op het gebied van de volksgezondheid nodig zijn om bijzondere categorieën persoonsgegevens zonder toestemming van de betrokkene te verwerken. Die verwerking moet worden onderworpen aan passende en specifieke maatregelen ter bescherming van de rechten en vrijheden van natuurlijke personen. In dit verband dient "volksgezondheid" overeenkomstig de definitie van Verordening (EG) nr. 1338/2008 van het Europees Parlement en de Raad te worden uitgelegd als alle elementen in verband met de gezondheid, namelijk gezondheidstoestand, inclusief morbiditeit en beperkingen, de determinanten die een effect hebben op die gezondheidstoestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheidszorg, de verstrekking van en de universele toegang tot gezondheidszorg, alsmede de uitgaven voor en de financiering van de gezondheidszorg en de doodsoorzaken. Dergelijke verwerking van persoonsgegevens over gezondheid om redenen van algemeen belang mag er niet toe

[114] AVG overweging 53.

te leiden dat persoonsgegevens door derden zoals werkgevers of verzekeringsmaatschappijen en banken voor andere doeleinden worden verwerkt. [115]

Toelichting /05 Rechtvaardiging voor verwerking van gegevens i.v.m strafrechtelijke veroordelingen en strafbare feiten

/05 Opsporingsinstanties dienen eerst na te gaan of Richtlijn (EU) 2016/680 van 27 april 2016 van toepassing is inzage de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens.

/05 De bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid en het vrije verkeer van die gegevens wordt geregeld in een specifieke rechtshandeling van de Unie. De AVG mag derhalve niet van toepassing zijn op de met die doeleinden verrichte verwerkingsactiviteiten. Overeenkomstig de AVG door overheidsinstanties verwerkte persoonsgegevens die voor die doeleinden worden gebruikt, moeten vallen onder een meer specifieke rechtshandeling van de Unie, namelijk Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad. De lidstaten kunnen bevoegde autoriteiten in de zin van Richtlijn (EU) 2016/680 taken opdragen die niet noodzakelijk worden verricht met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zodat de verwerking van persoonsgegevens voor die andere doeleinden binnen het toepassingsgebied van de AVG valt, voor zover zij binnen het toepassingsgebied van de Uniewetgeving valt. [116]

/05 Het aanwijzen van mogelijke strafbare feiten of gevaren voor de openbare veiligheid door de verwerkingsverantwoordelijke en de doorzending van de desbetreffende persoonsgegevens in individuele zaken of in verschillende zaken die met hetzelfde strafbare feit of dezelfde gevaren voor de openbare veiligheid te maken hebben, aan een bevoegde instantie moeten worden beschouwd als zijnde in het gerechtvaardigde belang van de verwerkingsverantwoordelijke. De doorgifte in het gerechtvaardigde belang van de verwerkingsverantwoordelijke of de verdere verwerking van persoonsgegevens moeten evenwel worden verboden wanneer de verwerking niet verenigbaar is met een wettelijke, beroepsmatige of anderszins bindende geheimhoudingsplicht. [117]

Toelichting /06 Rechtvaardiging gebruik nationaal identificerend nummer

/06 AVG Art. 87 geeft een grondslag om bij lidstatelijk recht specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer. UAVG Art. 46 regelt het gebruik van wettelijk voorgeschreven nummers. Dit artikel bepaalt dat een nummer dat ter

[115] AVG overweging 54.
[116] AVG overweging 19.
[117] AVG overweging 50.

identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. In feite is dit een kapstokbepaling op basis waarvan in andere wetten invulling kan worden gegeven aan dergelijke nummers.

/06 De MvT bij de UAVG zegt erover: "Aldus is een afweging op het niveau van de formele wet in beginsel gegarandeerd. Er is met andere woorden voor gekozen om op dit punt geen delegatie door de formele wetgever toe te staan en eventuele andere gebruiksdoeleinden dienen derhalve door de formele wetgever zelf te worden vastgesteld. Wel is het op grond van het tweede lid mogelijk om bij algemene maatregel van bestuur andere gevallen aan te wijzen waarin een persoonsnummer mag worden gebruikt. Ook bestaat hier voor verdere verwerking van een dergelijk nummer dus geen ruimte voor een eigen afweging van de verwerkingsverantwoordelijke."[118]

/06 Voor de overheid is het gebruik van een uniek persoonsnummer, het burgerservicenummer (BSN), geregeld in Wabb Art. 10. Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer zonder dat daarvoor nadere regelgeving vereist is. Voor instellingen die geen beroep kunnen doen op Wabb Art. 10 dient het gebruik te zijn voorgeschreven in sectorale wetgeving. Zo geldt bijvoorbeeld voor de zorgsector de Wet gebruik burgerservicenummer in de Zorg en moeten banken het BSN gebruiken voor uitwisseling van gegevens met de Belastingdienst. Daarnaast zijn andere identificerende nummers in gebruik, bijvoorbeeld het onderwijsnummer, dat overeenkomt met het burgerservicenummer tenzij de deelnemer geen burgerservicenummer heeft.

Toelichting /07 Rechtvaardiging geautomatiseerde individuele besluitvorming

/07.01 De betrokkene dient het recht te hebben niet te worden onderworpen aan een louter op geautomatiseerde verwerking gebaseerd besluit[119].

/07.01 Het begrip 'besluit' in de zin van de AVG dient hierbij ruimer te worden gelezen dan het besluitbegrip uit de AWB; ook private partijen vallen onder de reikwijdte van deze bepaling wanneer ze gebruik maken van geautomatiseerde besluitvorming. [120]

/07.01 Wanneer sprake is van uitoefening van gebonden bevoegdheden met geringe beoordelingsruimte, heeft menselijke tussenkomst bij besluitvorming in beginsel geen meerwaarde. De risico's die de verordening beoogt in te dammen doen zich hier feitelijk niet voor. [121] Ook de private sector heeft enige ruimte om, bij de vervulling van wettelijke verplichtingen, gebruik te maken van geautomatiseerde besluitvorming, anders dan op basis van profilering, zonder menselijke tussenkomst. [122]

---

[118] UAVG MvT, toelichting bij UAVG art 46; daar staat ook: "Uit een oogpunt van bescherming van de persoonlijke levenssfeer is het noodzakelijk geacht om aan het gebruik van identificatienummers beperkingen te stellen. Vast staat immers dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen".

[119] AVG overweging 66.

[120] UAVG MvT, toelichting op artikel 22.

[121] Toelichting op AVG art 38.

[122] Toelichting AVG op art 38.

/07.01 De negatieve kenmerken van een bepaalde groep mogen niet tegengeworpen worden aan een individu. Het individu hoeft deze kenmerken namelijk helemaal niet te hebben.[123]

/07.01 Kinderen hebben met betrekking tot hun persoonsgegevens recht op specifieke bescherming, aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens. Die specifieke bescherming moet met name gelden voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. In de context van preventieve of adviesdiensten die rechtstreeks aan een kind worden aangeboden is de toestemming van de persoon die de ouderlijke verantwoordelijkheid draagt niet vereist. [124]

/07.01 Indien de geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, is toegestaan bij de wet- en regelgeving is dit toegestaan, omdat dit noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is ter uitvoering van een taak van algemeen belang. [125]

/07.02 De maatregelen zijn passend ter bescherming van het gerechtvaardigd belang van de betrokkene. [126]

/07.03 In aanvulling van de maatregelen ter bescherming van het gerechtvaardigd belang van de betrokkene wordt de betrokkene de logica meegedeeld die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens. [127]

Toelichting /08 Rechtvaardiging verwerking i.v.m. wetenschappelijk of historisch onderzoek of met een statistisch oogmerk en archivering in het algemeen belang

/08 Verwerkingen ten behoeve van wetenschappelijk of historisch onderzoek of met een statistisch oogmerk worden op meerdere plaatsen in de AVG geadresseerd. Allereerst worden verdere verwerkingen ten behoeve van wetenschappelijk onderzoek niet als onverenigbaar beschouwd met het vereiste van doelbinding. Ook mogen persoonsgegevens ten behoeve van wetenschappelijk onderzoek langer worden opgeslagen, mits passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen. [128] Deze bepalingen werken rechtstreeks in de Nederlandse rechtsorde en behoeven geen omzetting naar Nederlands recht.

/08 Voor de verwerking van bijzondere categorieën persoonsgegevens ten behoeve van wetenschappelijk of historisch onderzoek of statistische doeleinden staan twee wegen open. In de eerste plaats is verwerking mogelijk op basis van uitdrukkelijke toestemming van de betrokkene. Ten aanzien van verwerkingen voor wetenschappelijk onderzoek geldt dat uitdrukkelijke toestemming van de betrokkenen een eigen, specifieke betekenis heeft. Het is vaak niet mogelijk op het ogenblik waarop de persoonsgegevens worden verzameld het

[123] Kamerstukken *II* 2017/18, 34851, nr. 3, p. 46 (MvT)
[124] AVG overweging 38.
[125] Toelichting AVG Art. 38 lid 1 /UAVG art 40 lid 1.
[126] Toelichting AVG Art. 38 lid 2 /UAVG art 40 lid 2.
[127] Toelichting AVG Art. 38 lid 3.
[128] AVG Art. 5 lid 1b en 1e.

doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Daarom moet de betrokkene worden toegestaan toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. De betrokkene moet de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat.[129]

De tweede mogelijkheid betreft de situatie waarin de uitdrukkelijke toestemming van de betrokkene niet kan worden verkregen of een onevenredige inspanning kost. Dan kan de verwerking alsnog plaatsvinden mits aan de overige voorwaarden genoemd in artikel 28 van de UAVG wordt voldaan. [130] De verwerking moet dan vanzelfsprekend ook voldoen aan de overige van toepassing zijnde voorwaarden van de AVG en UAVG.

[129] Grond 33 AVG en artikel 24 UAVG
[130] AVG Art. 28.

2.2.2 U.02 Register van verwerkingsactiviteiten

Om de naleving van de AVG aan te kunnen tonen dient de verwerkingsverantwoordelijke of de verwerker een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden.[131] Binnen een organisatie kan dit via gegevensmanagement worden vastgelegd. De vastlegging maakt duidelijk hoe de verschillende organisatieonderdelen de bedrijfsprocessen ondersteunen en welke beveiligingsmaatregelen (op hoofdlijnen) zijn getroffen voor de verwerkingen en betrokkenen. Het register maakt toezicht op de verwerkingsactiviteiten mogelijk.

U.02 Register van verwerkingsactiviteiten				
Criterium	De verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.			
Doelstelling	Het doel van een 'Register van verwerkingsactiviteiten' is inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens.			
Risico	Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.			
Referentie	AVG	UAVG		
	Art. 30			
Indicatoren en maatregelen				
/01 Register				
/01.01	Elke verwerkingsverantwoordelijke houdt een register bij van de verwerkings-activiteiten die onder hun verantwoordelijkheid plaatsvinden, tenzij er een uitzonderingsgrond is (/01.06). In voorkomend geval gebeurt de registratie door een vertegenwoordiger van de verwerkingsverantwoordelijke.			
/01.02	Het register van de verwerkingsverantwoordelijke met de verwerkingsactiviteiten bevat alle volgende gegevens[132]: 1. De naam en de contactgegevens van: a. De verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en: b. In voorkomend geval: • Van de vertegenwoordiger van de verwerkingsverantwoordelijke, en: • Van de Functionaris voor gegevensbescherming; 2. De verwerkingsdoeleinden; 3. Een beschrijving van de categorieën van betrokkenen;			

[131] AVG overweging 82.
[132] AVG Art. 30 lid 1.

U.02 Register van verwerkingsactiviteiten	
	4. Een beschrijving van de categorieën persoonsgegevens; 5. De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; 6. Bij doorgiften aan een derde land of een internationale organisatie: a. De doorgifte van verstrekte persoonsgegevens b. De vermelding van dat derde land of die internationale organisatie c. De documenten inzake de passende waarborgen; 7. De beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist (indien mogelijk); 8. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (indien mogelijk).
/01.03	De verwerker houdt een register bij van alle categorieën van verwerkingsactiviteiten die ten behoeve van de verwerkingsverantwoordelijke plaatsvinden, tenzij er een uitzonderingsgrond is (/01.06). In voorkomend geval gebeurt de registratie door een vertegenwoordiger van de verwerker.
/01.04	Het register van de verwerker met alle categorieën van verwerkingsactiviteiten bevat alle volgende gegevens[133]: 1. De naam en de contactgegevens van: a. De verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en: b. In voorkomend geval: • Van de vertegenwoordiger van de verwerkingsverantwoordelijke, en: • Van de Functionaris voor gegevensbescherming; 2. De categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd; 3. Bij doorgiften aan een derde land of een internationale organisatie: a. De doorgifte van verstrekte persoonsgegevens b. De vermelding van dat derde land of die internationale organisatie c. De documenten inzake de passende waarborgen; 4. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (indien mogelijk).
/01.05	Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.[134]
/01.06	Het register hoeft niet te worden bijgehouden indien: [135] 1. De onderneming of organisaties minder dan 250 personen in dienst heeft,

[133] AVG Art. 30 lid
[134] Artikel 30 lid 3 AVG.
[135] Artikel 30 lid 5 AVG.

U.02 Register van verwerkingsactiviteiten	
	2. Het niet waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, 3. De verwerking incidenteel is, en: 4. Geen verwerking plaatsvindt van bijzondere categorieën van gegevens of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten.
/02 Actueel en samenhangend beeld	
/02.01	De registers van de verwerkingsverantwoordelijke en van de verwerker geven één samenhangend beeld.
/02.02	Op verzoek van de AP wordt middels de registers een actueel beeld gegeven.
/02.03	De onderlinge samenhang (gegevensstromen) en afhankelijkheden zijn benoemd en beschreven tussen: • De bedrijfsprocessen; • Organisaties en organisatieonderdelen; • De verwerkingen; • De locaties waar persoonsgegevens worden opgeslagen; • De gegevensuitwisselingen (binnen en buiten de eigen organisatie); • De systemen.
/02.04	Bij wijzigingen in bestaande en nieuwe verwerkingen worden de resultaten vanuit de gegevensbeschermingseffectbeoordeling (DPIA) meegenomen als onderdeel van de opname van de verwerking in het register.

Toelichting /01 Register

/01 Het bijhouden van het register van gegevensverwerkingen kan worden uitgevoerd door een gecentraliseerd onderdeel. Dit verbetert de mogelijkheden een actueel en samenhangend beeld te geven. Dit wordt dan doorgaans door het onderdeel Gegevensmanagement uitgevoerd.

Toelichting /02 Actueel en samenhangend beeld

/02.01 De onderlinge samenhang en afhankelijkheden tussen alle in elkaar grijpende componenten, die betrokken zijn bij de verwerking van de persoonsgegevens, zijn benoemd en beschreven.

/02.03 Er kan behoefte zijn aan informatie over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de persoonsgegevens als bijvoorbeeld bijzondere computerprogrammatuur een wijze van verwerking mogelijk maakt die de betrokkene op het eerste gezicht niet geheel duidelijk is. Dit hoeft niet zo ver te gaan dat het Auteursrecht en/of het Intellectuele Eigendomsrecht, dat de software beschermt, of het bedrijfsgeheim geschonden wordt.

/02.04 De beschrijving van onderlinge afhankelijkheden geeft inzicht in de context van een verwerking en geeft bij veranderingen aan een verwerkingsproces inzicht in de gevolgen voor andere verwerkingen en omgekeerd.

/02.04 Als gevolg van veranderingen in de context, in het dreigingsbeeld, veranderingen op organisatorisch vlak, veranderingen in de stand der techniek of veranderingen van de verwerkingen, kunnen wijzigingen teweegbrengen in de verwerking zelf of in de waarborgen voor de veilige verwerking. Het register moet actuele relevante informatie bevatten die inzicht geeft in de compliance status en de beoordeling van de mate waarin de waarborgen passend zijn voor de verwerking.

