Grip op Privacy:

de Privacy Baseline

de Algemene verordening gegevensbescherming ontrafeld voor toepassing in organisaties

Status	versie 3.0 ; eerste oplevering in overeenstemming met de Avg
Auteurs	Marcel Koers (CIP), met medewerking van: Leden van de werkgroep PB2AVG en de Domeingroep Privacy (zie colofon) Ruud de Bruijn (CIP)
Datum	7 mei 2017
Filenaam	20170507 Privacy Baseline v3_0

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Deze publicatie valt in categorie 2: "becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties". Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site https://cip.pleio.nl.

CIP-documenten kunnen van tijd tot tijd aanpassingen ondergaan of worden ingetrokken als gevolg van veranderde inzichten. De CIP-redactie streeft binnen haar mogelijkheden naar een zo actueel mogelijke status van de documenten. In de praktijk zal enige tijd verstrijken voordat wijzigingen kunnen zijn doorgevoerd. Suggesties voor aanpassingen kunnen ook door lezers worden aangedragen en worden altijd in behandeling genomen.

Bij deze publicatie

Voor definities en achtergronden van de Privacy Baseline wordt primair verwezen naar de privacywetgeving, i.e. de Algemene verordening gegevensbescherming, De Uitvoeringswet Avg en het Memorie van Toelichting daarbij, secundair naar de publicaties van de Artikel 29-werkgroep en publicaties van de Autoriteit Persoonsgegevens.

In de Privacy Baseline wordt de privacywetgeving zo consciëntieus mogelijk vertaald naar concrete aanwijzingen of perspectieven voor handelen met als doel daarmee aan die wetgeving te kunnen voldoen alsmede een verantwoorde belangenafweging daarvoor te kunnen maken. De samenstellers zijn daarbij uitgegaan van wat bij het schrijven van de teksten praktisch en volgens de vigerende inzichten en beschikbare kennisbronnen juist werd geacht te zijn. Voortschrijdend inzicht, jurisprudentie en mogelijk aanpassing van de wetgeving zullen hierop in de toekomst aanleiding tot herziening, aanvulling of aanpassing zijn.

Vooraf

Het kan voor organisaties een uitdaging zijn om op een juiste manier met de 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. Daarvoor is de Privacy Baseline ontwikkeld: de Privacy Baseline geeft organisaties concrete handvatten om persoonsgegevens op de juiste manier te beschermen. In de Privacy Baseline zijn de eisen van de Algemene verordening gegevensbescherming (Avg) 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.

De eerste editie van de Baseline heeft de Wet bescherming persoonsgegevens (Wbp) als uitgangspunt. Dat document (versie 2.0) is nog geldig tot 25 mei 2018. Op die datum komt de nationale Wbp te vervallen en hebben organisaties zich te houden aan de Europese Avg. De Uitvoeringswet Algemene verordening gegevensbescherming en het Memorie van toelichting daarbij maken onderdeel uit van een breder pakket dat in zijn geheel de verordening EU/2016/679 en de richtlijn EU/2016/680 zal uitvoeren respectievelijk implementeren[1].

Déze editie van de Baseline (Versie 3.0) is de eerste versie die de Algemene verordening gegevensbescherming (Avg) als uitgangspunt neemt. De Avg is de eerste Europese privacywet en is op 26 mei 2016 in werking getreden. Aan de verordening is vijf jaar is gewerkt en zij bevat nog veel concessies van de lidstaten. Deze punten zullen naar verwachting nog nader worden uitgewerkt.

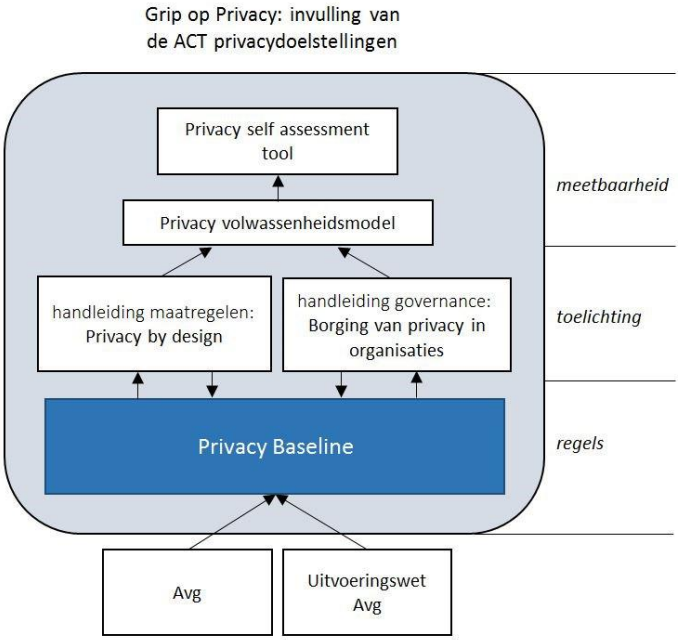
Vooralsnog wordt dit aan de Nationale wetgeving van de lidstaten overgelaten. Voor Nederland krijgt dit vorm in een uitvoeringswet bij de Avg. Deze wet vult de plaatsen in die in de Europese Avg aan de lidstaten ter invulling zijn overgelaten. De ambitie van CIP is om deze Baseline hiermee uiteindelijk volledig te laten overeenkomen. In dit document verwijzen wij naar deze uitvoeringswet plus het memorie van toelichting als: de Uitvoeringswet Avg.

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 'normenkader privacy' geworden en dat maakt het niet direct een gemakkelijk leesbaar document. Het is eerder een naslagwerk waarmee de verwerkingsverantwoordelijke kan controleren in hoeverre hij aan privacy wet- en regelgeving voldoet en afwegingen te maken bij die zaken die hem daarvoor – volgens de Baseline – nog te doen staan.

[1] De uitvoeringswet betreft de regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming) (PbEU 2016, L 119).

Grip op privacy
De Privacy Baseline is onderdeel van een set van samenhangende documenten onder de noemer 'Grip op privacy'. Naast deze Baseline heeft het CIP nog vier, daarop geënte documenten gepubliceerd:

- Privacy by Design
- Privacy Governance
- Het Privacy Volwassenheidsmodel
- Het Privacy Self Assessment



De eerste twee documenten zijn handreikingen voor de toepassing van de juiste maatregelen en de inrichting 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 (by design).
- Hoe je privacy in alle relevante bedrijfsprocessen implementeert, borgt, kunt onderhouden en verbeteren (governance).

Bij deze Baseline hoort een speciaal daarop gebaseerd volwassenheidsmodel. Door privacy actief te hanteren als kwalitatief element in de bedrijfsvoering, kunnen organisaties privacy benutten om de dienstverlening aan de klanten op een hoger peil te brengen (privacy als 'unique selling point') en zo naar een hoger niveau van volwassenheid te komen. 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 Privacy volwassenheidsmodel is tevens een referentiemodel, afgeleid van gangbare 5-laagse volwassenheidsmodellen. Het specificeert de niveaus op het aspect van privacy. De 5 niveaus worden gedefinieerd aan de hand van de de mate waarin je voldoet aan de Privacy Baseline.
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 tool antwoorden. Het geeft aan wat je nog te doen staat om het (aan het begin zelf gekozen) volwassenheidsniveau te bereiken.

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 maximaal de betrokkene te respecteren in zijn privacy. Dit wordt verderop in het document uitgebreid behandeld.

Draagvlak door brede inbreng uit het CIP-netwerk
De methode 'Grip op Privacy' en de afzonderlijke documenten daarvan zijn tot stand gekomen door nauwe samenwerking met en tussen verschillende partijen in het CIP-netwerk. De auteurs danken alle CIP-ers, geïnterviewde deskundigen, leden van de CIP Domeingroep Privacy, de Werkgroep Pb2Avg en de Werkgroep Privacy By Design, die een bijdrage hebben geleverd aan het samenstellen van de methode. Hun bijdragen en het gegeven dat een breed palet van organisaties hen daartoe in staat stelt, geven de auteurs het vertrouwen dat de methode 'Grip op privacy' voldoende draagvlak heeft voor een brede toepassing en verdere ontwikkeling.

Over CIP
CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheids-organisaties. Het heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waarin ook gespecialiseerde marktorganisaties als kennispartners deelnemen.
Het centrum is opgericht voor informatieuitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening. Inmiddels bestaat het CIP-netwerk uit een groot aantal overheidsorganisaties en (private) kennispartners. Kennis die in deze organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt.

Het produceren van themadocumenten met zoveel mogelijk inbreng vanuit het netwerk is er één van. Aangesloten organisaties leren van elkaars oplossingen en werkwijzen en kunnen samen komen tot afspraken daaromtrent. Door meer samen doen draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen. De producten van het CIP worden om niet ter beschikking gesteld.

Amsterdam, 7 mei 2017

Inhoudsopgave

Inleiding

Informationele privacy als uitgangspunt
Eind 2014 kreeg CIP uit de CIP community de vraag om eens op te schrijven "hoe dat nou moet, met die privacy". De vraag was niet uit voortgekomen uit naïviteit, maar uit de wirwar aan informatie en opvattingen over privacy.
Het antwoord hebben we gezocht in de pragmatiek: pak privacy bij de kop zoals organisaties en bedrijven ermee zouden moeten werken. Daarvoor gelden immers wetten en voorschriften en de discussie over óf het moet en wát er moet is dus al gepasseerd. Met de overgang van Wet bescherming persoonsgegevens naar de Algemene verordening gegevensbescherming (Avg) is er op dat laatste punt overigens nog wel wat te doen, wat betekent dat deze Baseline nog de nodige aanpassingen zal moeten ondergaan. Dat heeft het CIP niet belet om de huidige versie alvast deelbaar te maken, als een bijdrage aan het streven van organisaties om de omgang met persoonsgegevens op een verantwoorde manier in te regelen.
Alle andere, overigens zeer interessante bespiegelingen die mogelijk zijn over het privacybegrip begeven zich op terreinen van filosofie, sociologie en psychologie, kennen persoonlijke opvattingen en emoties en zijn plaats-, tijd- en cultuurgebonden. De Avg inclusief de Uitvoeringswet Avg en het daarbij horende Memorie van toelichting (Mvt) vormen de geldende privacykaders en wat je er ook van vindt, daaraan heb je als bedrijf of organisatie te voldoen[2,3].

Informationele privacy als uitgangspunt
Organisaties kunnen ervoor kiezen om 'slechts' te voldoen aan de wet. Maar Privacywetgeving is niet uitsluitend een hinderpaal. Door verantwoord en efficiënt om te gaan met de balans tussen wetgeving, de taakstelling van de organisatie en de persoonlijke levenssfeer van betrokkenen, is 'privacy' ook als een kwaliteitskenmerk ten voordele te benutten. Er zijn al commerciële bedrijven die hun privacybeleid bewust in hun marketing etaleren. Overheidsorganisaties moeten in dit opzicht bij uitstek het goede voorbeeld geven.
In dit 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 je als organisatie transparant en concreet wil zijn over je beleid, en als je en passant ook netjes wil voldoen aan de wettelijke vereisten om boetes, imagoschade en schadeclaims te voorkomen, dan moet je proactief werk maken van het type privacy dat informationele privacy wordt genoemd.

Informationele privacy gaat over bescherming van personen in verband met informatie die van of over hen bekend is en/of ten aanzien van hen wordt toegepast[4]. Dit wordt ook wel bescherming van persoonsgegevens (of: gegevensbescherming) genoemd en is verankerd in de Grondwet[5] en verder uitgewerkt in de Avg en de Uitvoeringswet Avg.

[2] Wij verwijzen naar deze Uitvoeringswet plus het Mvt als: de Uitvoeringswet Avg.
[3] Bedrijven en organisaties: wij hanteren 'organisatie' voor beide aanduidingen in de publieke en private sectoren.
[4] S. Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet*, SDU Uitgevers, Den Haag, 2005, p.19.
[5] Art. 10 lid 2 van de Grondwet.

De doelstelling van deze Privacy Baseline
De Privacy Baseline vertaalt de privacywetgeving naar concrete, hanteerbare normen die duidelijk aangeven waar organisaties wat moeten regelen in hun privacybeleid, de uitvoering en de controle erop; de Privacy Baseline biedt concrete handvatten voor de juiste omgang met persoonsgegevens. Correct omgaan met persoonsgegevens houdt in dat de organisatie voldoet aan de doelstellingen van Afscherming, Corrigeerbaarheid en Transparantie. Zij bieden adequate waarborgen voor borging van de informationele privacy van betrokkenen en helpen organisatie rode kaarten, bindende aanwijzingen en/of boetes vanuit de Autoriteit Persoonsgegevens (hierna: AP) te voorkomen. Want de Baseline is bij uitstek ook het hulpmiddel dat organisaties in staat stelt te voldoen aan de vereiste van 'accountability', in de Nederlandstalige Avg 'verantwoordingsplicht' genoemd, die inhoudt dat naleving van de wet moet kunnen worden aangetoond. Verantwoordingsplicht houdt tevens documentatieplicht in en ook die vereiste is concreet in de Baseline verwerkt.

Leeswijzer

In Deel I worden de beginselen van informationele privacy behandeld (de ACT-doelen) in relatie tot de wet. Zij geven de criteria in deel II een verband en context. De Baseline zelf (Deel II: De Privacybaseline: De Privacy Baseline) bevat de normen of 'criteria' die moeten worden gehaald, 13 stuks in totaal.

Voor wie is de Privacy Baseline geschreven?
De verwerkingsverantwoordelijke heeft vanuit de Avg de opdracht om te bepalen of en hoe persoonsgegevens verwerkt worden. De Privacy Baseline is een naslagwerk dat hem in staat stelt te controleren in hoeverre de verwerking aan de wet voldoet. Daaruit volgt eigenlijk al dat het een document is voor professionals die hands-on in de organisatie werken aan privacymaatregelen, de borging ervan en de controle erop, en zij die daar dicht bij in de buurt leiding aan geven. Zoals de Baseline helpt bij de realisatie van de documentatie- en verantwoordingsplicht ten behoeve van de controlerende autoriteit of de vragende burger, zo kan natuurlijk ook de interne rapportage ten behoeve van de verantwoordingsplicht ermee geholpen zijn.