2.2.3 U.03 Kwaliteitsmanagement

Kwaliteitsmanagement zorgt voor de processen die bij onjuistheid en onnauwkeurigheid van de gegevens of bij ongewenste verwerking de gegevens rectificeren, volledig maken, wissen, de verwerking beperken of toestemming tot verwerking intrekken.

U.03 Kwaliteitsmanagement				
Criterium	De verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit gebeurt op verzoek van betrokkene dan wordt deze over de status van de afhandeling geïnformeerd.			
Doelstelling	'Kwaliteitsmanagement' moet ervoor zorgen dat een gegevensverwerking correct en in overeenstemming met de wens van betrokkenen is.			
Risico	Wanneer de gegevens onjuist of onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene getrokken met negatieve consequenties of naar het oordeel van betrokkene ongewenste verwerking van zijn of haar persoonsgegevens tot gevolg.			
Referentie	AVG	UAVG		
	Art. 7 lid 3, 11 lid 2, 12, 16, 17, 18, 19, 20, 21, 22, 23			
Indicatoren / Maatregelen				
/01 Juistheid en nauwkeurigheid				
/01.01	De verwerkingsverantwoordelijke heeft de nodige maatregelen getroffen om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen.			
/01.02	De verwerkingsverantwoordelijke voert periodiek controles uit op de juiste werking van de getroffen maatregelen en brengt hierover rapportages uit aan het hogere management.			
/02 Gecorrigeerd, gestaakt of overgedragen				
/02.01	Op verzoek van betrokkene worden onjuiste persoonsgegevens gerectificeerd. [136]			
/02.02	Op verzoek van betrokkene worden onvolledige persoonsgegevens vervolledigd (met inachtneming van de doeleinden van de verwerking), onder meer op basis van een aanvullende verklaring van betrokkene. [137]			

[136] AVG Art. 16 .
[137] AVG Art. 16

U.03 Kwaliteitsmanagement	
/02.03	Op verzoek van de betrokkene worden de hem betreffende persoonsgegevens gewist wanneer een van de volgende gevallen van toepassing is[138]: a. De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt; b. De betrokkene trekt de toestemming waarop de verwerking berust in en er is geen andere rechtsgrond voor de verwerking; c. De betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking. d. De persoonsgegevens zijn onrechtmatig verwerkt; e. De persoonsgegevens moeten worden gewist om te voldoen aan een in het wettelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust; f. De persoonsgegevens van kinderen jonger dan 16 jaar zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.
/02.04	Bij bezwaar van betrokkene wordt de verwerking gestaakt, tenzij er dwingende gerechtvaardigde gronden voor de verwerking kunnen worden aangevoerd die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. [139]
/02.05	Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen om verwerkingsverantwoordelijken die de persoonsgegevens verwerken ervan op de hoogte te stellen, dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar of kopie of reproductie van die persoonsgegevens te wissen. [140]

[138] AVG Art. 17 lid 1.
[139] AVG Art. 21 lid 1.
[140] AVG Art. 17 lid 2.

U.03 Kwaliteitsmanagement	
/02.06	Op verzoek van betrokkene wordt de verwerking beperkt, indien[141]: a. De juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren; b. De verwerking onrechtmatig en de betrokkene zich verzet tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan; c. De verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of: d. De betrokkene bezwaar heeft gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.
/02.07	De betrokkene heeft het recht de hem betreffende persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt[142], als de verwerking berust op: a. Toestemming van betrokkene, of: b. Een overeenkomst waarbij de betrokkene partij is of de verwerking via geautomatiseerde procedés wordt verricht; en geldt niet als: a. De verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend; b. Het afbreuk doet aan de rechten en vrijheden van anderen.
/02.08	De betrokkene kan de gegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere laten overdragen indien /02.07 geldt en dit technisch mogelijk is.[143]
/03 Geïnformeerd	
/03.01	De verwerkingsverantwoordelijke stelt iedere ontvanger, aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie, gegevenswissing of verwerkingsbeperking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt. [144]
/03.02	***vervallen***

[141] Artikel 18 lid 1 AVG.
[142] AVG Art. 20.
[143] Artikel 20 lid 2 AVG.
[144] AVG Art. 19.

U.03 Kwaliteitsmanagement	
/03.03	De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het correctieverzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.[145]
/03.04	Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt; tenzij de betrokkene anderszins verzoekt. [146]
/03.05	De verwerkingsverantwoordelijke reageert schriftelijk of met andere middelen; indien passend met elektronische middelen. Als de betrokkene daarom verzoekt kan de informatie, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is, mondeling worden meegedeeld. [147]
/03.06	Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven en informeert hij hem over de mogelijkheid om een klacht in te dienen bij de AP en beroep bij de rechter in te stellen. [148]
/03.07	Als de verwerkingsverantwoordelijke kan aantonen dat hij de betrokkene niet kan identificeren, stelt hij de betrokkenen daarvan zo mogelijk in kennis. Betrokkene kan aanvullende gegevens verstrekken om identificatie mogelijk te maken. [149]

Toelichting /01 Juistheid en nauwkeurigheid

/01.01 De 'nodige maatregelen' zijn die maatregelen die in redelijkheid van de verwerkingsverantwoordelijke kunnen worden verwacht. Wat in redelijkheid kan worden verwacht hangt af van de soort gegevens, de stand van de techniek en de kosten die met de maatregelen gepaard gaan. Het zorg dragen voor juistheid en nauwkeurigheid van de persoonsgegevens is daarmee een inspanningsverplichting voor de verwerkingsverantwoordelijke en geen resultaatverplichting. Van de genomen maatregelen is aangetoond dat onderzocht en beoordeeld is dat deze maatregelen toereikend zijn. Voorbeelden van nodige maatregelen zijn:

1. Het inregelen van de (technische) mogelijkheid om te kunnen corrigeren;
2. Het vaststellen en bekrachtigen wanneer en door wie de periodieke controles op de juistheid, nauwkeurigheid, actualiteit, volledigheid en correct gebruik van de gegevens plaatsvinden en door wie de persoonsgegevens - indien nodig - gecorrigeerd worden;
3. Het identificeren en beperken van personen en afdelingen die toegang hebben tot de persoonsgegevens, waarbij tevens zekerheid wordt verkregen over de wijze waarop

[145] Artikel 12 lid 3.
[146] AVG Art. 12 lid 3.
[147] AVG Art. 12 lid 1.
[148] AVG Art. 12 lid 4.
[149] AVG Art. 11 en 12; zie ook AVG overweging 57.

de juistheid van gegevens bij toegang is gewaarborgd en dat de gegevens niet voor andere doeleinden worden gebruikt dan voor de vereiste doelstelling;

4. Het identificeren en beperken van partijen aan wie persoonsgegevens mogen worden verstrekt, waarbij tevens zekerheid wordt verkregen over de wijze waarop de juistheid van de gegevens bij verstrekking is gewaarborgd en dat de gegevens niet voor andere doeleinden worden gebruikt dan de vereiste doelstelling;
5. Het identificeren van de gevolgen van het onjuist gebruik van persoonsgegevens en of hoe deze gevolgen kunnen worden ondervangen;
6. Het bij aanstellen van een verwerker:
   a. Aantonen dat is onderzocht en beoordeeld dat de desbetreffende verwerker, gelet op de aard van de werkzaamheden en de daaraan gekoppelde privacyrisico's, voldoende kwaliteit biedt;
   b. De geheimhoudingsplicht is geborgd, door deze vast te stellen en vast te leggen in de verwerkersovereenkomst.

/01.01 Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, dan mag de verwerkingsverantwoordelijke een redelijke vergoeding aanrekenen, in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan, of: weigeren gevolg te geven aan het verzoek. Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen[150].

Toelichting /02 Gecorrigeerd, gestaakt of overgedragen

/02.01 Het recht op correctie kan worden beperkt door middel van wettelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn. [151]

/02.03 Het recht op *gegevenswissing* ('recht op vergetelheid') is niet van toepassing voor zover verwerking nodig is:

1. Voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
2. Voor het nakomen van een in een het wettelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
3. Om redenen van algemeen belang op het gebied van volksgezondheid;
4. Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, voor zover het recht op gegevenswissing de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
5. Voor de instelling, uitoefening of onderbouwing van een rechtsvordering. [152]

/02.06 Het recht de verwerking te beperken geldt als de verwerking (inclusief profilering) plaatsvindt voor[153]:

[150] AVG Art. 12 lid 5.
[151] AVG Art. 23 lid 1.
[152] AVG Art. 17 lid 3.
[153] AVG Art. 21 lid 1.

1. De vervulling van een taak van algemeen belang;
2. De vervulling van een taak van het openbaar gezag;
3. De behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is;
4. Direct marketing, of:
5. Wetenschappelijk of historisch onderzoek of statistische doeleinden, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Toelichting /03 Geïnformeerd

/03.07 De verwerkingsverantwoordelijke kan, wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene. [154]

2.2.4 U.04 Beveiligen van de verwerking van persoonsgegevens

Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen, alsmede procedures en processen om eventuele gevolgen van beveiligingsincidenten tot een acceptabel (passend), vooraf bepaald niveau te beperken. De maatregelen zijn gebaseerd op een risicoanalyse en wettelijke verplichtingen (waaronder - in het geval van persoonsgegevens - ook de AVG).

U.04 Beveiligen van de verwerking van persoonsgegevens				
Criterium	De verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen voor de verwerking van persoonsgegevens op een passend beveiligingsniveau[155].			
Doelstelling	Het doel van 'beveiligen van de verwerking van persoonsgegevens' is persoonsgegevens te beschermen tegen verlies, onbeschikbaarheid, corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.			
Risico	Het ongewenst openbaar worden, manipulatie, misbruik en niet beschikbaar zijn van gegevens.			
Referentie	AVG	UAVG		
	Art. 32	MvT §5.2.4		
Indicatoren en maatregelen				
/01 Technische en organisatorische maatregelen				
/01.01	De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de toegang beperkt is tot diegenen die toegang moeten hebben voor het uitvoeren van hun functie of taken of tot diegenen die daartoe wettelijk zijn gehouden[156].			

[154] AVG Art. 12 lid 6 en overwegingen 58, 59.
[155] AVG Art. 32.
[156] AVG Art. 32 lid 3.

U.04 Beveiligen van de verwerking van persoonsgegevens	
/01.02	Persoonsgegevens zijn fysiek beveiligd tegen diefstal en ongewenste toegang: 1. Als persoonsgegevens op fysieke wijze bestaan, zijn deze ook fysiek beschermd. 2. De wijze van verzameling van gegevens is niet privacygevoelig.
/01.03	Persoonsgegevens zijn organisatorisch beveiligd door middel van maatregelen voor de inrichting van de organisatie, welke zijn opgenomen in een informatiebeveiligingsplan.
/01.04	De maatregelen waarborgen een passend beveiligingsniveau en bevatten onder meer[157]: 1. De pseudonimisering en versleuteling van persoonsgegevens; 2. Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen; 3. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen; 4. Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
/02 Passend niveau	
/02.01	De technische, organisatorische en fysieke beveiligingsmaatregelen bieden voor alle verwerkingen van persoonsgegevens een passend beschermingsniveau en dit kan worden aangetoond. De maatregelen zijn daartoe proportioneel en subsidiair.
/02.02	De beveiligingsmaatregelen zijn gebaseerd op een analyse van het verwerkingsrisico (risicoanalyse). Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met verwerkingsrisico's als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig. [158]
/02.03	Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurde certificering kan worden gebruikt om aan te tonen dat de maatregelen passend zijn.

Toelichting/01 Technische en organisatorische maatregelen

/01.01 Maatregelen ter beperking van de toegang kunnen onder meer bestaan in het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens. [159] Technische maatregelen zijn maatregelen in en rondom informatiesystemen, zoals toegangscontroles, vastlegging van gebruik en back-up, wachtwoordbescherming en encryptie. De beveiliging is niet beperkt tot de eigen informatiesystemen, maar strekt zich uit tot extern geplaatste back-up en de opslag en verwerking bij en door derden. [160]

[157] AVG Art. 32. Dit is 'het informatiebeveiligingsartikel'.
[158] AVG Art. 32 lid 2.
[159] AVG overweging 78.
[160] Het ontvangen van een back-up en de opslag van persoonsgegevens zijn 'verwerkingen' van persoonsgegevens.

/01.01 Fysieke persoonsgegevens worden ook fysiek beschermd, denk hierbij aan bijvoorbeeld gebouwzonering en sloten op kasten.

/01.03 De verantwoordelijke heeft adequate organisatorische maatregelen genomen om de gegevens te beveiligen *en kan dat aantonen*. Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens, zoals toekenning en deling van de verantwoordelijkheden, bevoegdheden, instructies, trainingen, calamiteitenplannen en geheimhoudingsplichten. Een goede manier om dit te borgen en aan te tonen is het opstellen en actueel houden van een beveiligingsplan.

/01.03 De AVG spreekt in plaats van een beveiligingsplan over Bindende bedrijfsvoorschriften: "de toepassing van de algemene beginselen inzake gegevensbescherming, met name doelbinding, minimale gegevensverwerking, beperkte opslagtermijnen, kwaliteit van gegevens, gegevensbescherming door standaardinstellingen en door ontwerp, rechtsgrond voor verwerking, verwerking van bijzondere categorieën persoonsgegevens, maatregelen om gegevensbeveiliging te waarborgen en de vereisten inzake verdere doorgiften aan organen die niet door bindende bedrijfsvoorschriften zijn gebonden.

/01.03 Ten behoeve van privacy hoeft geen separaat beveiligingsplan gemaakt te worden; als extra beveiligingsmaatregelen genomen moeten worden om persoonsgegevens te bescherming, kan dit worden opgenomen in het reguliere beveiligingsplan. Ook de Richtsnoeren van de AP over het beveiligen van persoonsgegevens kan geïmplementeerd worden in het reguliere beveiligingsplan.

/01.03 Het beveiligingsplan bevat bijvoorbeeld informatie over:

1. Welke technische, organisatorische en fysieke beveiligingsmaatregelen genomen zijn
2. Welk normenstelsel de organisatie volgt;
3. Op welke wijze de eventuele aanwijzingen (richtsnoeren, beleidsregels) van de AP over het beveiligen van persoonsgegevens ingeregeld zijn;
4. Hoe geheimhouding van de medewerkers geregeld is;
5. Welke acties de verantwoordelijke verwerker neemt bij datalekken;
6. Hoe de verwerker zich periodiek verantwoordt over de nakoming van afspraken;
7. Hoe controle op de naleving van de beveiligingsmaatregelen is ingeregeld;
8. Het geven van instructies en trainingen over de manier waarop persoonsgegevens beschermd worden;
9. Een calamiteitenplan (of: het calamiteitenplan zelf);
10. Het cyclisch inregelen van beveiliging als onderdeel van de dagelijkse praktijk van de organisatie, zodat de beveiligingsmaatregelen onderdeel zijn van de dagelijkse praktijk van de organisatie;
11. De opname van de technische en organisatorische maatregelen in de verwerkersovereenkomst, met voortdurende controle op de uitvoering ervan en direct ingrijpen als daar niet aan wordt voldaan;
12. De periodieke toetsing van maatregelen en aanpassing als ze niet meer voldoende bescherming bieden;
13. De toekenning en deling van de verantwoordelijkheden en bevoegdheden met de omgang van persoonsgegevens;

14. Het benoemen van een algehele verantwoordelijke binnen de organisatie voor het opstellen, implementeren en handhaven van het beveiligingsbeleid.