Deze Privacybaseline beoogt zo concreet mogelijk aan te geven wat een organisatie moet doen om te voldoen aan de privacywetgeving. Wij hebben dat ingevuld door de wetgeving naar concrete ondubbelzinnige normen te vertalen. Een privacy-normenkader dus. De ingevoerde lezer, de (privacy) professional die thuis is in de informatiebeveiliging, zal het format van de Privacy Baseline herkennen en 'normen' op waarde weten te schatten en naar de praktijk weten te vertalen.
Wie zich eerst beter wil inlezen of verdieping zoekt raadpleegt de twee handleidingen: 'Privacy by design' en 'De borging van privacy in organisaties' ('Privacy Governance') [6].

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 wél naar het privacyvolwassenheidsniveau 3, en doorgaans is dat niveau voldoende om de compliancy-toets te doorstaan. Wij komen over de volwassenheidsniveaus nog te spreken.

[6] Beide publicaties zijn te vinden op www.cip-overheid.nl.

Reikwijdte van dit document
Deze Baseline richt zich op de eisen die de privacywetgeving stelt aan organisaties en wat organisaties moeten doen. De bevoegdheden van de AP, de Nederlandse toezichthouder, en de eisen die de wet aan de AP stelt, vallen daarom buiten de scope van dit document.
Over de AP nog dit: de Avg spreekt consequent over "de bevoegde toezichthoudende autoriteit". Dat moet omdat het kan voorkomen dat de toezichthouder die een overtreding behandelt niet altijd de toezichthouder voor het land is, waarin de overtreding is geconstateerd. Tenzij de context anders vereist spreken wij hierna van de AP als de bevoegde toezichthoudende autoriteit.

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

Wanneer is de Baseline van toepassing?
De Privacy Baseline is voor organisaties die met persoonsgegevens werken. Ga, alvorens te beginnen met deze Baseline, het volgende na:

	Vraag	Antwoord
Vraag 1	Wil/moet ik een persoonsgegeven verwerken? (Een persoonsgegeven bevat informatie over een geïdentificeerde of identificeerbare natuurlijke, levende persoon). Persoonsgegevens kunnen direct of indirect identificeerbaar zijn, zie hiervoor §1.3.3. Een verwerking is een bewerking of een geheel van bewerkingen met betrekking tot (een) persoonsgegeven(s) en is een zeer breed begrip (zie §1.3.1).	Nee? De Avg - en dus deze Baseline - is niet van toepassing.
Vraag 2	Kan ik deze verwerking baseren op een van de rechtmatige gronden van de privacywetgeving het criterium U.01 Doelbinding gegevensverwerking (§2.2.1).	Is het antwoord op vraag 1 'ja', maar is het antwoord op vraag 2 'nee'? U mag dan geen persoonsgegevens verwerken.

Aan deze vragen ligt het centrale uitgangspunt uit de Avg ten grondslag dat persoonsgegevens enkel moeten worden verwerkt indien het doel van de verwerking redelijkerwijs niet op een andere wijze kan worden verwezenlijkt. Dit houdt concreet in dat je persoonsgegevens alleen mag verwerken als je de gegevens noodzakelijk zijn om het beoogde doel te bereiken. Ga dus altijd na of je het doel ook kan bereiken *zonder* gegevens daarbij te gebruiken die te herleiden zijn tot een natuurlijke persoon.

Wijzigingen in versie 3.0
In versie 3.0 is de Baseline aangepast aan de gewijzigde privacywetgeving die van toepassing is per 25 mei 2018. Dit document is geschreven vanuit de kennis van de wetgeving in april 2017; met name de Uitvoeringswet Avg is dan nog niet definitief. Tevens is zijn de baselinecriteria 'gesaneerd' en is hun aantal teruggebracht tot 13. Van een 'trendbreuk' is echter geen sprake.

Naslagliteratuur
De feitelijke tekst van de verordening, waarin de overwegingen en artikelen ongerelateerd achter elkaar worden neergezet, is nogal gebruikersonvriendelijk. Even zoeken op internet met "GDPR" (General Data Protection Regulation) levert een reeks aan titels op die in dit opzicht soelaas bieden. Wij noemen er enkele uit eigen ervaring. Deze publicaties zijn niet vrijelijk te verkrijgen:

- http://www.bju.nl/juridisch/catalogus/tekstuitgave-privacyverordening-1
- https://www.managementboek.nl/boek/9789082083446/de-algemene-verordening-gegevensbescherming-editie-2017-arnoud-engelfriet
- http://www.nomos-shop.de/Albrecht-Jotzo-neue-Datenschutzrecht-EU/productview.aspx?product=27238

Deze verwijzingen komen uit de CIP-publicatie "20170425 Tussen Wbp en Avg, over de invoering van de Avg" (april 2017), te vinden op www.cip-overheid.nl. Op deze site vind je ook alle documenten van de methode 'Grip op privacy'.

Colofon

Deze versie van de Privacy Baseline is mede tot stand gekomen dankzij de slagvaardigheid van de Werkgroep PB2Avg (2017), die de realisatie van de nieuwe Baseline als project heeft geadopteerd. De werkgroep is ontstaan als een initiatief vanuit de Domeingroep Privacy en zal nog actief blijven totdat een 'definitieve' versie is gemaakt op basis van een vastgestelde Uitvoeringswet Avg - naar verwachting dus nog tot uiterlijk eind mei 2018.

De Domeingroep en de Werkgroep zijn samengesteld uit professionals die bij elkaar een breed palet van organisaties uit het CIP-netwerk bijeen brengen. Zonder anderen te kort te willen doen, zijn bij deze productie in het bijzonder te noemen: Barry Bastiaansen (Min.BZK), Leo Benschop (ControlSolutions International), Remy van den Boom (IND/MinV&J), Patrick Dersjant (RWS), Meine van Essen (RWS), Ludwig Geers (UvT), Jan de Heer (NOREA), Marcia van den Hil (CBR), Ted Mos (DJI/MinV&J|TBM Groep), Daniëlle Oudhuis (Hoogheemraadschap Hollands Noorderkwartier), Annemarie Paalhaar (CompLions) en Herman Weenink (IBM). Het werk van Marjon Mertens van het BKWI heeft ons een hele goede start gegeven.

Het CIP is tevens dank verschuldigd aan de vele organisaties en hun afgevaardigden die betrokken zijn geweest bij de eerste editie van de Privacy Baseline (versies 1 en 2). Hoewel de samenstelling van de huidige groep contribuanten uit het CIP-netwerk een heel andere is, blijft de oorspronkelijke Baseline zeer herkenbaar en in de kern volledig overeind in deze nieuwe editie.

Verantwoordelijk voor de eindredactie en het publicatieklaar maken zijn Ruud de Bruijn en Marcel Koers. Reacties kun je sturen naar ruud.cip.debruijn@uwv.nl.

Amsterdam, 7 mei 2017

1 Deel I: Beginselen van de Avg en de Baseline

Voor organisaties die met persoonsgegevens werken bieden de Avg en de Uitvoeringswet Avg de enige 'harde' maatstaf om concreet, effectief en controleerbaar privacybeleid te voeren, volgens de drie doelstellingen Afscherming, Corrigeerbaarheid en Transparantie (ACT)[7]. ACT beoogt expliciet de betrokkene te beschermen[8]. De Avg formuleert in artikel 5.1 met dezelfde bedoeling dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene "rechtmatig, behoorlijk en transparant" is[9]. Met enige lenigheid is deze trits gemakkelijk te verzoenen met het ACT-trio (meer hierover in §1.3.4).

1.1 Zelf persoonsgegevens verwerken of uitbesteden?

Nadat we hebben vastgesteld dat we persoonsgegevens moeten verwerken om een bepaald doel te bereiken, moeten we ook 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, maar een organisatie kan 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[10]. 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[11].
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. Er moet altijd een geldige grondslag zijn voor het verwerken van de persoonsgegevens: uiteraard geldt dat 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.

---

[7] Vergelijkbaar met de BIV-doelstellingen bij informatiebeveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid. De ACT-privacydoelstellingen zijn gebaseerd de Privacy Protection Goals van ENISA (Unlinkability, Transparency, Intervenability). In: Privacy and data protection by design. From policy to engineering. ENISA dec 2014. Directe link: hier.

[8] 'Betrokkene' is de aanduiding voor de persoon over wie een verwerkt persoonsgegeven informatie bevat, in het kader van de Avg is dat privacygevoelige informatie. Voor (overheids)organisaties zijn het vaak de 'burgers' of klanten die hiermee bedoeld zijn. Maar ook het eigen personeel kan 'betrokkene' zijn, bijvoorbeeld bij de informatie die de personeelsadministratie bevat.

[9] Deze beginselen worden geformuleerd en behandeld in Avg art. 5.1, Avg overweging 39 en par.4.2 van de Mvt bij Uitvoeringswet Avg (versie april 2017).

[10] Avg art. 28, lid 3 en verder.

[11] 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 niet mogelijk om afspraken middels een overeenkomst vast te leggen.

1.2 Verwerkersovereenkomst

Hoewel de term 'verwerkersovereenkomst' in de Nederlandstalige Avg niet letterlijk wordt gebruikt, bepaalt artikel 28 toch nauwkeurig dat er een "*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*" [12, 13].
Wij hanteren de term 'verwerkersovereenkomst' hierna in deze zin. Voor de overeenkomst tussen twee verwerkingsverantwoordelijken (bij doorgifte/overdracht van persoonsgegevens, gebruiken we in dit document de term 'samenwerkingsovereenkomst', om het verschil tussen de overeenkomst tussen de verantwoordelijke en de verwerker en de overeenkomst tussen verantwoordelijke en verantwoordelijke te kunnen onderscheiden.

1.3 Werken met persoonsgegevens

Hoofdstuk II van de Avg beschrijft de beginselen van de verwerking van persoonsgegevens[14]. Wij beperken ons hier tot de beschrijving van wat verstaan wordt onder 'verwerken', 'persoonsgegevens' en 'bijzondere categorieën van persoonsgegevens. Daarna gaan we in op de ACT-doelen, benoemen we risico's en lichten we kort het format toe waarin de criteria in het volgende hoofdstuk worden beschreven.

1.3.1 Verwerking van persoonsgegevens

Verwerken is een breed begrip. Verwerken omvat alles wat je kunt doen met persoonsgegevens van verzameling tot vernietiging. De informatie tot je nemen is reeds 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"[15].

1.3.2 Verwerkingsverantwoordelijke en verwerker

In paragraaf 1.1 hebben we het al gehad over de verwerkingsverantwoordelijke en de verwerker. Voor de volledigheid volgen hier nog de volledige definities:

- 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.

[12] Avg art. 28, lid 3 en verder.
[13] In deel II komt dit nog nader ter sprake, bij B.02 Organieke inbedding, en vooral: U.07 Doorgifte persoonsgegevens.
[14] Avg art. 5 - 11.
[15] Avg art. 4 "Definities".

Het kan geen kwaad ook te wijzen op de *verantwoordingsplicht* van de verwerkingsverantwoordelijke. Avg artikel 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')".

1.3.3 Persoonsgegevens en bijzondere 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 ermee 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 van persoonsgegevens
De Avg spreekt van 'bijzondere categorieën van persoonsgegevens' [16]. 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[17]. Deze voorwaarden kennen significante verschillen ten opzichte van de voorwaarden voor de verwerking van persoonsgegevens in het algemeen[18]. Het criterium U.01 Doelbinding gegevensverwerking (§2.2.1) gaat hier uitgebreid op in.

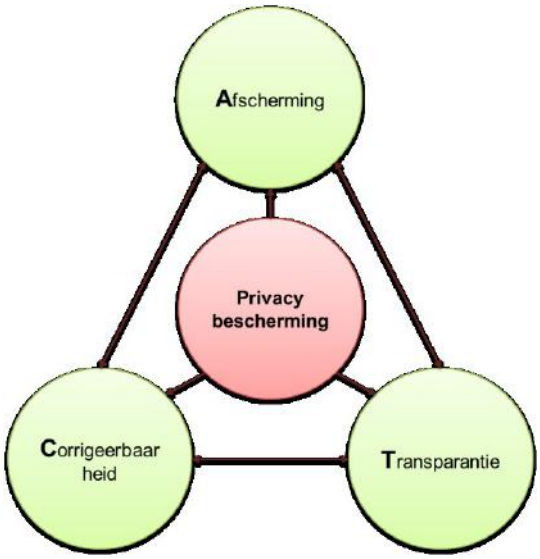
[16] Avg art. 9.
[17] Merk op dat dit vertrekpunt in algemene zin voor de verwerking van persoonsgegevens geldt.
[18] Avg art. 9.

In de overwegingen van de Avg komen we nog de term 'gevoelige gegevens' tegen; deze 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[19].

Strafrechtelijke gegevens en het BSN
Strafrechtelijke gegevens worden in de Avg niet als bijzondere persoonsgegevens aangemerkt. In artikel 10 Avg 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 Uitvoeringswet Avg worden wel aanvullende voorwaarden gesteld aan het gebruik van een dergelijk nummer, in Nederland het BSN (zie verder onder U.01 Doelbinding gegevensverwerking, §2.2.1). Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald[20].

1.3.4 De ACT doelen van privacybescherming

Er zijn verschillende soorten privacy te onderscheiden. Het recht op bescherming van persoonsgegevens wordt informationele privacy genoemd, we hebben het er in de inleiding reeds over gehad. Het beschermen van de informationele privacy kan worden uitgedrukt in ACT doelen: Afscherming, Corrigeerbaarheid en Transparantie.



In artikel 5 Avg wordt overigens geschreven over: *rechtmatig, behoorlijk en transparant*. Vergeleken bij ACT is dat meer te beschouwen als een "juridische doelstelling". ACT daarentegen is meer een "functionele doelstelling", overigens ook handig 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. 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: ten aanzien van 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: ten aanzien van elke verwerking van persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, de categorieën van 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.

[19] Avg overweging 10, 51 en 91.
[20] Uitvoeringswet Avg art. 44.

Deze doelen zijn gebaseerd op de privacywetgeving en geven daarnaast invulling aan de actuele privacyprincipes, zoals beschreven door de Organisation for Economic Cooperation and Development (OECD)[21]. In de onderstaande 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, zoals de term aangeeft, ondersteunend voor de leidende criteria en daarmee randvoorwaardelijk voor een effectieve invulling van de leidende criteria.