/01.04 Privacy Enhancing Technologies (PET) is een gangbare verzamelnaam voor een aantal technieken voor privacybescherming die kunnen worden toegepast. Een centraal principe van PET is het verminderen van de herleidbaarheid van persoonsgegevens naar de betrokkene, met anonimisering van gegevens als zwaarste vorm: na anonimisering zijn de gegevens niet meer te herleiden tot de oorspronkelijke gegevens en daarmee ook niet langer een onderwerp voor de AVG. [161]

/01.04 Een verwante techniek is pseudonimisering. De AVG definieert pseudonimisering als: "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, op voorwaarde dat deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld"[162].

/01.04 Bij het toepassen van pseudonimisering moeten de aanvullende gegevens, die gebruikt worden om de persoonsgegevens aan een specifieke betrokkene te koppelen, apart worden bewaard.

/01.04 De uitdrukkelijke invoering van pseudonimisering genoemd in de AVG is niet bedoeld om andere gegevensbeschermingsmaatregelen uit te sluiten. [163] Na pseudonimisering blijft de AVG van toepassing.

/01.04 Bijzondere aspecten in dit verband zijn:

- Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist. [164]
- De verwerkingsverantwoordelijke dient, met name met betrekking tot online-diensten en online-identificatoren, alle redelijke maatregelen te nemen om de identiteit te controleren van een betrokkene die om inzage verzoekt. [165]

Toelichting /02 Passend niveau

/02.01 Bij het bepalen van het passende niveau dient rekening gehouden te worden met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. [166]

/02.01 Een verwerkingsverantwoordelijke maakt alleen gebruik van diensten van verwerkers die afdoende garanties bieden voor het toepassen van de vereiste technische en organisatorische maatregelen.[167]

/02.01 Er hoeft niet voor de zwaarste technische beveiliging gekozen te worden, *maar voor de meest adequate*. De NEN-ISO 27001/27002 en daaraan gerelateerde overheidsnormen -

---

[161] Borking, J., Privacyrecht is code. *Over het gebruik van Privacy Enhancing Technologies*, Kluwer, Den Haag, 2010, pag. 117 en CBP, *Richtsnoeren voor het beveiligen van persoonsgegevens*, Den Haag, 2013, pag. 13.
[162] AVG Art. 4 lid 5.
[163] AVG Art. 4 lid 5.
[164] AVG overweging 39.
[165] AVG overweging 64.
[166] AVG overweging 83.
[167] AVG Art. 28 lid 1.

zoals de Baseline Informatieveiligheid Overheid (BIO) - zijn momenteel de standaard baselines om te komen tot een 'adequate' beveiliging. [168]

/02.01 Voor de BIO geldt daarbij dat een 'verklaring van toepasselijkheid' moet worden opgesteld. Een VvT of SOA (statement of applicability) is een document waarmee een organisatie vastlegt welke Beheersmaatregelen zijn geïmplementeerd op het gebied van informatiebeveiliging. [169]

/02.01 Om aan de hand van de risicoanalyse het passend beschermingsniveau vast te stellen wordt voldaan aan de volgende kwaliteitseisen[170]:

a. Beschikbaarheid (de ongestoorde voortgang van de gegevensverwerking): de persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarvoor gemaakte afspraken en de wettelijke voorschriften.
b. Integriteit (de juistheid van de gegevens): de persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
c. Vertrouwelijkheid (ook wel: Exclusiviteit van de gegevens): uitsluitend bevoegde personen hebben toegang tot de persoonsgegevens.
d. Controleerbaarheid (het achteraf kunnen verifiëren of aan bovenstaande kwaliteitseisen is voldaan): de mate waarin het mogelijk is om te achterhalen dat de verwerking van persoonsgegevens overeenkomstig de hiervoor genoemde kwaliteitsaspecten is uitgevoerd.

/02.01 De verwerkingsverantwoordelijke kan de maatregelen aantonen door beleidsmaatregelen te nemen en maatregelen toe te passen die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (zie B.03).

/02.01 Als met geringe extra kosten meer beveiliging kan worden bewerkstelligd, dan moeten deze als 'passend' worden beschouwd terwijl kosten, die disproportioneel zijn in verhouding tot de extra beveiliging die daardoor zou worden verkregen, niet worden vereist.

/02.02 In de risicoanalyse wordt het gewenste niveau van beveiliging vastgesteld. Door een risicoanalyse uit te voeren wordt inzichtelijk welke maatregelen waar nodig zijn om welke risico's te beheersen. Daarbij moet proportionaliteit zijn tussen de beveiligingsmaatregelen en de aard van te beschermen gegevens. Naarmate de gegevens bijv. een vertrouwelijker karakter hebben of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Sommige gegevens zijn naar hun aard vertrouwelijker (zoals bijzondere categorieën persoonsgegevens zoals ras, religie, seksuele voorkeur, biometrische gegevens en inloggegevens), andere gegevens worden vertrouwelijk als ze in een bepaalde context

---

[168] Zwenne, G.J. en Knol. PC., *Tekst en Commentaar Telecommunicatie- en Privacyrecht*, Kluwer, Deventer, 2013, pag. 726.

[169] De ISO27001 zegt er in hoofdstuk 6.1.3, lid d het volgende over: "(…) een verklaring van toepasselijkheid op te stellen die de benodigde beheersmaatregelen bevat, een rechtvaardiging voor het opnemen ervan, de informatie of ze zijn geïmplementeerd of niet, en de rechtvaardiging om beheersmaatregelen van bijlage A uit te sluiten". Zie: https://www.informatiebeveiligingdoejezo.nl/verklaring-van-toepasselijkheid-nuttig-noodzakelijk-kwaad/.

[170] Borking, J., Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies, Kluwer, Den Haag, 2010, pag. 117 en CBP, Richtsnoeren voor het beveiligen van persoonsgegevens, Den Haag, 2013, pag. 13.

worden geplaatst (bijv. gegevens over uithuisplaatsing van een minderjarige, of over de financiële situatie van een persoon). Een bijkomende vuistregel: hoe groter de verzameling van persoonsgegevens van een specifieke betrokkene is, des te risicovoller en daarmee vertrouwelijker deze gegevens kunnen worden.

/02.02 Het niveau van de technische, organisatorische en fysieke maatregelen wordt periodiek geëvalueerd en zo nodig geactualiseerd zodat het niveau passend blijft. [171]

/02.02 Als sprake is van bijzondere categorieën persoonsgegevens, uniek identificerende gegevens (zoals BSN's, vingerafdrukken, biometrische gegevens) of gegevens over kwetsbare groepen, personen of gebruikersnamen, wachtwoorden en andere inloggegevens, dan vraagt dit om extra aandacht in de risicoanalyse en eventuele maatregelen. [172]

2.2.5 U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens

Wie persoonsgegevens verstrekt aan een organisatie heeft het recht te weten waarvoor, op welke wijze en door wie deze gegevens worden gebruikt. De organisatie heeft hiertoe een informatieplicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen worden ontvangen.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens				
Criterium	De verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.[173]			
Doelstelling	Het doel van 'Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens' is om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking, zodat de betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking. [174]			
Risico	De organisatie is niet transparant, waardoor de organisatie niet kan verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking, met mogelijk hoge kosten tot gevolg.			
Referentie	AVG	UAVG		
	Art. 13, 14 en 15	Art. 5, 22, 24, 27, 28, 32, 41		
Indicatoren en maatregelen				
/01 Tijdig				

[171] Een 'Information Security Management System (ISMS)' biedt een organisatie een procesbenadering voor het beheersen van de informatiebeveiliging. ISO/IEC 27001 is daarvoor de norm. Dit normdocument beschrijft het cyclische proces (plan/do/check/act) voor het bepalen van beveiligingsdoelstellingen op basis van een risicobeoordeling, het treffen van maatregelen en het monitoren en beoordelen van de uitkomsten. Zie voor informatiebeveiliging in de zorg: https://www.werkenmetnen7510.nl.

[172] De lidstaten kunnen de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer of enige andere identificator van algemene aard nader vaststellen (AVG Art. 87).

[173] AVG Art. 14.

[174] AVG Art. 12 en overweging 60.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
/01.01	De toestemming van de betrokkene wordt verkregen voorafgaand aan de verwerking[175], het doorgeven aan derden en het verder verwerken. [176] Dit geldt voor persoonsgegevens die via betrokkenen of anderen worden of zijn verkregen.
/01.02	Informatie over de niet van betrokkene verkregen persoonsgegevens wordt binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens aan betrokkene verstrekt. [177]
/02 Informatie	
/02.01	Het verzoek om toestemming wordt in een begrijpelijke en gemakkelijk toegankelijke vorm opgesteld, in duidelijke en eenvoudige taal zodanig dat precies duidelijk is waarvoor betrokkene toestemming geeft en zodanig dat een duidelijk onderscheid kan worden gemaakt van andere aangelegenheden waarvoor eventueel ook toestemming wordt gevraagd. [178]
/02.02	Wanneer persoonsgegevens bij de betrokkene worden verzameld, ontvangt de betrokkene de volgende informatie[179]: a. De identiteit en contactgegevens van de verantwoordelijke en, in voorkomend geval, zijn of haar vertegenwoordiger; b. In voorkomend geval de contactgegevens van de Functionaris voor gegevensbescherming; c. De verwerkingsdoeleinden en ook de rechtsgrond van de gegevensverwerking; d. De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is[180]; e. In voorkomend geval de ontvangers of categorieën van ontvangers van persoonsgegevens; f. In voorkomend geval dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of internationale organisatie of een adequaatheidsbesluit van de commissie bestaat, welke de passende waarborgen zijn en hoe deze kunnen worden ingezien; g. De periode dat de gegevens worden opgeslagen of de criteria ter bepaling van die termijn;

[175] AVG Art. 6 lid 1.
[176] AVG Art. 14 lid 3.
[177] AVG Art. 14 lid 3.
[178] AVG Art. 7 lid 2.
[179] AVG Art. 13.
[180] AVG Art. 6 lid 1 f

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
	h. Dat de betrokkene recht heeft op inzage, rectificatie of wissing of beperking van de hem betreffende verwerking en het recht heeft bezwaar tegen de verwerking te maken en dat de betrokkene het recht heeft op gegevensoverdraagbaarheid; i. Dat de betrokkene zijn toestemming te allen tijde kan intrekken (voor zover de verwerking is gebaseerd op de rechtsgrond toestemming); j. Dat de betrokkene een klacht mag indienen bij de AP; k. Of de verstrekking een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten; l. Of de betrokkene verplicht is de gegevens te verstrekken en wat de mogelijke gevolgen zijn als deze de gegevens niet verstrekt; m. Of geautomatiseerde besluitvorming en/of profilering bestaat en in die gevallen nuttige informatie over de onderliggende logica alsmede het belang en de verwachte gevolgen voor de betrokkene; n. Informatie over het andere doel, wanneer een verwerking gaat plaatsvinden voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld.
/02.03	Wanneer persoonsgegevens bij een ander dan de betrokkene worden verzameld, ontvangt de betrokkene de volgende informatie[181]: a. De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en in voorkomend geval van de vertegenwoordiger van de verwerkingsverantwoordelijke; b. In voorkomend geval de contactgegevens van de Functionaris voor gegevensbescherming; c. De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking; d. De betrokken categorieën persoonsgegevens; e. In voorkomend geval de ontvangers of categorieën van ontvangers van de persoonsgegevens; f. Als persoonsgegevens aan een ontvanger in een derde land of aan een internationale organisatie wordt doorgegeven, wordt informatie gegeven over hoe een kopie kan worden verkregen over de waarborgen of voorschriften of waar ze kunnen worden geraadpleegd; g. De periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is de criteria om die termijn te bepalen; h. Indien van toepassing de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde; i. Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage, en rectificatie of wissing van persoonsgegevens of om beperking van

[181] AVG Art. 7.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
	de hem betreffende verwerking, alsmede het recht tegen verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid; j. Wanneer verwerking is gebaseerd is op toestemming van betrokkene, heeft de betrokkene het recht de toestemming te allen tijde in te trekken. Dit doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming van vóór de intrekking; k. Dat de betrokkene het recht heeft een klacht in te dienen bij een AP; l. De bron waar de persoonsgegevens vandaan komen en in voorkomend geval of zij afkomstig zijn van openbare bronnen; m. Het bestaan van geautomatiseerde besluitvorming (inclusief profilering) inclusief de informatie over de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
/03 Uitzondering	
/03.01	De verplichting tot het verstrekken van informatie geldt niet, indien[182]: a. De betrokkene reeds over de informatie beschikt; b. Het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen; c. De verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te worden of ernstig in het gedrang dreigt te brengen; in dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie; d. Het verkrijgen of verstrekken van de gegevens uitdrukkelijk wettelijk is voorgeschreven en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen, of: e. De persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim, waaronder een statutaire geheimhoudingsplicht; f. Wanneer de verwerking berust op een wettelijke bepaling, waarbij een specifieke uitzondering geldt; g. Het de verwerking betreft van persoonsgegevens die deel uitmaken van archiefbescheiden en die op grond van de Archiefwet niet voor vernietiging in aanmerking komen en zijn overgebracht naar een archiefbewaarplaats. [183]
/04 Toestemming	
/04.01	De toestemming moet door de betrokkene vrijelijk gegeven kunnen worden. Bij de beoordeling of dit vrijelijk gebeurt, is gekeken of de verwerking noodzakelijk is voor de uitvoering van een met de betrokkene overeengekomen overeenkomst. [184]

[182] Artikel 14 lid 5 AVG.
[183] UAVG MvT toelichting bij Art. 41.
[184] AVG Art. 14 lid 4.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
/04.02	Bij aanbieden van een dienst aan een kind en het kind is jonger dan 16 jaar, dan is de toestemming of machtiging tot toestemming verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. [185]

Toelichting /01 Tijdig

/01.01 De betrokkene hoeft zijn persoonsgegevens pas te verstrekken als hij de informatie van de verantwoordelijke heeft ontvangen.

/01.01 Ook bij het verder verwerken voor een ander doel dan waarvoor de gegevens in eerste instantie zijn verzameld, moet de betrokkene nu actief door de verwerkingsverantwoordelijke geïnformeerd worden. [186]

/01.02 Bij informatieverkrijging van persoonsgegevens van een ander dan de betrokkene, kan gedacht worden aan de koppeling van gegevens, keteninformatisering en netwerkinformatisering:

- *Keteninformatisering* is gegevensuitwisseling tussen twee organisatie in een keten (dienstenketen).
- *Netwerkinformatisering* is gegevensuitwisseling of de gezamenlijke beheersing van gegevens zonder dat een vaste opvolging (keten) van actoren is.

/01.02 Doorgifte van persoonsgegevens tussen partijen in landen binnen de EU (daarmee ook binnen Nederland) valt onder het algemene begrip van verwerken. De 'doorgever' van de gegevens (de verstrekker) blijft verantwoordelijk voor een goed gebruik van de persoonsgegevens door anderen. Voor doorgifte naar personen/organisaties in landen buiten de EU gelden andere/aanvullende eisen; zie voor nadere informatie over doorgifte van persoonsgegevens U.07.

/01.02 In de AVG is een plicht opgenomen voor de verstrekker (dus niet alleen voor de ontvanger) om actief de betrokkene te informeren over de doorgifte van zijn/haar persoonsgegevens vóórdat de doorgifte plaats vindt. [187]

Toelichting /02 Informatie

/02.01 De informatie moet goed toegankelijk, leesbaar en begrijpelijk zijn voor 'de gewone burger'.

/02.01 De informatie moet zodanig worden verstrekt dat de betrokkene daarover daadwerkelijk beschikt. Dit kan op vele manieren; zowel mondeling, schriftelijk, digitaal, etc. Het is aan de verantwoordelijke om te kunnen aantonen dat de informatie daadwerkelijk aan de betrokkene is verstrekt, daarom heeft schriftelijke verstrekking de voorkeur.

Toelichting /03 Uitzonderingen

/03.01 De verantwoordelijke moet kunnen aantonen dat de betrokkene reeds op de hoogte is, wil hij zich kunnen beroepen op deze uitzonderingsgrond.