Afscherming		
Privacyprincipe 1. ***Doelbinding***		
Persoonsgegevens worden alleen verzameld en verwerkt voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en worden niet verder verwerkt voor andere doelen die hiermee onverenigbaar zijn.		
Criteria Privacy Baseline	***Leidende criteria***	***Ondersteunende criteria***
	U.01 Doelbinding gegevensverwerking (§2.2.1) U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens (§2.2.5)	B.01 (§2.1.1) U.02 (§2.2.2)
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 (§2.2.1)	U.02 (§2.2.2) B.03 (§2.1.3)
Privacyprincipe 3. ***Bewaren***		
Persoonsgegevens 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.		
Criteria Privacy Baseline	***Leidende criteria***	***Ondersteunende criteria***
	U.06 Bewaren van persoonsgegevens (§2.2.6)	U.02 (§2.2.2)
Privacyprincipe 4. ***Beveiliging***		
Passende technische en organisatorische maatregelen, zoals pseudonimisering van persoonsgegevens, zijn op een dusdanige manier genomen 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 (§2.2.4)	B.03 (§2.1.3) C.03 (§2.3.3)
Privacyprincipe 5. ***Doorgifte naar derden***		
Persoonsgegevens worden slechts doorgegeven wanneer er formeel afdoende garanties zijn vastgelegd, zodat aangetoond kan worden dat ook bij de doorgifte aan de Avg wordt voldaan.		
Criteria Privacy Baseline	***Leidende criteria***	***Ondersteunende criteria***
	U.07 Doorgifte persoonsgegevens (§2.2.7)	B.02 (§2.1.2) U.02 (§)

[21] http://oecdprivacy.org/

Corrigeerbaarheid		
Privacyprincipe 6. ***Kwaliteit***		
De persoonsgegevens en de verwerking ervan voldoet 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 (§2.2.3)	C.02 (§2.3.2)

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 (GEB's) en het gebruik van standaardinstellingen..		
Criteria Privacy Baseline	***Leidende criteria***	***Ondersteunende criteria***
	B.03 Risicomanagement, Privacy by Design en de GEB (§2.1.3) C.01 Intern toezicht (§2.3.1)	B.02 (§2.1.2) U.02 (§2.2.2)
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 vrijheden van natuurlijke personen.		
Criteria Privacy Baseline	***Leidende criteria***	***Ondersteunende criteria***
	B.01 Privacybeleid (§2.1.1) C.02 Toegang gegevensverwerking voor betrokkenen (§2.3.2) C.03 Meldplicht Datalekken (§2.3.3)	B.02 (§2.1.2) U.02 (§2.2.2) U.05 (§2.2.5)

1.4 Risico's bij niet voldoen aan de Avg

Algemene risico's
Hoewel we vanaf deze plaats geen volledige garantie kunnen geven dat je voldoet aan de Avg als je voldoet aan de Baseline, kan toch met grote mate van zekerheid worden gesteld dat voldoen aan de Baseline betekent dat een organisatie de beginselen van de Avg voldoende naleeft.
Niet naleving van de Avg kan verregaande (negatieve) consequenties hebben.

Voorbeelden van risico's voor de betrokkene:

- De mogelijkheid om anoniem gebruik te make van bepaalde diensten wordt gefrustreerd.
- Persoonsgegevens worden gedeeld en gebruikt op onrechtmatige wijze.
- 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.
- Kwetsbare groepen personen worden eerder het slachtoffer van oneigenlijk gebruik van hun persoonsgegevens en kunnen hierdoor gevolgen van ondervinden als uitsluiting, discriminatie of stigmatisering.
- persoonsgegevens worden niet of onjuist gemanaged waardoor er een wildgroei aan bestanden met persoonsgegevens ontstaat; hierdoor stijgen de veiligheidsrisico's.

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 privacy maatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business.
- Datalekken leiden tot wantrouwen.

Voorbeelden van juridische risico's:

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

Specifieke risico's
Voorts brengt elke eis die de privacywetgeving stelt een eigen risico met zich wanneer er niet aan voldaan wordt. 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.

1.5 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[22]. De eisen worden gestructureerd op basis van een template waarin de elementen wie, wat en waarom geadresseerd worden. In principe wordt er antwoord 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.					
...	...					

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 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 in de toelichtingen onder het kader nadere uitleg bij de maatregelen.

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

2 Deel II: De Privacybaseline

Hoofdstuk 2 is verdeeld in de volgende drie delen:

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

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

2.1 Het beleidsdomein

Inleiding
In dit hoofdstuk zijn richtlijnen opgenomen voor 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 zorgdragen dat op strategisch niveau afdoende randvoorwaarden en condities bestaan om persoonsgegevens verantwoord te verwerken, opdat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.

Risico's
Het ontbreken van een door het management uitgevaardigd beleid geeft het risico dat onvoldoende sturing wordt gegeven aan de verwerking van persoonsgegevens. Dit zal een negatieve impact hebben op de realisatie 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. Het privacybeleid heeft twee aspecten:

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, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Het volstaat dus niet om eenmalig het beleid op te stellen en niet meer aan te passen. Maar ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde missie of visie kunnen bepalend zijn om te komen tot aanpassing van het beleid. Door het beleidsproces cyclisch in te richten wordt bereikt dat het beleid op de ontwikkelingen en de uitvoering is afgestemd.

Proces
De ontwikkeling van de organisatie tot een organisatie die aantoonbaar aan de wet- en regelgeving voldoet (ofwel: 'compliant' aan de wet- en regelgeving is), vraagt om een cyclisch proces. Er is dan sprake 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 hoe dit cyclische proces vormgegeven wordt maakt daarmee onderdeel uit van het beleid.

B.01 Privacybeleid				
Criterium	De organisatie heeft privacybeleid en procedures ontwikkeld, waarin is vastgelegd en vastgesteld op welke wijze persoonsgegevens worden verwerkt en invulling wordt geven aan de wettelijke beginselen[23].			
Doelstelling	Het doel van het privacybeleid is om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de gegevensverwerking op een rechtmatige wijze plaatsvindt.			
Risico	Het ontbreken van een privacybeleid leidt ertoe dat de organisatie geen duidelijkheid heeft wat er exact wordt verwacht, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden verwerkt (waaronder verzamelen, bewerken, inzien et cetera).			
Referentie	Avg	Uitvoeringswet Avg		
	Art. 5, 24, 40	Art. 2, 4, 78 en 157		
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")[24].			
/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 rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens in overeenstemming met de wet.			
/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 die de uitvoering van de Avg nader concretiseert voor de eigen organisatie of branche en met welke frequentie de gedragscode en de naleving ervan wordt gecontroleerd en geëvalueerd door de verantwoordelijke en - indien aangesteld - de Functionaris voor de Gegevensbescherming (FG)[25].			
/02 Invulling geven aan de wettelijke beginselen				
/02.01	Beschreven is hoe gewaarborgd wordt hoe vooraf, door het conform B.03 (§2.1.3) toepassen van Privacy by Design, het uitvoeren van GEB's en het gebruik van standaardinstellingen, verantwoordelijken aantoonbaar maatregelen hebben genomen.			

[23] Avg art. 5, lid 1.
[24] Avg art. 5 lid 2.
[25] Avg art. 25 en 64 lid 2.