[185] AVG Art. 8.
[186] AVG Art. 14 lid 4.
[187] AVG Art. 14 lid 1e.

/03.01 Als de betrokkene over de informatie beschikt, bijv. doordat deze aan hem is overhandigd of toegezonden, dan is hij daarmee op de hoogte, ongeacht of hij het initiatief neemt de informatie tot zich te nemen. [188]

/03.01 De volgende specifieke uitzonderingsgronden worden gesteld[189]:

1. De nationale veiligheid;
2. De landsverdediging;
3. De openbare veiligheid;
4. De voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
5. Andere belangrijke doelstellingen van algemeen belang van de EU of van een lidstaat, met name een belangrijk economisch of financieel belang van de EU of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
6. De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
7. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
8. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten (a) tot en met (e) en punt (g) bedoelde gevallen;
9. De bescherming van de betrokkene of van de rechten en vrijheden van anderen;
10. De inning van civielrechtelijke vorderingen.

/03.01 Bij de toepassing van de uitzonderingsgronden houdt de verwerkingsverantwoordelijke rekening met in ieder geval, voor zover van toepassing[190]:

1. De doeleinden van de verwerking of van de categorieën van verwerking;
2. De categorieën persoonsgegevens;
3. Het toepassingsgebied van de ingevoerde beperkingen;
4. De waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
5. De specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
6. De opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
7. De risico's voor de rechten en vrijheden van de betrokkenen; en
8. Het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

[188] MvT WBP, Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr.3, pag. 151, 152.
[189] AVG Art. 23 lid 1 en UAVG Art. 41 lid 1.
[190] AVG Art. 23 lid 2 en UAVG Art. 41 lid 2.

Toelichting /04 Toestemming

/04.02 De verwerkingsverantwoordelijke doet, met inachtneming van de beschikbare technologie, redelijke inspanningen om te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend. [191]

2.2.6 U.06 Bewaren van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld of niet langer dan de bewaartermijn die sectorspecifieke wetgeving stelt.

De bewaartermijn kan worden beëindigd door actieve verwijdering van de gegevens of door anonimisering van de persoonsgegevens. Bij anonimisering zijn de gegevens niet meer herleidbaar tot de betrokkenen. NB: de AVG is niet van toepassing op de persoonsgegevens van overleden personen.. [192]

U.06 Bewaren van persoonsgegevens				
Criterium	Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.			
Doelstelling	Het doel van 'Bewaren persoonsgegevens' is te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel.			
Risico	Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.			
Referentie	AVG	UAVG		
	Art. 5, lid 1e	Art. 43		
Maatregelen/indicatoren				
/01 Nodige maatregelen				
/01.01	Als de bewaartermijnen verlopen, zijn de gegevens verwijderd, vernietigd of geanonimiseerd.			
/01.02	De verantwoordelijke bepaalt na elke verwerking van persoonsgegevens of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.			
/02 Bewaartermijn				
/02.01	Van alle persoonsgegevens is de bewaartermijn vastgesteld en bekrachtigd.			
/02.02	De bewaartermijn is de maximale periode waarin de persoonsgegevens noodzakelijk worden bewaard om het doel van de verwerking te bereiken of niet langer dan de termijn die verankerd is in sectorspecifieke wetgeving[193].			
/02.03	Als in sectorspecifieke wetgeving een bewaartermijn is vastgelegd voor specifieke persoonsgegevens, dan geldt die bewaartermijn.			

[191] AVG Art. 8 lid 2.
[192] AVG overweging 27: "De lidstaten kunnen regels vaststellen betreffende de verwerking van de persoonsgegevens van overleden personen."
[193] AVG Art. 5 lid 1e.

U.06 Bewaren van persoonsgegevens	
/02.04	Wanneer persoonsgegevens voor langere perioden worden opgeslagen, dan worden ze louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden verwerkt[194] en zijn voor de rechten en vrijheden van de betrokkene ("opslagbeperking") passende waarborgen getroffen in overeenstemming met de AVG.[195]

Toelichting /01 Nodige maatregelen

/01.01 De verantwoordelijke moet zich na elke verwerking van persoonsgegevens afvragen of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.

/01.01 De wet formuleert als volgt: persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.[196] Met andere woorden: wanneer de betrokkene niet langer te identificeren is aan de hand van de gegevens, dan geldt voor deze gegevens geen maximale bewaartermijn op grond van de AVG.

/01.01 Er is controle op de verwijdering, vernietiging of anonimisering. Softwarematige verwijdering of anonimisering en vernietiging van gegevensdragende hardware wordt bij voorkeur door een gespecialiseerde organisatie gedaan.

/01.01 Indien de persoonsgegevens zijn vastgelegd op een 'read only' gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, maar waarvan gegevens wel kunnen worden gekopieerd, zoals een CD-ROM of DVD, dan zijn maatregelen getroffen zodat de gegevens op geen enkele wijze meer kunnen worden ingezien, gebruikt of anderszins worden verwerkt. Ook wordt de betrokkene op de hoogte gesteld van de onmogelijkheid van verwijdering of anonimisering. [197]

/01.02 Indien aan de persoonsgegevens gekoppelde gegevens van belang zijn om langer te worden bewaard, dan dienen de persoonsgegevens zodanig te worden geanonimiseerd dat het daarna niet meer mogelijk is deze geanonimiseerde gegevens weer herleidbaar te maken. [198]

Toelichting /02 Bewaartermijn

/02.01 Soms vereist het bereiken van een doel juist dat persoonsgegeven bewaard blijven, bijv. iemands emailadres moet bewaard blijven voor nazending van berichten.

/02.02 In sommige (sectorspecifieke) wetgeving is voor bepaalde persoonsgegevens een bewaartermijn aangegeven. Een voorbeeld hiervan is het bewaren van medische gegevens: in het Burgerlijk Wetboek is de termijn hiervoor vastgesteld op 15 jaar.[199] Denk ook aan specifieke bewaartermijnen voor gegevens over financiële transacties.

---

[194] AVG Art. 5 lid 1e.
[195] AVG Art. 89 lid 1.
[196] Artikel 5 lid 1 onder e AVG.
[197] *Handleiding voor verwerkers van persoonsgegevens* - Handleiding van de WBP, Min. van Justitie, 2002, pag. 37.
[198] *Handleiding voor verwerkers van persoonsgegevens* - Handleiding van de WBP, Min. van Justitie, 2002, pag. 126.
[199] BW Art. 7:454 lid 3.

/02.04 De waarborgen bestaan uit technische en organisatorische maatregelen die zijn getroffen om het beginsel van minimale gegevensverwerking te garanderen. Zij hebben ten minste tot gevolg dat de gegevens niet langer herleidbaar zijn tot de betrokkenen.

/02.04 De maatregelen kunnen pseudonimisering omvatten, zodat de oorspronkelijke doelstellingen in het kader van het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden alsnog kunnen worden behaald.

2.2.7 U.07 Doorgifte persoonsgegevens

Doorgifte kan plaatsvinden aan verwerker(s) en aan andere verwerkingsverantwoordelijke(n). Een verwerker verricht de verwerking namens een verwerkingsverantwoordelijke.[200] NB: indien een verwerker in strijd met de AVG handelt, wordt die verwerker als verwerkingsverantwoordelijke beschouwd.[201] Waar sprake is van meerdere verwerkingsverantwoordelijken, bepalen zij gezamenlijk de doelstellingen en middelen voor de verwerking en zijn zij gezamenlijke verwerkingsverantwoordelijken.[202] Bij de doorgifte wordt onderscheid gemaakt tussen doorgifte binnen de EU, waar de AVG geldt, en doorgifte naar buiten de EU. Als doorgifte naar buiten de EU plaatsvindt, dan spreekt de AVG van doorgifte aan derde landen en internationale organisaties.

U.07 Doorgifte persoonsgegevens				
Criterium	Bij doorgifte aan een andere verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er afdoende garanties. Bij de doorgifte naar buiten de EU: • Is er een vertegenwoordiger, en: • Is geen sprake van uitzonderingsgronden, en: • Geldt een door de Europese Commissie genomen adequaatheidsbesluit, of: • Zijn er passende waarborgen[203], of: • Geldt een afwijking voor een specifieke situatie.			
Doelstelling	Het doel van de vereisten bij 'Doorgifte persoonsgegevens' is te waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid ingeregeld blijft.			
Risico	Als een organisatie niet voldoet aan dit criterium is het niet duidelijk voor de organisatie wat exact wordt verwacht bij het doorgeven van persoonsgegevens waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig verder worden verwerkt en gebrek is aan het nemen van verantwoordelijkheid en controle.			
Referentie	AVG	UAVG		

[200] AVG Art. 28 lid 1.
[201] AVG Art. 28 lid 10.
[202] AVG Art. 27 lid 1.
[203] AVG Art. 44.

U.07 Doorgifte persoonsgegevens				
	Art. 26, 27, 28, 29, 44, 45, 46, 47, 48, 49 en 96			
Indicatoren en Maatregelen				
/01 De onderlinge verantwoordelijkheden				
/01.01	Bij doorgifte aan een andere verantwoordelijke zijn: a. De respectieve verantwoordelijkheden duidelijk, zodat door alle partijen aan de AVG-verplichtingen voldaan kan worden, met name met betrekking tot[204]: • De uitoefening van de rechten van de betrokkene (conform C.02), en: • Het informeren van de betrokkenen bij ontvangst van de persoonsgegevens (conform U.05) b. De regeling met de respectieve verantwoordelijkheden aan de betrokkene beschikbaar gesteld. [205]			
/02 Afdoende garanties				
/02.01	De verwerking door een verwerker is in een overeenkomst of andere rechtshandeling vastgelegd, met daarin[206] : a. Het onderwerp en de duur van de verwerking. b. De aard en het doel van de verwerking waarvoor de persoonsgegevens worden verstrekt, inclusief: • Welke persoonsgegevens worden verstrekt aan de verwerker • Hoe dataminimalisatie is toegepast c. Het soort persoonsgegevens, inclusief de classificatie van de persoonsgegevens d. De categorieën van betrokkenen, en: e. De rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.			
/02.02	In de overeenkomst of andere rechtshandeling met de verwerker is bepaald dat[207]: a. De persoonsgegevens uitsluitend verwerkt worden op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften; b. De gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden; c. De beveiliging van de verwerking is geborgd, conform U.04, inclusief: • Welke medewerkers van de verwerker toegang tot de persoonsgegevens nodig hebben.			

[204] AVG Art. 26 lid 1.
[205] AVG Art. 26 lid 3.
[206] AVG Art. 28 lid 23
[207] Artikel 28 lid 3 AVG.

U.07 Doorgifte persoonsgegevens	
	• Welke procedure wordt gevolgd in geval van een datalek. • In welke landen de persoonsgegevens worden opgeslagen. d. De vereisten aan de verwerkers gelden ook als vereisten voor het in dienst nemen van een andere verwerker. e. Passende technische en organisatorische maatregelen zijn genomen als betrokkene zijn rechten doet gelden, inclusief: • Hoe de betrokkene wordt geïnformeerd over het uitbesteden van de persoonsgegevens aan de verwerker; • Het contact dat de verwerker mag hebben met de betrokkenen. f. De verwerkingsverantwoordelijke bijstand wordt verleend om te voldoen aan zijn verplichtingen ten aanzien van het borgen de van beveiliging van de verwerking. g. Na afloop van de verwerkingsdiensten, naar gelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens worden wist of deze aan hem terugbezorgd worden en bestaande kopieën worden verwijderd, conform U.06. h. De verwerker alle informatie aan de verwerkingsverantwoordelijke ter beschikking stelt en bijdraagt ten behoeve van audits en om aan te kunnen tonen dat hij aan zijn verplichtingen voldoet, waaronder inspecties. i. De verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis stelt als naar zijn mening een instructie inbreuk oplevert op de AVG of op andere wet- en regelgeving inzake gegevensbescherming.
/02.03	De overeenkomst of de rechtshandeling is in schriftelijke vorm, waaronder elektronische vorm, opgesteld.[208]
/03 Vertegenwoordiger	
/03.01	Als een verwerkingsverantwoordelijke of verwerker niet in de EU is gevestigd, dan is door de verwerkingsverantwoordelijke of de verwerker schriftelijk een vertegenwoordiger in de EU aangewezen[209], tenzij[210]: 1. Sprake is van een incidentele verwerking die geen grootschalige verwerking van bijzondere categorieën persoonsgegevens betreft, of: 2. Bij de verwerking van persoonsgegevens die verband houden met strafrechtelijke veroordelingen en strafbare feiten en waarbij de kans gering is dat zij een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. 3. Het een verwerking door een overheidsinstantie of overheidsorgaan betreft.
/03.02	De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over het toepassen van

[208] Artikel 28 lid 9 AVG.
[209] Artikel 27 lid 1 AVG.
[210] Artikel 27 lid 2 AVG.

U.07 Doorgifte persoonsgegevens	
	passende technische en organisatorische maatregelen bieden[211], zie B.03, door de verwerker.
/03.03	Een verwerker laat een verwerking pas door een andere verwerker uitvoeren als voorafgaand een specifieke of algemene schriftelijke toestemming is van de verwerkingsverantwoordelijke. [212]
/04 Uitzonderingsgronden	
/04.01	De verwerking vindt niet plaats als er een rechterlijke uitspraak of een besluit van een administratieve autoriteit is van een derde land op grond waarvan een verwerkingsverantwoordelijke of een verwerker persoonsgegevens moet doorgeven of verstrekken en waarbij dit niet erkend of afdwingbaar is gemaakt dat dit is gebaseerd op een internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand tussen het verzoekende derde landen en de EU of een lidstaat. [213]
/04.02	De doorgifte kan worden beperkt als in de wet- en regelgeving of bepalingen om gewichtige redenen van openbaar belang uitdrukkelijk grenzen worden gesteld aan de doorgifte van specifieke categorieën persoonsgegevens aan een derde land of een internationale organisatie.[214]
/05 Adequaatheidsbesluit	
/05.01	Doorgifte naar buiten de EU is alleen toegestaan, wanneer naar het oordeel van de Europese Commissie in het derde land, in het gebied of in één of meerdere nader bepaalde sectoren in het derde land, of bij de internationale organisatie in kwestie een passend beschermingsniveau is gewaarborgd. [215]
/06 Passende waarborgen	
/06.01	Wanneer door de Europese commissie geen *adequaatheidsbesluit* is genomen, dan zijn passende waarborgen geboden doordat er[216]: a. Een juridisch bindend en afdwingbaar instrument is tussen overheidsinstanties of -organen; b. Door de AP goedgekeurde bindende bedrijfsvoorschriften zijn; c. standaardbepalingen zijn inzake gegevensbescherming die in de door de Europese Commissie bedoelde onderzoeksprocedure zijn vastgesteld[217];

[211] Artikel 28 lid 1 AVG.
[212] AVG Art. 28 lid 1.
[213] AVG Art. 48.
[214] Artikel 49 lid 5 AVG.
[215] AVG Art. 45.
[216] AVG Art. 46.
[217] AVG Art. 93, lid 2.

U.07 Doorgifte persoonsgegevens	
	d. Standaardbepalingen zijn inzake gegevensbescherming die door een AP zijn vastgesteld en die in de door de Europese Commissie bedoelde onderzoeksprocedure zijn goedgekeurd[218]; e. Een goedgekeurde gedragscode is, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen toe te passen, waaronder waarborgen voor de rechten van de betrokkenen; f. Een goedgekeurd certificeringmechanisme is, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of de verwerker in het derde land om de passende waarborgen, onder meer voor de rechten van de betrokkenen, toe te passen, of: g. Door de AP passende waarborgen zijn, waarbij er met name: • Contractbepalingen zijn tussen de verwerkingsverantwoordelijke of de verwerker en de verwerkingsverantwoordelijke, de verwerker of de ontvanger van de persoonsgegevens in het derde land of de internationale organisatie, of: • Bepalingen zijn opgenomen in administratieve regelingen tussen overheidsinstanties of -organen, waaronder afdwingbare en effectieve rechten van betrokkenen.
/06.02	Als bindende bedrijfsvoorschriften worden gebruikt om passende waarborgen te bieden, dan[219]: a. Zijn die juridisch bindend of van toepassing en worden deze gehandhaafd door alle betrokken leden van het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen; met inbegrip van hun werknemers; b. Kunnen betrokkenen uitdrukkelijk afdwingbare rechten toekennen met betrekking tot de verwerking van hun persoonsgegevens, en: c. Zijn de hier beknopt weergegeven elementen vastgelegd (zie voor de volledige weergave AVG Art. 47 lid 2): • De structuur en de contactgegevens; • De gegevensdoorgiften of reeks van doorgiften; • Het intern en extern juridisch bindende karakter; • De toepassing van de algemene beginselen inzake gegevensbescherming; • De rechten van betrokkenen; • De aanvaarding van aansprakelijkheid voor alle inbreuken;

[218] AVG Art. 93, lid 2.
[219] Artikel 47 lid 1 AVG.

U.07 Doorgifte persoonsgegevens	

	• De wijze waarop informatie wordt verschaft over de bindende bedrijfsvoorschriften;
	• De taken van elke Functionaris voor gegevensbescherming, of elke andere persoon of entiteit die is belast met het toezicht op:
	  • De naleving van de bindende bedrijfsvoorschriften binnen het concern of de groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen,
	  • Opleiding, en:
	  • De behandeling van klachten;
	d. De klachtenprocedures;
	e. De bestaande procedures om te controleren of de bindende bedrijfsvoorschriften zijn nageleefd;
	f. De procedures om die veranderingen in de regels te melden, te registreren en aan de AP te melden;
	g. De procedure voor samenwerking met de AP;
	h. De procedures om eventuele wettelijke voorschriften aan de AP te melden, en:
	i. De passende opleiding inzake gegevensbescherming voor personeel.

/06.03	Wanneer de verwerking niet had mogen plaatsvinden, dan wordt door de verwerkingsverantwoordelijke de doorgifte beëindigd en de AP en de betrokkenen hierover geïnformeerd. [220]
/07 Afwijking voor een specifieke situatie	
/07.01	De doorgifte mag ook plaatsvinden als[221]: a. De betrokkene uitdrukkelijk heeft ingestemd met de voorgestelde doorgifte, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen, tenzij dit door een overheidsinstantie ten behoeve van een openbare bevoegdheid wordt verricht; b. De doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen, tenzij dit door een overheidsinstanties ten behoeve van een openbare bevoegdheid wordt verricht; c. De doorgifte noodzakelijk is voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst, tenzij dit door een overheidsinstanties ten behoeve van een openbare bevoegdheid wordt verricht;

[220] AVG Art. 49.
[221] AVG Art. 49.

U.07 Doorgifte persoonsgegevens	
	d. De doorgifte noodzakelijk is wegens gewichtige redenen van algemeen belang, dat is erkend bij de wet- en regelgeving; e. De doorgifte noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering; f. De doorgifte noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of van andere personen, als de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; g. De doorgifte verricht is vanuit een register dat volgens het Wettelijk recht is bedoeld om het publiek voor te lichten en dat door eenieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen kan worden geraadpleegd, maar alleen voor zover in het geval in kwestie wordt voldaan aan de in het wettelijk recht vastgestelde voorwaarden voor raadpleging; h. De doorgifte aan derde landen of internationale organisaties is gebaseerd op internationale overeenkomsten die door de lidstaten zijn gesloten vóór 24 mei 2016 en die overeenkomsten in overeenstemming zijn met het vóór die datum toepasselijke Unierecht en nog niet is gewijzigd, vervangen of ingetrokken[222].

Toelichting /01 De onderlinge verantwoordelijkheden

/01.01 De verantwoordelijkheden van de verwerkingsverantwoordelijken kunnen ook in de wet- en regelgeving zijn vastgelegd.

/01.01 Voor het uitoefenen van de rechten door betrokkenen kan een contactpunt worden aangewezen. Ook kan de betrokkene zijn rechten uit hoofde van de AVG tot en jegens iedere verwerkingsverantwoordelijke uitoefenen[223].

/01.01 Voorbeelden van regelingen zijn te vinden op: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#welke-modelcontracten-zijn-er-voor-doorgifte-naar-een-derde-land-5524.

Toelichting /02 Afdoende garanties

/02 Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringmechanisme kan worden gebruikt als element om aan te tonen dat voldoende garanties worden geboden.

/02 Deze vereisten in de overeenkomst gelden ook voor door de verwerker ingehuurde verwerkers.

/02.03 Deze vereiste geldt ook voor door de verwerker ingehuurde verwerkers.

Toelichting /03 Vertegenwoordiger

/03.01 Bij het bepalen van de kans wordt rekening houdend met de aard, de context, de omvang en de verwerkingsdoeleinden.

[222] AVG Art. 96.
[223] AVG Art. 26 lid 3.

/03.01 De vertegenwoordiger is gevestigd in een van de lidstaten waar zich de betrokkenen bevinden wier persoonsgegevens in verband met het hun aanbieden van goederen of diensten worden verwerkt of wier gedrag wordt geobserveerd.

/03.01 De vertegenwoordiger is door de verwerkingsverantwoordelijke of de verwerker gemachtigd om naast hem of in zijn plaats te worden benaderd.

/03.01 Het aanwijzen van een vertegenwoordiger doet niet af aan de mogelijkheid om tegen de verwerkingsverantwoordelijke of de verwerker zelf vorderingen in te stellen.

/03.03 In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

Toelichting /04 Uitzonderingsgrond

/04.01 Met het begrip 'doorgifte naar landen buiten de EU' wordt gedoeld op het ter kennis brengen van de gegevens aan een persoon of organisatie die zich bevindt buiten de rechtsmacht van een van de landen van de Unie. Het gaat daarbij om:

1. Het gebruik van gegevens binnen concernverband, indien onderdelen van een concern zich binnen en buiten de EU bevinden; bindende bedrijfsvoorschriften zijn dan van toepassing.
2. De verstrekking aan derden die zich buiten de EU bevinden;
3. Het ter beschikking stellen van de gegevens aan derden buiten de EU;
4. Het verzamelen van gegevens door landen buiten de EU.

Toelichting /05 Adequaatheidsbesluit

/05.01 Voor een dergelijke doorgifte is geen specifieke toestemming nodig.

/05.01 Canada: de Europese Commissie heeft voor commerciële bedrijven in Canada een adequaatheidsbesluit genomen.

/05.01 Verenigde Staten: Op 10 juli 2023 zijn nieuwe afspraken in werking getreden tussen de Europese Commissie (EC) en de VS over de doorgifte van persoonsgegevens vanuit de EER naar de VS. Die afspraken staan bekend onder de naam Data Privacy Framework. De EC heeft een adequaatheidsbesluit genomen over de VS. Dit adequaatheidsbesluit is onderdeel van het Data Privacy Framework. Organisaties in de VS kunnen meedoen aan het Data Privacy Framework. Je moet eerst controleren of de organisatie in de VS waarnaar je persoonsgegevens wilt doorgeven, meedoet aan het Data Privacy Framework. Je controleert dit op de website van het Data Privacy Framework.

Doet de organisatie in de VS waarnaar je persoonsgegevens wilt doorgeven niet mee het Data Privacy Framework? Dan mag je de persoonsgegevens alleen doorgeven als je aan deze twee voorwaarden voldoet:

1. Je gebruikt een doorgifte-instrument voor doorgifte naar een land buiten de EER. Zoals een modelcontract of binding corporate rules (BCR).
2. Je neemt extra maatregelen om de persoonsgegevens te beschermen.

/05.01 Tot de Europese Economische Ruimte behoren de landen van de EU, Noorwegen, Liechtenstein en IJsland. Aan deze landen mogen persoonsgegevens dus worden doorgegeven.

Toelichting /06 Passende waarborgen

/06.01 Wanneer de waarborgen kunnen worden geboden, is voor de verwerking geen specifieke toestemming van een AP vereist.

2.3 Het Control- of Beheerdomein

Inleiding

In dit hoofdstuk zijn richtlijnen opgenomen voor de specifieke beheeraspecten van de gegevensverwerking; dit houdt onder meer in dat adequate technische- en organisatorische maatregelen moeten zijn ingericht, om de beheerprocessen vorm te geven.

Doelstelling

De doelstelling van Intern toezicht is te zorgen voor en/of vast te stellen dat maatregelen ter waarborging van de privacy afdoende zijn ingericht (control, beheersing).

Risico's

Door het ontbreken van noodzakelijke maatregelen binnen het beheersingsdomein is het niet zeker dat de verwerking aan de vereisten voldoet en dat de governance van die omgeving toereikend is ingericht.

2.3.1 C.01 Intern toezicht

Binnen de organisatie wordt toezicht gehouden op de rechtmatigheid van de gegevensverwerking. Een gegevensverwerking is rechtmatig als deze voldoet aan de eisen die de AVG, sectorspecifieke wetgeving en/of een (eventuele) Gedragscode stelt.

C.01 Intern toezicht				
Criterium	Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.			
Doelstelling	Het doel van 'Intern toezicht' is het garanderen van een rechtmatige, behoorlijke en transparantie verwerking van persoonsgegevens, het garanderen van naleving van de AVG en van andere wet- en regelgeving betreffende de gegevensbescherming, en het garanderen en aantoonbaar maken van naleving van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens.			
Risico	Als de verwerking van persoonsgegevens niet voldoet aan de AVG, dan zijn de risico's tweeledig: de betrokkene loopt persoonlijke privacyrisico's en de verwerkingsverantwoordelijke wordt geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago als gevolg van communicatieve of handhavende maatregelen van betrokkenen, derden en/of de toezichthoudende autoriteiten.			
Referentie	AVG	UAVG		
	Art. 5.			
Indicatoren en maatregelen				
/01 Evaluatie				
/01.01	De verantwoordelijke en - indien aangesteld - de Functionaris voor gegevensbescherming controleert of de gegevensverwerkingen voldoen aan de wettelijke verplichtingen. Hiertoe worden periodiek compliancy assessments uitgevoerd en de resultaten geregistreerd.			

C.01 Intern toezicht	
/01.02	Als blijkt dat niet voldaan wordt aan de eisen van de AVG, dan rapporteert de verantwoordelijke over de te nemen maatregelen om de privacyschending te beëindigen. De evaluatierapportages worden beschikbaar gesteld aan het management.
/01.03	Er is een planning van activiteiten in het kader van het beoordelen van de compliancy.
/02 Rechtmatigheid aangetoond	
/02.01	Aangetoond is dat, conform U.01, de persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt (doelbinding).
/02.02	Aangetoond is dat, conform U.01, de verwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).
/02.03	Aangetoond is dat, conform U.01, de verwerking ten aanzien van de betrokkene rechtmatig is.
/02.04	Bij het aantonen van de rechtmatigheid wordt gebruik gemaakt van de overeenkomsten voor de doorgiften zoals beschreven in U.07.
/02.05	Aangetoond is dat, conform U.04, passende technische en organisatorische maatregelen op een dusdanige manier worden verwerkt, dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid).
/02.06	Aangetoond is dat, conform U.03, de persoonsgegevens juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (kwaliteitsmanagement).
/02.07	Aangetoond is dat, conform B.03, de wijze van verwerken ten aanzien van de betrokkene 'behoorlijk' is.
/02.08	Aangetoond is dat de persoonsgegevens op een wijze worden verwerkt die voor de betrokkene transparant is, conform U.05, U.02 en C.02
/02.09	De verwerkingsverantwoordelijke toont compliancy aan door middel van een dossier (al dan niet door een Functionaris voor gegevensbescherming bijgehouden). [224]
/02.10	Bij het aantonen van het compliant en het compleet zijn van het dossier wordt gebruik gemaakt van het register (U.02: Register van verwerkingsactiviteiten).

Toelichting /01 Evaluatie

/01.01 Als de verantwoordelijke op de hoogte is van een schending van de privacy en hij laat na om de nodige maatregelen te treffen om deze schending te beëindigen, dan is hij hierop aanspreekbaar. Hij moet daarom tijdig de nodige maatregelen treffen. De 'nodige

[224] AVG Art. 5 lid 2.

maatregelen' bestaan uit corrigerende maatregelen die het mogelijk maken binnen een passende termijn de schending van de privacy te beëindigen.

/01.01 Als de FG onregelmatigheden heeft aangetroffen, dan meldt hij dit bij de verantwoordelijke of de organisatie waarvoor hij is aangesteld en geeft hij adviezen over de juiste uitvoering van de privacy verplichtingen.

Toelichting /02 Rechtmatigheid aangetoond

/02.09 De uitkomst van het compliancy proces kan ook worden gebruikt voor publicatie over de behaalde resultaten van het waarborgen van de privacy van de klanten.

2.3.2 C.02 Toegang gegevensverwerking voor betrokkenen

Iedere betrokkene heeft (binnen grenzen van redelijkheid) het recht te weten of, door wie, waarvoor en op welke wijze zijn persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke moet deze transparantie kunnen bieden. Deze transparantie is nodig om de betrokkene of diens wettelijke vertegenwoordiger in staat te stellen - indien nodig - zonder onevenredige kosten en/of moeite zijn gegevens te laten corrigeren of de verantwoordelijke (in rechte) aan te spreken bij onrechtmatigheid van een gegevensverwerking opdat deze onrechtmatigheid beëindigd wordt.

Voorafgaand aan de verwerking van de persoonsgegevens worden betrokkenen geïnformeerd over de verwerking conform U.05: Bewaren van persoonsgegevens, en zijn binnen de verwerkingen voorzieningen getroffen waarmee de betrokkene controle over zijn gegevens kan houden, conform U.03: Kwaliteitsmanagement.

C.02 Toegang gegevensverwerking voor betrokkene				
Criterium	De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen , tenzij er een specifieke uitzonderingsgrond geldt.			
Doelstelling	Het doel van 'Toegang gegevensverwerking voor betrokkene' is om zo nodig transparantie te bieden over de gegevensverwerking, zodat de betrokkene zijn rechten kan uitoefenen en zo de verantwoordelijke kan aanspreken bij onrechtmatigheid van een gegevensverwerking, opdat deze onrechtmatigheid beëindigd wordt.			
Risico	De organisatie is niet transparant, waardoor het inzicht in de rechtmatigheid van organisaties ontbreekt, waardoor het vertrouwen in een organisatie verloren gaat.			
Referentie	AVG	UAVG		
	Art. 11, 12, 15, 86			
Indicatoren en maatregelen				
/01 Informatie over de verwerking van persoonsgegevens				
/01.01	De betrokkene krijgt op verzoek uitsluitsel over het al dan niet verwerken van hem betreffende persoonsgegevens.[225]			

[225] Artikel 15 lid 1 AVG.

C.02 Toegang gegevensverwerking voor betrokkene	
/01.02	De inzage over de verwerkte persoonsgegevens bevat de volgende informatie[226]: a. De verwerkingsdoeleinden; b. De betrokken categorieën persoonsgegevens; c. De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties; d. Indien mogelijk: de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen of, als dat niet mogelijk is, de criteria om die termijn te bepalen; e. Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat zijn persoonsgegevens te rectificeren of te wissen of de verwerking van de hem betreffende persoonsgegevens te beperken, alsmede het recht tegen die verwerking bezwaar te maken; f. Dat de betrokkene het recht heeft klacht in te dienen bij de AP; g. Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens; h. Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, inclusief nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene; i. Bij doorgifte aan een derde land of een internationale organisatie en op verzoek van betrokkene de informatie over van de passende waarborgen; j. Op verzoek van betrokkene een kopie van de persoonsgegevens die worden verwerkt.
/01.03	De inzage doet geen afbreuk aan de rechten en vrijheden van anderen[227].
/02 Tijdig	
/02.01	De informatie is onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek verstrekt[228], tenzij[229]: • De complexiteit van de verzoeken en van het aantal verzoeken verlenging nodig maakt, en: • De informatie binnen een termijn van nog eens twee maanden worden verstrekt, en: • De betrokkene binnen één maand na ontvangst van het verzoek in kennis wordt gesteld van een dergelijke verlenging.