B.01 Privacybeleid	
/02.02	Beschreven is hoe gewaarborgd wordt dat persoonsgegevens , conform U.01 (§2.2.1), voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt.
/02.03	Beschreven is hoe gewaarborgd wordt dat, conform U.01 (§2.2.1), de verwerking toereikend is, ter zake dienend en beperkt 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 (§2.2.3), de persoons-gegevens 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.
/02.05	Beschreven is hoe gewaarborgd wordt dat, conform U.04 (§2.2.4), passende technische en organisatorische maatregelen, zoals pseudonimisering van persoonsgegevens, op een dusdanige manier worden genomen dat een passende beveiliging van de verwerking en de persoonsgegevens gewaarborgd wordt, en dat zij onder meer beschermd worden tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
/02.06	Beschreven is hoe gewaarborgd wordt dat, conform U.05 (§2.2.5) en C.02 (§2.3.2), 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 (§2.2.6), persoonsgegevens niet langer worden bewaard dan waarvoor de persoonsgegevens worden verwerkt noodzakelijk is en in welke vorm de opslag moet plaatsvinden, zodat na deze periode de betrokkenen niet langer zijn te identificeren.
/02.08	Beschreven is hoe gewaarborgd wordt dat, conform U.07 (§2.3), persoonsgegevens slechts worden doorgegeven wanneer er formeel afdoende garanties zijn vastgelegd, zodat aangetoond kan worden dat ook bij de doorgifte aan de Avg wordt voldaan en wat in een verwerkersovereenkomsten en een samenwerkingsovereenkomsten moet worden vastgelegd.
/02.09	Beschreven is hoe gewaarborgd wordt hoe, conform C.01 (§2.3.1), verantwoor-delijken 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 (U.02, §2.2.2) en een dossier kan worden aangetoond.
/02.10	Beschreven is hoe gewaarborgd wordt dat, conform C.03 (§2.3.3), bij een inbreuk in verband met persoonsgegevens (datalek, 'personal data breach') de betrokkenen en de AP worden geïnformeerd als deze inbreuk waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Toelichting /01 Privacybeleid

/01.02 De ontwikkeling van het beleid komt cyclisch tot stand zodat het beleid kan worden bijge-stuurd 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 lacunes. 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 transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins 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 hun persoonsgegevens die worden verwerkt. 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 wanneer de persoonsgegevens worden verzameld. 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 maakt een analyse of zij de vanuit de van toepassing zijnde wet- en regelgeving vereiste passende maatregelen kunnen nemen.

/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, Wet BRP. Bij overlapping gaan de bijzondere regels van de sectorspecifieke voor op de algemene regels van de Avg. Als sectorspecifieke wetgeving niets heeft bepaald, dan gelden dus de algemene regels van de Avg.

/01.06 De organisatie kan ervoor kiezen om een Gedragscode[26] op te stellen. In deze Gedragscode worden de eisen van de Avg voor een specifieke branche of organisatie uitgewerkt tot concrete te nemen maatregelen om aan de Avg te voldoen. Deze Gedragscode moet voldoen aan eisen[27]. Deze eisen zijn nog afkomstig van voor de komst van de Avg[28]:

a. Elke bepaling heeft een toelichting waarom die is opgenomen;
b. Als de bepaling een uitwerking is van de wet, is aangegeven waarom de wet op die specifieke manier is vertaald;
c. De aanvrager van de gedragscode is voldoende representatief voor de betrokken sector en de betrokken sector is voldoende nauwkeurig omschreven in de Gedragscode;

[26] Avg art. 40.
[27] Bij het schrijven van deze versie van de Privacy Baseline waren nog geen andere eisen bekend ten aanzien van gedragscodes.
[28] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gedragscodes.

d. De Gedragscode is concreter dan de Avg;
e. De Gedragscode vormt een juiste uitwerking van de Avg, of: andere wettelijke bepalingen voor de verwerking van persoonsgegevens;
f. Als een bepaling uit de Gedragscode uit een gedeelte of een parafrasering van een wettelijke bepaling bestaat, dan is deze afwijking gemotiveerd;
g. De AP of (indien aangesteld) de Functionaris Gegevensbescherming kan verzocht worden om de gedragscode op juistheid te controleren.

/01.06 Als een Gedragscode voorziet in beslechting van geschillen over de naleving ervan, 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 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	Zorgdragen dat dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de Avg.			
Risico	Door het ontbreken van een goede, inzichtelijke taakverdeling en de daartoe benodigde middelen en rapporteringslijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de Avg, sectorspecifieke wetgeving en het privacybeleid niet effectief worden ingevuld.			
Referentie	Avg	Uitvoeringswet Avg		
	5, 37, 38, 39			
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 ten alle tijde duidelijk wie deze verantwoordelijke is.			
/01.02	De verwerkingsverantwoordelijke en de verwerker hebben (de beschikking over) een functionaris voor gegevensbescherming, indien: • **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; • **stelselmatige observatie op grote schaal vereist:** een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen, of:			

B.02 Organieke inbedding	
	• **bijzondere categorieën en strafrechtelijke veroordelingen en strafbare feiten:** de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens (U01/04 of Avg art. 9) en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (U01/05 of Avg art. 10). In de 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 functionaris voor gegevensbescherming aangewezen.
/01.03	Bij elke uitvoering van een gegevensverwerking door een verwerker, zijn de taken en afspraken om de rechtmatigheid van een gegevensverwerking te garanderen schriftelijk vastgesteld en vastgelegd in een overeenkomst.
/01.04	De taken, bevoegdheden en verantwoordelijkheden zijn duidelijk belegd in een TVB-matrix, 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 Rapporteringsmiddelen	
/03.01	De rapportage- en verantwoordingslijnen tussen de betrokken verantwoordelijken, verwerkers en – indien aangesteld – de Functionaris Gegevensbescherming zijn vastgesteld en vastgelegd.

Toelichting /01 Verdeling taken en verantwoordelijkheden

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

/01.02 Eisen FG:

a) **Bereikbaarheid**

Een concern kan één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is. (Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.)

b) **Voor één of meerdere organisaties**

De functionaris voor gegevensbescherming kan optreden voor dergelijke verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.

c) **Professionele kwaliteiten**

De functionaris voor gegevensbescherming 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 en zijn vermogen de volgende taken te vervullen:

- de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de Avg en andere wettelijke gegevensbeschermingsbepalingen;
- toezien op naleving van de Avg, van andere wettelijke gegevensbeschermings-bepalingen 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 advies verstrekken met betrekking tot de GEB en toezien op de uitvoering daarvan;
- met de AP samenwerken;
- optreden als contactpunt voor de AP inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging ten behoeve van de gegevensbeschermingseffectbeoordeling (GEB) (zie B.03, §2.1.3), en, waar passend, overleg plegen over enige andere aangelegenheid.
- De FG houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

d) **Rechtsbescherming**
De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

e) **Bekendmaking**
De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de AP.

/01.03 Elke aanstelling van een verwerker is vastgelegd in een schriftelijke overeenkomst, waarin de concrete afspraken zijn verankerd over hoe voldaan wordt aan de eisen van de Avg.

/01.03 Vanaf 1 januari 2016 moeten afspraken over de meldplicht datalekken in de verwerkersovereenkomst opgenomen zijn.

/01.04 De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming 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 wordt, voor het vervullen van deze taken en het in stand houden van zijn deskundigheid, toegang verschaft tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen.

c) **Het niet ontvangen van instructies**
De FG ontvangt geen instructies met betrekking tot de uitvoering van die taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming 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) **Vertrouwelijkheid**
De FG is met betrekking tot de uitvoering van zijn taken is, binnen de geldende wetgeving, gehouden tot geheimhouding of vertrouwelijkheid.