[226] AVG Art. 15.
[227] AVG Art. 14 lid 4.
[228] AVG Art. 12 lid 3 en 4.
[229] Artikel 12 lid 3 AVG.

C.02 Toegang gegevensverwerking voor betrokkene	
/02.02	Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, dan[230]: • Is dit de betrokkene onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek meegedeeld waarom het verzoek zonder gevolg is gebleven, en: • Is de betrokkene geïnformeerd over de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.
/03 Passende vorm	
/03.01	De communicatie vindt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is, plaats in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Hierbij kan gebruik gemaakt worden van gestandaardiseerde iconen om het overzicht te houden.[231]
/03.02	De informatie is schriftelijk of met andere middelen en als dit passend is met inbegrip van elektronische middelen verstrekt.[232]
/03.03	Op verzoek van de betrokkene is de informatie mondeling meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.[233]
/03.04	Het verstrekken van de informatie en de communicatie zijn kosteloos, tenzij de verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn. Als de verzoeken buitensporig zijn, met name vanwege hun repetitieve karakter, en dit kan worden aangetoond, dan mag de verwerkingsverantwoordelijke ofwel: • Een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan ofwel: • Weigeren gevolg te geven aan het verzoek.[234]
/03.05	De verantwoordelijke beschikt over gegevens ter identificatie van de betrokkene om hem zijn rechten te laten doen gelden. Deze gegevens worden niet behouden, verkregen of verwerkt als er geen doeleinden zijn (overeenkomstig U.01) om nog persoonsgegevens van betrokkene te verwerken.[235] Als identificatie niet mogelijk is wordt de betrokkene daarvan indien mogelijk in kennis gesteld.
/04 Specifieke uitzonderingsgrond	
/04.01	De verantwoordelijke verstrekt geen informatie als de verwerking berust op een wettelijke bepaling, waarbij een specifieke uitzondering geldt.[236]

[230] Artikel 12 lid 4 AVG.
[231] Artikel 12 lid 1 en 7 AVG.
[232] Artikel 12 lid 1 AVG.
[233] Artikel 12 lid 1 AVG.
[234] Artikel 12 lid 5 AVG.
[235] AVG Art. 11.
[236] AVG Art. 23.

Toelichting: /01 Informatie over de verwerking van persoonsgegevens

/01.01 Er kan behoefte zijn aan informatie over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de persoonsgegevens als bijvoorbeeld bijzondere computerprogrammatuur een wijze van verwerking mogelijk maakt die de betrokkene op het eerste gezicht niet geheel duidelijk is. Deze mededeling hoeft niet zo ver te gaan dat het Auteursrecht en/of Intellectuele Eigendomsrecht dat de software beschermt of het bedrijfsgeheim geschonden wordt.

/01.03 Het publiek heeft toegang tot persoonsgegevens in officiële documenten die voor de uitvoering van een taak van algemeen belang in het bezit zijn van een overheidsinstantie, een overheidsorgaan of een particulier orgaan. Deze gegevens mogen door de instantie of het orgaan in kwestie worden bekendgemaakt in overeenstemming met het wettelijke recht dat op de overheidsinstantie of het orgaan van toepassing is teneinde het recht van toegang van het publiek tot officiële documenten in overeenstemming te brengen met het recht op bescherming van persoonsgegevens uit hoofde van de AVG.

Toelichting /02 Tijdig

/02.01 Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Toelichting /03 Passende vorm:

/03.02 Als de betrokkene om bijkomende kopieën verzoekt, dan kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient en niet om een andere regeling verzoekt, dan wordt de informatie in een gangbare elektronische vorm verstrekt.

Toelichting /04 Specifieke uitzonderingsgrond

/04.01 De volgende specifieke uitzonderingsgronden worden gesteld[237]:

1. De nationale veiligheid;
2. De landsverdediging;
3. De openbare veiligheid;
4. De voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
5. Andere belangrijke doelstellingen van algemeen belang van de EU of van een lidstaat, met name een belangrijk economisch of financieel belang van de EU of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
6. De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
7. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

[237] AVG Art. 23 lid 2 en UAVG Art. 41 lid 1.

8. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten (1) tot en met (5) en punt (7) bedoelde gevallen;
9. De bescherming van de betrokkene of van de rechten en vrijheden van anderen;
10. De inning van civielrechtelijke vorderingen.

/04.01 Bij de toepassing van de uitzonderingsgronden houdt de verwerkingsverantwoordelijke rekening met in ieder geval, voor zover van toepassing[238]:

1. De doeleinden van de verwerking of van de categorieën van verwerking;
2. De categorieën persoonsgegevens;
3. Het toepassingsgebied van de ingevoerde beperkingen;
4. De waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
5. De specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
6. De opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
7. De risico's voor de rechten en vrijheden van de betrokkenen; en
8. Het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

Indien een verwerking wordt verricht door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, kan de verwerkingsverantwoordelijke het recht op inzage buiten toepassing laten.

2.3.3 C.03 Meldplicht Datalekken

Het bieden van inzicht in een datalek en de mogelijke gevolgen ervan, kan mogelijk (negatieve) consequenties voor de betrokkenen beperken. Een datalek is een "inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. [239]

C.03 Meldplicht Datalekken	
Criterium	De verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de Autoriteit Persoonsgegevens, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.
Doelstelling	Het doel van 'Meldplicht datalekken' is negatieve consequenties van een datalek te beperken en waar mogelijk te voorkomen.

[238] AVG Art. 23 lid 2 en UAVG Art. 41 lid 2.

[239] AVG Art. 4. De Engelse tekst spreekt hier van "personal data breach". De meldplicht datalekken wordt behandeld in AVG Art. 33 en 34. Zie ook AVG overweging 85. In de UAVG is niets over de meldplicht opgenomen, anders dan het uitsluiten van financiële ondernemingen als bedoeld in de Wet op het financieel toezicht (UAVG Art. 42).

C.03 Meldplicht Datalekken				
Risico	Negatieve consequenties die de persoonlijke levenssfeer van de betrokkene treffen.			
Referentie	AVG	UAVG		
	Art. 33, Art. 34	Art. 41 en 42		
Indicatoren en maatregelen				
/01 Meldt een datalek				
/01.01	Een datalek is op basis van de AVG gemeld bij de AP, tenzij een uitzondering van toepassing is (zie /04.01)			
/01.02	De melding aan de AP bevat ten minste[240]: a. De aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie; b. De naam en de contactgegevens van de Functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen; c. De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens; d. De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.			
/01.03	Een datalek is gemeld aan betrokkenen, tenzij een uitzondering van toepassing is (zie /04.02).			
/01.04	In de melding aan de betrokkene wordt van de aard van de inbreuk in verband met persoonsgegevens ten minste het volgende omschreven of meegedeeld[241]: a. De naam en de contactgegevens van de Functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen; b. De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens; c. De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.			
/01.05	De melding aan de betrokkene is in duidelijke en eenvoudige taal.			
/02 Termijn				

[240] AVG Art. 33 lid 3.
[241] AVG Art. 33, lid 3b, 3c en 3d.

C.03 Meldplicht Datalekken	
/02.01	Een verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging, zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.[242]
/02.02	De melding aan de AP heeft plaatsgevonden zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen.[243]
/02.03	Als de melding aan de AP niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.[244]
/02.04	De melding aan de betrokkene gebeurt onverwijld.[245]
/03 Documenteert de inbreuk	
/03.01	De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.[246]
/03.02	De documentatie stelt de toezichthoudende autoriteit (AP) in staat de naleving te controleren.[247]
/03.03	De documentatie bevat de noodzakelijke gegevens plus de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.[248]
/03.04	Het feit dat de kennisgeving is gedaan zonder onredelijke vertraging moet worden vastgesteld, met name rekening houdend met de aard en de ernst van de inbreuk in verband met persoonsgegevens en de gevolgen en negatieve effecten voor de betrokkene. [249]
/04 Uitzondering	
/04.01	De verantwoordelijke hoeft het datalek niet te melden ***aan de AP*** als: • Het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, of: • Wanneer melding afbreuk zou doen aan een zwaarwegend belang[250]; • De verantwoordelijke een aanbieder is van openbare elektronische communicatiediensten zoals bedoeld in de Telecommunicatiewet[251].

[242] Artikel 33 lid 1 AVG.
[243] Artikel 33 lid 1 AVG.
[244] Artikel 33 lid 1 AVG.
[245] Artikel 34 lid 1 AVG.
[246] Artikel 33 lid 5 AVG.
[247] Artikel 33 lid 5 AVG.
[248] Artikel 33 lid 3 AVG.
[249] Overweging 87 AVG.
[250] Artikel 41 UAVG.
[251] AVG Art. 95.

C.03 Meldplicht Datalekken	
/04.02	De verantwoordelijke hoeft het datalek niet te melden ***aan de betrokkene*** als: • Het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, en/of[252]: • De verwerkingsverantwoordelijke passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling, en/of: • De verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het bij het eerste streepje bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen, of: • De mededeling onevenredige inspanningen zou vergen; in dat geval komt in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd, of: • Het een verwerking is die berust op een andere wettelijke bepaling waarvoor een specifieke meldplicht geldt[253], of: • De organisatie een financiële onderneming is in de zin van de Wet op het financieel toezicht. [254] • De verwerking van persoonsgegevens door een natuurlijke persoon in het kader van een louter persoonlijke of huishoudelijke activiteit plaatsvindt, die als zodanig geen enkel verband houdt met een beroeps- of handelsactiviteit.[255]

Toelichting /01 Meldt een datalek

/01. Het gaat in de AVG om twee verschillende meldplichten: er is een meldplicht aan de AP, en een meldplicht aan de betrokkene, op wiens persoonsgegevens een inbreuk is gemaakt.

Toelichting /02 Termijn

/02 Als en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, dan kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Toelichting /03 Documenteert de inbreuk

/03.01 De documentatie bevat de noodzakelijke gegevens van alle datalekken, ook die welke niet gemeld zijn.

/03.02 Desgevraagd moet meer documentatie voorhanden zijn die direct in verband staat met de melding van een inbreuk zelf. Nagegaan moet kunnen worden of alle passende technische en organisatorische maatregelen zijn genomen om vast te stellen of een inbreuk in verband

[252] Artikel 34 lid 1 en 3 AVG.
[253] AVG Art. 23; UAVG Art. 42.
[254] UAVG Art. 42.
[255] AVG overweging 18.

met persoonsgegevens heeft plaatsgevonden, en om de AP en de betrokkene daarvan onverwijld in kennis te stellen [256].

/03.02 Ook bij een besluit om een inbreuk *niet* te melden, moet deze afweging en het besluit worden gedocumenteerd en door de AP gecontroleerd kunnen worden.

/03.03 De documentatie is actueel en accuraat en kan op verzoek onmiddellijk worden overlegd. De documentatie bevat zelf geen persoonsgegevens.

/03.03 Bij het documenteren wordt gebruik gemaakt van het Register van verwerkingsactiviteiten zoals bedoeld in U.02. Het advies is om de documentatie van datalekken binnen deze registratie bij te houden. Hiermee wordt dubbele opslag en dubbel beheer van informatie over de gegevensverwerkingen voorkomen.

Toelichting /04 Uitzondering

/04.02 Telecommunicatiewet: heeft eigen meldingsverplichting bij datalekken. [257]

/04.02 UAVG 42 luidt "Artikel 34 van de verordening is niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht". AVG Art. 34 betreft de meldplicht aan betrokkenen. Financiële ondernemingen moeten dus wél aan AP melden maar niet aan de betrokkenen. De financiële sector kent een eigen zorgplicht jegens betrokkenen.

/04.02 De volgende specifieke uitzonderingsgronden worden gesteld[258]:

a. De nationale veiligheid;
b. De landsverdediging;
c. De openbare veiligheid;
d. De voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e. Andere belangrijke doelstellingen van algemeen belang van de EU of van een lidstaat, met name een belangrijk economisch of financieel belang van de EU of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
f. De bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
g. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten (a) tot en met (e) en punt (g) bedoelde gevallen;
i. De bescherming van de betrokkene of van de rechten en vrijheden van anderen;
j. De inning van civielrechtelijke vorderingen.

/04.02 De wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste[259]:

---

[256] AVG overweging 87.
[257] Art. 11.3a Telecommunicatiewet.
[258] AVG Art. 23 lid 1.
[259] AVG Art. 23 lid 2.

a. De doeleinden van de verwerking of van de categorieën van verwerking;
b. De categorieën persoonsgegevens;
c. Het toepassingsgebied van de ingevoerde beperkingen;
d. De waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
e. De specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. De opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
g. De risico's voor de rechten en vrijheden van de betrokkenen, en:
h. Het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

/04.02 De AVG geldt ook voor verwerkingsverantwoordelijken en verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.

/04.02 Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten. [260]

[260] AVG overweging 18.

3 Aanvullende informatie

In dit gedeelte vind je nadere informatie over werken met persoonsgegevens, de ACT-doelen, risico's van nalatigheid, grip op privacy en privacy volwassenheid. Ook lichten we kort het format toe waarin de criteria van de Baseline worden beschreven.

3.1 Werken met persoonsgegevens

De AVG beschrijft de beginselen van de verwerking van persoonsgegevens.[261]Wij beperken ons hier tot de beschrijving van enkele kenmerkende begrippen.

3.1.1 Verwerking van persoonsgegevens

Verwerken is een breed begrip en omvat alles wat je kunt doen met persoonsgegevens van verzamelen tot vernietigen. De informatie tot je nemen is al een verwerking. In de definitie van de AVG: "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens" (AVG Art. 4 "Definities").

3.1.2 Zelf persoonsgegevens verwerken of uitbesteden

Als we persoonsgegevens verwerken om een bepaald doel te bereiken, dan moeten we vaststellen of we dat doen in de rol van verwerkingsverantwoordelijke of verwerker. Een verwerkingsverantwoordelijke bepaalt zelf het doel van en de middelen voor de betreffende verwerking(en) van persoonsgegevens; een verwerker verwerkt persoonsgegevens in opdracht van of ten behoeve van een verwerkingsverantwoordelijke. Deze rollen kunnen samenvallen; een organisatie kan ook ervoor kiezen (bepaalde) persoonsgegevens niet zelf te verwerken (inclusief de keuze om (bepaalde) persoonsgegevens niet zelf te verzamelen en op te slaan).

Bij het uitbesteden van een verwerking of bij het verwerken van persoonsgegevens van een andere partij moeten afspraken worden gemaakt tussen de verwerkingsverantwoordelijke en de verwerker (AVG Art. 28, lid 3 en verder). Deze afspraken kunnen worden vastgelegd in een overeenkomst, die we in deze Privacy Baseline de 'verwerkersovereenkomst' zullen noemen. Dit is een gangbare, maar geen officiële term uit de AVG.

De afspraken kunnen ook volgen uit een andere rechtshandeling krachtens Unierecht of lidstatelijke recht. Van belang is dat onder meer verantwoordelijkheden worden benoemd, bijvoorbeeld bij wie de regie berust en waar betrokkenen een aanspreekpunt kunnen vinden met betrekking tot de verwerking. In een verwerkersverhouding tussen twee overheidsinstanties ligt het eerder voor de hand om deze afspraken in nadere regelgeving te vast te leggen dan in een overeenkomst. Wanneer twee overheden privaatrechtelijk onder dezelfde rechtspersoon vallen, dan is het contractrechtelijk zelfs onmogelijk om afspraken middels een overeenkomst vast te leggen.