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

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 doelgroepgericht training van medewerkers op privacybestendig werken;
- de middelen voor de facilitering van de transparantie voor betrokkenen (zoals toegang);
- 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 voor een functionaris voor de gegevensbescherming.

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

Risicomanagement is een continu proces dat de privacyrisico's signaleert, beoordeelt en een passende behandeling daarvan bewaakt. Privacyrisicomanagement richt zich op het beheersen van privacyrisico's bij het verwerken, waaronder verzamelen, opslaan en doorgeven van persoons-gegevens. Door middel van privacy-risicomanagement worden bij de ontwikkeling, inrichting en de inzet van de gegevensverwerking en de organisatie de privacyrisico's in lijn gebracht met het privacybeleid (zie: B01, §2.1.1). Zo wordt voldaan aan de wet- en regelgeving, waarbij de belangen van de betrokkenen gewaarborgd worden.

B.03 Risicomanagement, Privacy by Design en de GEB				
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 de maatregelen.			
Doelstelling	Bepalen wat de privacyrisico's (de kans en hun potentiele omvang/impact) zijn en hoe deze, door het treffen van de benodigde maatregelen, teruggebracht worden voor binnen de voor de organisatie acceptabele grenzen.			
Risico	Privacyrisico's worden niet of niet tijdig gesignaleerd, waardoor de verwerking van de persoonsgegevens niet aan de Avg voldoet en onderhevig is aan een hoge kans op inbreuken op de beveiliging. Dit beide kan leiden tot schade voor natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.			
Referentie	Avg	Uitvoeringswet Avg		
	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 nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden) wordt voorafgaand aan de verwerking voor een verwerking een GEB uitgevoerd[29].			
/01.02	Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een GEB diens advies in.			
/01.03	Ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden, verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling (GEB) wordt uitgevoerd[30].			
/01.04	Wanneer uit een GEB blijkt dat de verwerking een hoog risico zou opleveren (indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken), raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de AP[31].			
/02 Passende maatregelen				
/02.01	De maatregelen bestaan uit technische en organisatorische maatregelen.			
/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)[32].			
/02.03	De maatregelen zijn blijvend passend door het uitvoeren van gegevensbeschermings-effectbeoordelingen (GEB's).			
/02.04	De resultaten van de GEB worden gebruikt om de organisatie (beter) bewust te maken van het van belang om aan privacy te doen.			
/03 Aantonen				

[29] Avg art. 35 lid 1.
[30] Avg art. 35 lid 11.
[31] Avg art. 36.
[32] Avg art. 25.

B.03 Risicomanagement, Privacy by Design en de GEB	
/03.01	Van alle verwerkingen waarop een GEB is uitgevoerd en is een GEB rapportage beschikbaar, waardoor bekend welke risico's bestaan en welke maatregelen genomen (moeten) worden.
/03.02	Er is een procesbeschrijving voor het uitvoeren van GEB's en het opvolgen van de uitkomsten.
/03.03	De risicomanagementaanpak wordt aantoonbaar toegepast, doordat bijvoorbeeld in de vorm van een plan van aanpak aantoonbaar opvolging wordt gegeven aan de aanbevelingen/verbetervoorstellen uit de GEB's.
/03.04	Een tot standaard verheven GEB toetsmodel wordt toegepast en voldoet aan de gestelde eisen vanuit de Avg.
/03.05	Privacy by Design en de GEB en maken onderdeel uit tot een tot standaard verheven risicomanagementaanpak.

Toelichting /01 Het beoordelen van de privacyrisico's

/01 Een GEB wordt in een zo vroeg mogelijk stadium uitgevoerd; in ieder geval voordat over wordt gegaan tot de verwerking van persoonsgegevens. Zo kunnen gegevensbeschermings-maatregelen vooraf in het ontwerp worden meegenomen en wordt voorkomen dat achteraf geconstateerd wordt dat de gegevensverwerking niet voldoet aan de verplichtingen die volgen uit de Avg inzake het treffen van passende technische en organisatorische maat-regelen om onrechtmatige gegevensverwerkingen te voorkomen. Op deze manier kunnen ook kosten bespaard worden: zo is bijvoorbeeld het tijdig inregelen van beveiligingsmaat-regelen bij de ontwikkeling van een ICT-systeem waarin persoonsgegevens worden verwerkt 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 GEB bevat ten minste:

a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
c) een beoordeling van de hierboven genoemde risico's, en:
d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veilig-heidsmaatregelen 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 GEB in verband met een hoog risico is met name vereist in de volgende gevallen c.q. bij de volgende risico's[33]:

a) 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

[33] Avg art. 35, lid 3.

rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens (U.01/04, §2.2.1, of Avg art. 9, lid 1), of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (U.04/05, §2.2.4) of Avg art. 10), of:
c) 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 zou kunnen 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 vrijheden van de betrokkenen inhouden, met name wanneer betrokkenen als gevolg van die verwerkingen hun rechten moeilijker kunnen uitoefenen.

/01.01 Een GEB dient ook te worden gemaakt 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 van persoonsgegevens, biometrische gegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

/01.01 Een GEB is tevens nodig voor de grootschalige bewaking van openbaar toegankelijke ruimten, met name wanneer optisch-elektronische apparatuur wordt gebruikt, of voor alle andere verwerkingen wanneer 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 dienst of een overeenkomst, of omdat deze verwerkingen systematisch op grote schaal worden uitgevoerd.

/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 GEB niet verplicht worden gesteld.

/01.04 Wanneer de verwerkingsverantwoordelijke de AP raadpleegt, verstrekt hij informatie over[34]:

a) indien van toepassing, de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijke, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerking binnen een concern;
b) de doeleinden en de middelen van de voorgenomen verwerking;
c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de Avg;
d) indien van toepassing, de contactgegevens van de functionaris voor gegevensbescherming;
e) de GEB, en:
f) alle andere informatie waar de AP om verzoekt.

[34] 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[35]:

- 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 ernst van de risico's met name waar de verwerking[36] kan leiden tot:

- discriminatie,
- identiteitsdiefstal of -fraude,
- financiële verliezen,
- reputatieschade,
- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens,
- ongeoorloofde ongedaanmaking 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. Uitzondering hierop[37] zijn verwerkingen uit hoofde van een wettelijke verplichting of voor de invulling van algemeen belang (zie U.01, §2.2.1).

/02.02 Privacy by design and by default betekent feitelijk[38] dat de verwerkingsverantwoordelijke van het begin af privacyoverwegingen betrekt bij het opstellen van nieuw beleid en het ontwerp van nieuwe verwerkingen van persoonsgegevens.

[35] Avg art. 24, lid 1.
[36] Avg overweging 75.
[37] Avg art. 35, lid 10.
[38] Paragraaf 5.2.1 Mvt van de Uitvoeringswet Avg.

/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 aan bijvoorbeeld aan:

- pseudonimisering (zie ook U.04, §2.2.4)
- 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, waar privacyrisico's het grootst zijn (risico = kans x impact), dan is dit ondersteunend aan de prioritering 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 de kans van optreden van een activiteit waarop het risico berust *in relatie* met de potentiele 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 Tbv het aantonen van het passend zijn van de maatregelen kan gebruik gemaakt worden[39] van goedgekeurde gedragscode.

/03.03 Het beschikken over passende maatregelen kan worden aangetoond door certificering van de verwerking[40].