[261] AVG Art. 5 lid 11.

Er moet altijd een geldige grondslag zijn voor het verwerken van de persoonsgegevens: uiteraard geldt dit ook voor de verwerking ten behoeve van een ander doel. De ontvangende partij is zelf verantwoordelijk voor de technische en organisatorische maatregelen die voor de beveiliging van de gegevens nodig zijn.

Belangrijke aspecten aan de verwerking van persoonsgegevens waarmee de Bij gegevensuitwisseling tussen twee verwerkingsverantwoordelijken is het eveneens aan te bevelen een overeenkomst te sluiten waarin de betrokken partijen afspraken over de gegevensdeling vastleggen, bijvoorbeeld dat de deling van de gegevens rechtmatig is en veilig plaatsvindt. verwerkingsverantwoordelijke - en soms ook verwerker - in het kader van de AVG rekening moet houden zijn accountability/aantoonbaarheid en risicoanalyse.

3.1.3 Verwerkingsverantwoordelijke en verwerker

Een belangrijk onderscheid met het oog op rolverdelingen en verantwoordelijkheden. De definities van de AVG (AVG Art. 4, lid 7 en 8) luiden als volgt:

- Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het wettelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verantwoording ('accountability') is een plicht van de verwerkingsverantwoordelijke. AVG Art. 5.2 luidt: "De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 (i.e. Beginselen inzake verwerking van persoonsgegevens) *en kan deze aantonen* ('verantwoordingsplicht')".

3.1.4 Verwerkersovereenkomst

Hoewel de term 'verwerkersovereenkomst' in de Nederlandstalige AVG niet letterlijk wordt gebruikt, bepaalt AVG artikel 28 toch nauwkeurig dat er een "overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt" moet zijn, "waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven" (AVG Art. 28 lid 3 en verder). Bij de criteria B.02 Organieke inbedding, en: U.07 Doorgifte persoonsgegevens komt dit nader ter sprake.

Wij hanteren de term 'verwerkersovereenkomst' in deze zin. Voor de overeenkomst tussen twee verwerkingsverantwoordelijken (bij doorgifte/overdracht van persoonsgegevens, gebruiken we de term 'samenwerkingsovereenkomst', om het verschil aan te kunnen duiden tussen de overeenkomst tussen de verantwoordelijke en de verwerker en de overeenkomst tussen verantwoordelijke en verantwoordelijke.

Wanneer twee instanties tot dezelfde overheid behoren, zoals rijksoverheid, dezelfde provincie of dezelfde gemeente, dan kunnen zij, volgens het algemeen verbintenissenrecht, onderling geen juridische overeenkomst aangaan. Het vastleggen van een verwerkersverhouding in nadere regelgeving of een convenant ligt dan meer voor de hand. Overheidsinstanties die tot verschillende overheden behoren kunnen onderling wel verwerkersovereenkomsten contractueel vastleggen.

3.1.5 Persoonsgegevens en bijzondere categorieën persoonsgegevens

Onder persoonsgegevens verstaat de AVG alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

- *Direct identificeerbaar*: Gegevens die naar hun aard rechtstreeks betrekking hebben op een persoon, zoals iemands naam.
- *Indirect identificeerbaar*: Gegevens die naar hun aard geen betrekking hebben op een persoon worden als persoonsgegeven aangemerkt als deze mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Voorbeelden hiervan zijn het type huis of auto van een betrokkene, omdat dit iets zegt over het inkomen en vermogen van de betrokkene. Ook gegevens die in combinatie met andere gegevens tot identificeerbaarheid kunnen leiden worden aangemerkt als persoonsgegeven.

Merk op dat een definiëring van "Betrokkene" is af te leiden uit de definitie van "Persoonsgegevens". De betrokkene is degene op wie een persoonsgegeven betrekking heeft en daarmee geïdentificeerd kan worden. Daarover nog het volgende: de betrokkene is *géén eigenaar* van zijn/haar data; eigendom van data is in juridische zin niet mogelijk.

Bijzondere categorieën persoonsgegevens

De AVG spreekt van 'bijzondere categorieën persoonsgegevens' (AVG Art. 9). Dit zijn gegevens over:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gezondheid;
- Seksueel gedrag of seksuele gerichtheid.

Bijzondere persoonsgegevens zijn naar hun aard vertrouwelijker dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens. Het vertrekpunt is dat verwerking van deze categorieën van gegevens verboden is tenzij aan een aantal voorwaarden is

voldaan. Deze voorwaarden kennen significante verschillen ten opzichte van de voorwaarden voor de verwerking van persoonsgegevens in het algemeen (AVG Art. 9). Het criterium U.01 Doelbinding gegevensverwerking gaat hier uitgebreid op in.

In de overwegingen van de AVG komen we nog de term 'gevoelige gegevens' tegen. Deze aanduiding wordt gebruikt als kwalificatie van bijzondere persoonsgegevens en geeft feitelijk de aanleiding weer voor de bijzondere, strengere vereisten die voor de verwerking van deze gegevens gelden (AVG overweging 10, 51 en 91).

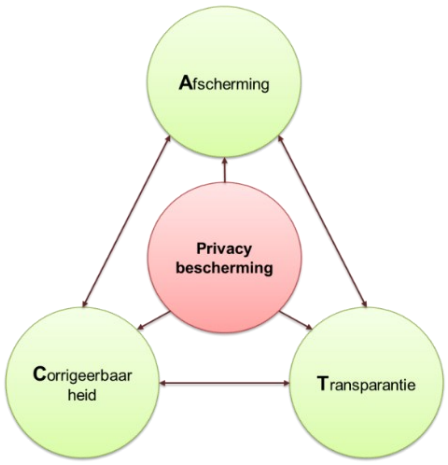
3.1.6 Strafrechtelijke gegevens en het BSN

Strafrechtelijke gegevens worden in de AVG niet als bijzondere persoonsgegevens aangemerkt. In AVG Art. 10 zijn specifieke bepalingen opgenomen ten aanzien van de verwerking van deze gegevens.

In de AVG wordt een nationaal identificatienummer niet aangemerkt als een bijzonder persoonsgegeven. In de UAVG worden aanvullende voorwaarden gesteld aan het gebruik van een dergelijk nummer, in Nederland het BSN (zie verder onder U.01 Doelbinding gegevensverwerking).

Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald (UAVG Art. 44).

3.2 De ACT-doelen van privacybescherming



Figuur 2: De ACT doelen van privacybescherming

Er zijn verschillende soorten privacy te onderscheiden. Het recht op bescherming van persoonsgegevens wordt informationele privacy genoemd. Het beschermen van de informationele privacy kan worden uitgedrukt in ACT-doelen: Afscherming, Corrigeerbaarheid en Transparantie.

In AVG Art. 5 wordt in dit verband geschreven over: *rechtmatig, behoorlijk en transparant*. Vergeleken bij ACT is dat meer te beschouwen als een "juridische doelstelling"; ACT is een "functionele doelstelling" - overigens ook handig als richtlijn bij Privacy by Design.

In de (functionele) kern zijn het naar onze mening geen verschillende uitgangspunten c.q. doelstellingen. Het gaat per saldo niet om compliancy aan de wet, maar om deugdelijke privacybescherming.

Deze beginselen worden geformuleerd en behandeld in AVG Art. 5.1, AVG overweging 39 en §4.2 van de MvT bij Uitvoeringswet AVG (versie april 2017). Met enige lenigheid is deze trits gemakkelijk te verzoenen met het ACT-trio.

De ACT-doelen zijn als volgt gedefinieerd:

- *Afscherming*: houdt in dat persoonsgegevens worden afgeschermd voor het gebruik voor andere doelen dan de doelen waarvoor ze mogen worden gebruikt.
- *Corrigeerbaarheid*: voor elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens aan te passen of te vernietigen, indien de verwerking niet voldoet aan de eisen; bijvoorbeeld in geval van onjuiste informatie of als er geen noodzaak meer is om de informatie te bewaren.
- *Transparantie*: over elke verwerking van persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, de categorieën persoonsgegevens, categorieën van betrokkenen, categorieën van ontvangers, doelbinding, de wettelijke grondslag, de bewaartermijnen, de beveiligingsmaatregelen en de organisatorische en technische inrichting van verwerking van de persoonsgegevens.

In de volgende tabellen staan per ACT-doel de privacyprincipes beschreven. Per privacyprincipe wordt aangegeven welke criteria leidend zijn om aan het privacyprincipe te kunnen voldoen. De ondersteunende criteria zijn randvoorwaardelijk voor een effectieve invulling van de leidende criteria.

Afscherming		
Privacyprincipe 1: Doelbinding		
Persoonsgegevens worden slechts verzameld en verwerkt voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en worden niet verder verwerkt voor doelen die hiermee onverenigbaar zijn.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.01 Doelbinding gegevensverwerking U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	B.01, U.02
Privacyprincipe 2: Doelbinding		
De verzameling en verwerking van persoonsgegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. De persoonsgegevens zijn daartoe toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.01 Doelbinding gegevensverwerking	U.02, B.03

Afscherming		
Privacyprincipe 3: Bewaren		
Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.06 Bewaren van persoonsgegevens	U.02
Privacyprincipe 4: Beveiliging		
Passende technische en organisatorische maatregelen, zoals pseudonimisering van persoonsgegevens, zijn op een dusdanige manier getroffen dat een passende beveiliging van de verwerking en de persoonsgegevens gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.04 Beveiligen van de verwerking van persoonsgegevens	B.03, C.03
Privacyprincipe 5: Doorgifte naar derden		
Persoonsgegevens worden slechts doorgegeven wanneer formeel afdoende garanties zijn vastgelegd, zodat aangetoond kan worden dat ook bij doorgifte aan de AVG wordt voldaan.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.07 Doorgifte persoonsgegevens	B.02, U.02

Corrigeerbaarheid		
Privacyprincipe 6: Kwaliteit		
De persoonsgegevens en de verwerking ervan voldoen aan vooraf vastgestelde kwaliteitseisen, zodat ze juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens, die gelet op de doeleinden waarvoor zij worden verwerkt onjuist zijn, onverwijld te wissen of te rectificeren.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.03 Kwaliteitsmanagement	C.02

Transparantie		
Privacyprincipe 7: Verantwoording (accountability)		
Verantwoordelijken hebben aantoonbaar maatregelen genomen, zodat de wijze van verwerken ten aanzien van de betrokkene behoorlijk is, waarbij de risico's zijn geëlimineerd of gemitigeerd door het toepassen van Privacy by Design, het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's) en het gebruik van standaardinstellingen.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	B.03 Risicomanagement, Privacy by Design en de DPIA C.01 Intern toezicht	B.02, U.02

Transparantie		
Privacyprincipe 8: Recht op transparantie		
De wijze waarop de persoonsgegevens worden verwerkt is voor het publiek en de betrokkene transparant en maakt het de betrokkene mogelijk zijn rechten uit te oefenen. Hierbij is specifiek aandacht voor de bescherming van kinderen. Bij een inbreuk in verband met persoonsgegevens (datalek, 'personal data breach') worden de betrokkenen en de AP geïnformeerd als deze inbreuk waarschijnlijk een risico inhoudt voor de rechten en/of vrijheden van natuurlijke personen.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	B.01 Privacybeleid C.02 Toegang gegevensverwerking voor betrokkenen C.03 Meldplicht Datalekken	B.02, U.02, U.05

3.3 Risico's bij niet voldoen aan de AVG

Hoewel we vanaf deze plaats niet mogen garanderen dat je voldoet aan de AVG als je voldoet aan de Baseline, kan toch redelijkerwijs worden gesteld dat voldoen aan de Baseline betekent dat een organisatie de beginselen van de AVG voldoende naleeft. Het *niet* naleven van de AVG kan verregaande (negatieve) consequenties hebben.

Voorbeelden van risico's voor de betrokkene:

- De mogelijkheid om anoniem gebruik te maken van bepaalde diensten wordt gefrustreerd.
- Persoonsgegevens worden op onrechtmatige wijze gedeeld of gebruikt.
- Persoonsgegevens worden gebruikt voor doeleinden waar de betrokkenen niet van op de hoogte zijn.
- Het koppelen van systemen kan ertoe leiden dat meer persoonsgegevens worden gebruikt dan noodzakelijk is en er mogelijk nieuwe en niet gecontroleerde gegevensprofielen ontstaan uit combinaties van op zichzelf staande brongegevens, waardoor onverenigbaarheid ontstaat met de wettelijke grondslag en/of doelbinding.
- Personen in kwetsbare groepen lopen een groter risico op nadelige gevolgen, zoals uitsluiting, discriminatie of stigmatisering, wanneer zij het slachtoffer zijn geworden van oneigenlijk gebruik van hun persoonsgegevens.
- Persoonsgegevens worden niet of onjuist beheerd, waardoor een wildgroei aan bestanden met persoonsgegevens ontstaat met stijgende veiligheidsrisico's tot gevolg.

Voorbeelden van risico's voor de organisatie:

- Negatieve publiciteit en imagoschade.
- Dwangmaatregelen of boetes opgelegd door de toezichthouder wegens het niet naleven van de wetgeving.
- Schadeclaims door betrokkenen.
- Hogere kosten bij het achteraf nemen van privacymaatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business c.q. de keten.
- Datalekken leiden tot wantrouwen.

Voorbeelden van juridische risico's:

- Niet naleven van privacy regelgeving.
- Niet naleven van sectorale regelgeving.
- Niet naleven van mensenrechten.

Ten slotte: elke eis die de privacywetgeving stelt brengt een eigen risico met zich mee wanneer je er niet aan voldoet. In de Baseline zijn de wettelijke eisen vertaald naar concrete normen en is per norm aangegeven welke (niet-juridische) risico's het niet-voldoen aan de norm met zich meebrengt.

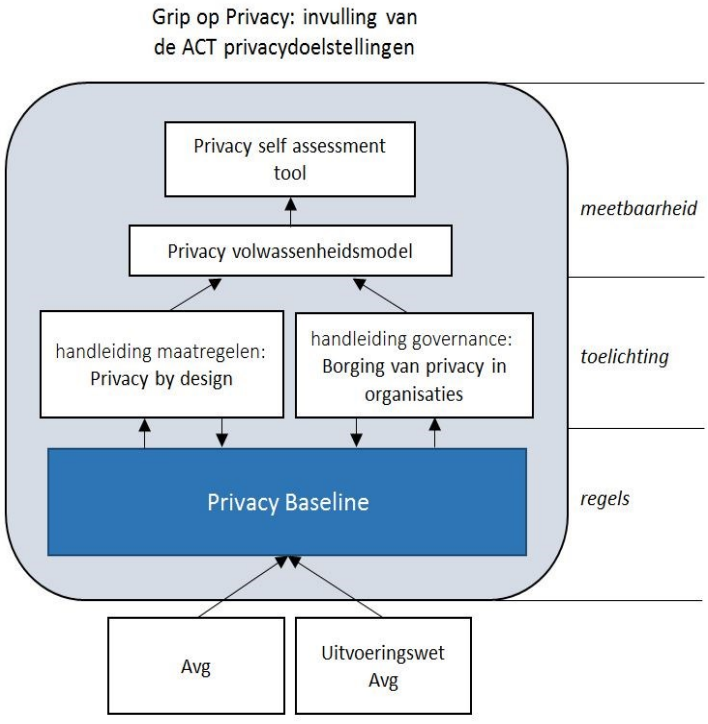
3.4 Grip op privacy

De Privacy Baseline is onderdeel van een set van samenhangende documenten onder de noemer 'Grip op privacy'. Geënt op deze Baseline heeft het CIP de volgende vier documenten gepubliceerd:

- Privacy by Design
- Privacy Governance ('Borging van privacy in organisaties')
- Privacy Volwassenheidsmodel
- Privacy Self Assessment

De eerste twee documenten zijn handreikingen voor het toepassen van de juiste maatregelen en het inrichten van de organisatie waarmee grip op privacy op de meest efficiënte en effectieve wijze kan worden bereikt. Het zijn toelichtende verhandelingen over:

- Hoe je kunt bewerkstelligen dat het aspect privacy niet achteraf nog eens moet worden 'bijgeplakt', maar van begin af aan in de ontwikkeling van programmatuur wordt meegenomen (privacy *by design*).
- Hoe je privacy in alle relevante bedrijfsprocessen implementeert, borgt, kunt onderhouden en verbeteren (governance).



Figuur 3: Grip op Privacy

3.5 Privacyvolwassenheid

Bij deze Baseline hoort een speciaal daarop gebaseerd volwassenheidsmodel. Door privacy actief te hanteren als kwaliteitselement in de bedrijfsvoering kunnen organisaties naar een hoger niveau van volwassenheid groeien en privacy benutten om de dienstverlening aan klanten of ketenafnemers op een hoger peil te brengen. Dit aspect wordt ter hand genomen in het document 'Privacy volwassenheidsmodel', een praktische handleiding voor het vaststellen en vergroten van de organisatievolwassenheid in relatie tot de omgang met persoonsgegevens. Het model is afgeleid van gangbare 5-laagse volwassenheidsmodellen. Op basis van de mate waarin voldaan wordt aan de dertien criteria van de Privacy Baseline specificeert het model 5 niveaus op het aspect van privacy.

Hoe volwassen gaat de organisatie met privacy om? Welk niveau wil de organisatie nastreven en wat is daarvoor nodig? Op deze vragen geeft het Privacy Self assessment (PriSa) antwoorden. Het assessmentrapport geeft aan wat nog te doen staat om het (zelf te kiezen) beoogde volwassenheidsniveau te bereiken. Op de website van het CIP (www.cip-overheid.nl) lees je er meer over. Daar vind je ook de overige hier aangehaalde Grip-op-privacy documenten.

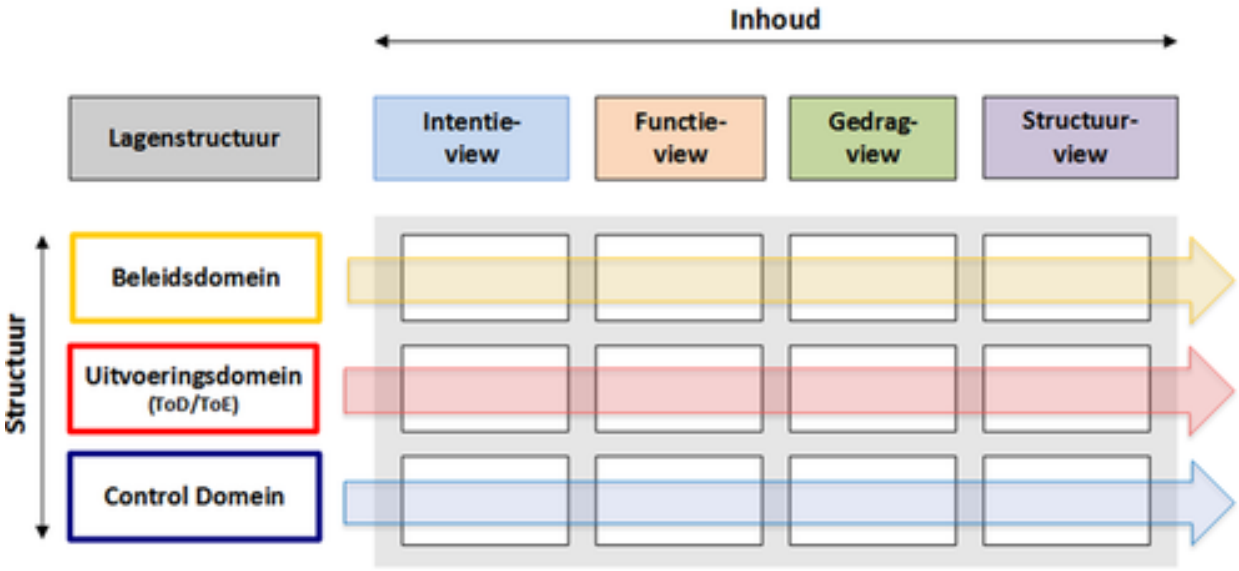
Grip op privacy biedt concrete handvatten om de juiste omgang met persoonsgegevens te bewerkstelligen, te waarborgen en het privacybeleid passend, effectief en efficiënt in te passen in de bedrijfsvoering. Het gaat niet om de normen. Het gaat erom de ACT principes: *Afscherming*, *Corrigeerbaarheid* en *Transparantie* te realiseren en daarmee de betrokkene maximaal te respecteren in zijn privacy.

Bijlage: De SIVA-methode, korte uitleg

Het raamwerk

De Privacy Baseline is gebaseerd op de SIVA-methode[262]. Deze methode hanteert een raamwerk dat is onderverdeeld in domeinen, met daarbij een separaat algemeen gedeelte dat beleidsaspecten en beheersingsaspecten bevat. Dit raamwerk bevat specifieke lagen en kolommen om een verband tussen de beveiligingsmaatregelen voor de applicatie-omgeving weer te geven.

De structuurdomeinen zijn: Beleid, Uitvoering en Control; de inhoudsdomeinen: Intentie, Functie, Gedrag en Structuur. Zo ontstaat de volgende matrix:



Figuur 4: Het SIVA-raamwerk

[262] W.N.B. Tewarie, SIVA, Methodiek voor de ontwikkeling van auditreferentiekaders, VU University Press, Amsterdam 2014. Het proefschrift waarop deze publicatie is gebaseerd is: Tewari, W.N.B., Model Based Development of Audit Terms of Reference: A Structured Approach to IT Auditing, Amsterdam 2010, ISBN 978-90-8659-456-6.

Het voordeel van het hanteren van deze methode is dat duidelijk wordt aangegeven wie wat binnen een norm moet doen, terwijl tevens duidelijk wordt wat de context is van de norm.

Door uit bestaande kaders, zoals ISO27002, SoGP, etc. normen in deze matrix onder te brengen, wordt zichtbaar waar nog gaten zitten en wordt duidelijk waar aanvullingen nodig zijn. De uitkomst van een consequent doorgevoerde SIVA-aanpak is een complete en eenduidig geformuleerde beschrijving van de normen.

Het SIVA-raamwerk

Het SIVA-raamwerk bestaat uit vier componenten, te weten *Structuur*, *Inhoud*, *Vorm* en *Analysevolgorde*. Deze componenten zijn hulpmiddelen en worden als volgt omschreven:

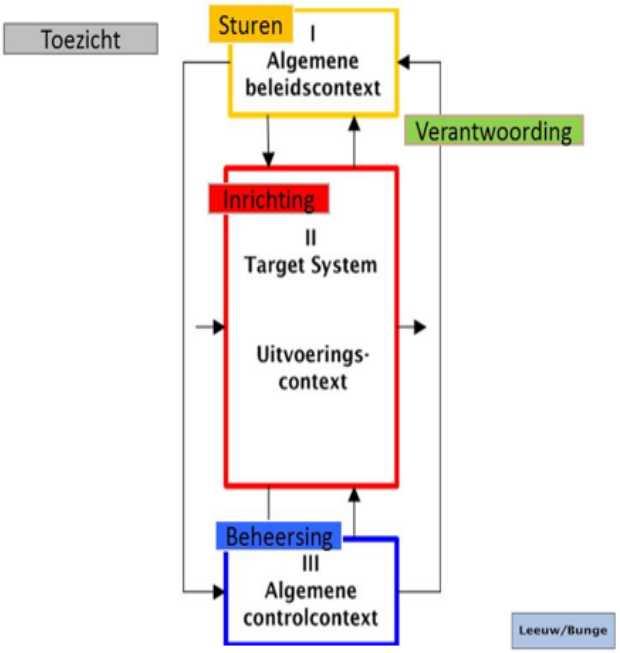
- ***S****tructuur*: De omgeving, in dit geval de applicatie-omgeving, is verdeeld in een aantal domeinen. Dit bevordert de volledigheid, relevantie, duidelijkheid en samenhang van de aspecten die worden onderzocht.
- ***I****nhoud*: Vanuit verschillende invalshoeken worden per domein basiselementen geïdentificeerd.
- ***V****orm*: Per element worden de beveiligingseisen geformuleerd door middel van een formuleringsvoorschrift (template).
- ***A****nalysevolgorde*: Een iteratief analyseproces van de bij structuur genoemde lagen.

Structuur

De structuur van de Privacy Baseline komt overeen met drie contexten: de beleids-, uitvoerings- en control-context. De SIVA-methode hanteert deze structuur, die is gebaseerd op de algemeen gangbare structuur voor een auditomgeving en past daarbij de functionele benadering toe uit de systeemtheorie[263]. Deze structuur is nodig voor het verkrijgen van een compleet overall beeld, waarbinnen de criteria voor de Privacy Baseline konden worden geïdentificeerd.

[263] Voor de concrete invulling van deze functionele benadering is gebruik gemaakt van het 3C model (Leeuw, 1974 en Bunge, 1979) en de managementcyclus (MC) Planning, Implementation en Evaluation (PIE) (Starreveld, 2002).

Inhoud



Figuur 5

De component 'inhoud' wordt in de SIVA-methode bereikt door middel van vier invalshoeken: intentie, functie, gedrag en structuur (IFGS). Vanuit elke IFGS-invalshoek kan een specifieke verzameling basiselementen (objecten) worden geïdentificeerd.

De invalshoeken houden het volgende in:

Intentie - het waarom-aspect. De bestaansreden van een organisatie. Voorbeelden: organisatie, visie, doelstellingen, wetten en beleid, stakeholders en middelen.

Functie - het wat-aspect. De organisatorische en technologische elementen die de intenties van de organisatie moeten realiseren. Voorbeelden: organisatorische- en technische functies, processen, taken en taakvereisten.

Gedrag - het hoe-aspect (gedragsaspect). De menselijke en technische resources en eigenschappen van de technische resources die de organisatorische- en technische functies moeten vormgeven. Voorbeelden: actor, object, interactie, toestand, eigenschap en historie.

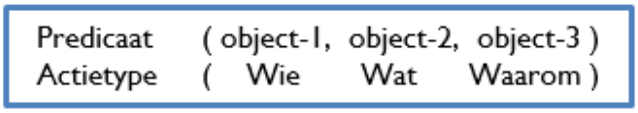
Structuur - het hoe-aspect (vormaspect). De manier waarop een organisatorische- en personele structuur is vormgegeven. Voorbeelden zijn: business-organisatiestructuur, business-architectuur, IT-architectuur en business-IT-alignment.

De relaties tussen de objecten vanuit de IFGS-invalshoeken kunnen als volgt worden gelezen: de elementen uit de intentie- of doel-invalshoek reguleren en/of worden bereikt door elementen uit de functie-invalshoek. De elementen uit de functie-invalshoek gebruiken of realiseren de elementen uit de gedrag-invalshoek die op hun beurt worden vormgegeven door elementen uit de structuur-invalshoek.

Het gebruik van de invalshoeken (views) is een belangrijk kernonderdeel van de SIVA-methode om, voorafgaand aan het opstellen van de principes en normen, lacunes in de objectenanalyse te ontdekken.

Het onderwerp van de Privacy Baseline is echter niet Privacy, maar de Privacywetgeving. De pretentie van de Privacy Baseline niet om de wet op volledigheid en consistentie te toetsen, doch om de gebruiker een handzame en geannoteerde set van toetsbare criteria mee te geven die hem helpen zich aan de wet te houden.

Vorm



Figuur 6: Formele syntax

De Vorm-component van het SIVA-raamwerk geeft een formule (syntax) weer voor de normen:

In deze formule komen vier elementen voor. Het eerste element is de handeling (actietype). Het tweede en derde element zijn de objecten welke de handeling uitvoeren (actor, wie) respectievelijk ondergaan (wat). Het vierde element vertegenwoordigt het resultaat of doel van de handeling. De onderstaande tabel verduidelijkt deze elementen.

Wie	*Betrokken Actor*
Wat	*Hierbij worden zaken uitgedrukt:* • *die gedaan moeten worden om doelen te bereiken/te realiseren/te controleren/te bewaken en verantwoording te kunnen afleggen,* • *wat iemand moet doen of* • *wat een gegevensverwerking doet.*
Actietype	*Specifieke werkwoorden gerelateerd aan het wat-aspect en aan een bepaalde laag.*

Figuur 7: Functionele relaties

Analysevolgorde

Analysevolgorde gaat over het proces om te komen tot de normen en is hier niet relevant, omdat we uitgaan van de wettelijke kaders.

Gebruikte template

De elementen 'wat' en 'waarom' zijn separaat vermeld. In de uitdrukking van de normen worden trefwoorden gebruikt die als indicatoren dienst doen. Per indicator worden indicatoren benoemd. De indicatoren geven inzicht in hoe aan het criterium kan worden voldaan. De trefwoorden in de formulering van het criterium zorgen ervoor dat slechts relevante aspecten per criterium worden benoemd.

Bij de uitwerking van de criteria van de Privacy Baseline is gebruik gemaakt van een template, waarbij het element 'wie' veelal achterwege is gelaten. Dit element komt wel terug in de indicatoren van de criteria, zodat duidelijk wordt wie welke verantwoordelijkheid heeft voor de realisatie van dat deel van de norm. Het gebruikte template voor de normen is:

Onderwerp van de norm						
Criterium (wie en wat)	Wat (xxxxxx) <werkwoord> xxxxx trefwoorden xxxxx					
Doelstelling (waarom)	De reden waarom de norm gehanteerd wordt.					
Risico	Het risico dat de aanleiding vormt om de norm te hanteren.					
Referentie	Bron 1	Bron 2	...			
Conformiteitsindicatoren en maatregelen						
Conformiteitsindicator (trefwoord)						
/01	Maatregel 01					
/02	Maatregel 02.					
...	...					

Figuur 8: De SIVA-schrijfwijze

Een *conformiteitsindicator* is een (sub)norm waaraan voldaan moet worden om aan het criterium (de hoofdnorm) te kunnen voldoen. Conformiteitsindicatoren hebben in de tekst van de hoofdnorm een anker in de vorm van een *trefwoord* dat de subnorm aanduidt. Je kunt stellen dat ieder onderstreept trefwoord gedefinieerd en uitgewerkt wordt in de vorm van maatregelen.

Per conformiteitsindicator worden een of meer maatregelen (/01, /02, etc.) geformuleerd, op basis waarvan een uitspraak mogelijk is over de desbetreffende conformiteitsindicator.

In veel gevallen volgt een nadere uitleg van de maatregelen in toelichtingen onder het kader.

Dit maakt de Baseline niet alleen een heldere verzameling van instructies die je stapsgewijs vertellen hoe je privacy in de organisatie kunt bewerkstelligen, hij biedt ook het kader waartegen je gedetailleerd kunt toetsen hoe de organisatie ervoor staat.

Bijlage: Logboek kleine wijzigingen

Rapport van kleine aanpassingen die zijn doorgevoerd, meestal op aangeven van gebruikers, zonder dat het versienummer is opgehoogd.
In de wiki-versie https://www.noraonline.nl/wiki/De_Privacy_Baseline worden dergelijke aanpassingen doorgevoerd waarbij de redactiedatum van de pagina wordt aangepast.

2020-10-27: foutieve nummering van toelichtende tekstblokjes gecorrigeerd op p. 67 en p. 74.
2

2024-05: enkele taalkundige en actualisatie updates