[39] Avg art. 24, lid 3.

[40] Avg art. 42.

2.2 Het uitvoeringsdomein

Inleiding
In dit hoofdstuk zijn de eisen opgenomen voor uitvoering van de gegevensverwerking. Het beleid dat op de beleidslaag vanuit het hogere management niveau is ontwikkeld en bekrachtigd, is leidend voor de invulling van de specifieke aspecten van de gegevensverwerking.
Doelstelling
In het uitvoeringsdomein worden persoonsgegevens 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 welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. '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 bij voorbeeld 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.

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. bijzondere persoonsgegevens; d. de persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten; e. het nationaal identificerend nummer; f. de persoonsgegevens ten behoeve van wetenschappelijk of historisch onderzoek met een statistisch oogmerk en archivering in het algemeen belang.
Doelstelling	Waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden.

U.01 Doelbinding gegevensverwerking				
Risico	Het ongeoorloofd en onrechtmatig verzamelen en (verder) verwerken van persoonsgegevens.			
Referentie	Avg	Uitvoeringswet Avg		
	Art. 5, 6, 9, 10, 22, 23,	Art. 22, 23, 24,25, 26, 27, 28, 29, 30, 31,		
Indicatoren en maatregelen				
/01 Tijdig welbepaald en uitdrukkelijk omschreven				
/01.01	Het doel is welbepaald en uitdrukkelijk omschreven vóórdat de gegevensverwerking begint en wordt niet tijdens het verzamelproces of het verwerkingsproces vastgesteld of gewijzigd[41].			
/01.02	Van alle gegevens zijn de rechtmatige gronden en de doeleinden van de verzameling en verwerking welbepaald en uitdrukkelijk omschreven en gerechtvaardigd[42].			
/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 gegevens verenigbaar zijn met het oorspronkelijke doel[43].			
/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 zijn 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[44]: a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden; b) 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; c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; e) 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; f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde			

[41] Avg art. 5, lid 1 en overweging 50.
[42] Avg art. 5, lid 1b.
[43] Avg art. 6, lid 4.
[44] Avg art. 6 lid 1 Avg.

U.01 Doelbinding gegevensverwerking	
	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 punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken. g) De rechtsgrond voor de verwerking moet worden vastgesteld bij het recht dat op de verwerkingsverantwoordelijke van toepassing is[45].
/02.03	Persoonsgegevens moeten behoorlijk en transparant worden verwerkt ten opzichte van de betrokkene [46, 47]. Hiertoe: a) Dient de gegevensverwerking transparant te zijn (U.02, §2.2.2) en U.05 (§2.2.5). b) Dienen de gegevens juist te zijn, indien nodig te worden bijgewerkt (U.03. §2.2.3). c) Dienen de gegevens passend worden beveiligd (U.04, §2.2.4). d) Dienen de gegevens niet langer dan noodzakelijk te worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren is (U.06, §2.2.6).
/03 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 persoons-gegevens aanvankelijk zijn verzameld en de verwerkingsverantwoordelijke bij de beoordeling van de verenigbaarheid onder meer rekening houdt met[48]: 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 de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft; c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt[49] en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt[50]; d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering. of:

[45] Avg art. 6 lid 3.
[46] Avg art. 5.
[47] De Avg is niet van toepassing op de persoonsgegevens van overleden personen (Avg overweging 27).
[48] Avg art. 6 lid 4.
[49] Avg art. 9.
[50] Avg art. 10.

U.01 Doelbinding gegevensverwerking	
	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 een verdere verwerking voorneemt moet de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken (zie U.05, §2.2.5). Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt[51].
/04 Bijzondere persoonsgegevens	
/04.01	Er vindt geen verwerking van persoonsgegevens plaats waaruit ras of etnische afkomst blijkt, tenzij: • aan /04.09 is voldaan, of: • de verwerking geschiedt[52]: a) met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is; b) met het doel personen van een bepaalde etnische of culturele minderheids-groep 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 indien: 1. dit voor dat doel noodzakelijk is; 2. de gegevens slechts betrekking hebben op het geboorteland van de betrokkene, van diens ouders of grootouders, dan wel op andere, bij wet vastgestelde criteria, op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een minderheidsgroep als bedoeld in de aanhef van onderdeel b behoort, en: 3. de betrokkene daartegen geen schriftelijk bezwaar heeft gemaakt.
/04.02	Er vindt geen verwerking van persoonsgegevens plaats waaruit politieke opvattingen blijkt, tenzij: • aan /04.09 is voldaan, of: • 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[53].
/04.03	Er vindt geen verwerking van persoonsgegevens plaats waaruit religieuze of levensbeschouwelijke overtuigingen blijkt, tenzij: • aan /04.09 is voldaan, of: • de verwerking geschiedt door instellingen, voor zover dit noodzakelijk is met het

[51] Avg overweging 61.
[52] Uitvoeringswet Avg art. 22.
[53] Uitvoeringswet Avg art. 30.

U.01 Doelbinding gegevensverwerking	
	oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar heeft gemaakt[54]. Hierbij worden ook geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.
/04.04	Er vindt geen verwerking van persoonsgegevens plaats waaruit het lidmaatschap van een vakbond blijkt, tenzij aan /04.09 is voldaan
/04.05	Er vindt geen verwerking van persoonsgegevens plaats van genetische gegevens, tenzij: • aan /04.09 is voldaan, of tenzij[55]: • een zwaarwegend geneeskundig belang prevaleert, of: • de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek of statistiek en de betrokkene uitdrukkelijke toestemming heeft gegeven.
/04.06	Er vindt geen verwerking van persoonsgegevens plaats Van biometrische gegevens met het oog op de unieke identificatie van een persoon, tenzij: • aan /04.09 is voldaan, of: • de verwerking geschiedt met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel noodzakelijk en proportioneel is voor behartiging van de gerechtvaardigde belangen van de verwerkingsverant-woordelijke of een derde [56] [57].
/04.07	Er vindt geen verwerking van persoonsgegevens plaats van gegevens over gezondheid, tenzij: • aan /04.09 is voldaan, of: • dit noodzakelijk is met het oog op redenen van 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. In die situatie 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 gegevens persoonlijk 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 krachtens het eerste lid bevoegd zijn tot verwerking daarvan.
/04.08	Er vindt geen verwerking van persoonsgegevens plaats met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, tenzij aan /04.09 is voldaan.

[54] Uitvoeringswet Avg art. 29.
[55] Uitvoeringswet Avg art. 24.
[56] Uitvoeringswet Avg art. 26.
[57] De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

U.01 Doelbinding gegevensverwerking	
/04.09	Indien wel de in /04.01 - /04.08 genoemde verwerkingen plaats vindt is aan één van de onderstaande voorwaarden voldaan[58]: a. Betrokkene toestemming heeft gegeven; b. Verwerking noodzakelijk is voor de uitvoering van verplichtingen en uitoefening van specifieke rechten op het gebied van het arbeidsrecht en socialezekerheidsrecht en sociale beschermingsrecht (zie ook /04.10); c. Verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene; d. De verwerking wordt verwerkt door een rechtspersoon zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is; e. De gegevens openbaar zijn gemaakt; f. De verwerking noodzakelijk is voor de instelling, uitoefening of verdediging van een rechtsvordering; g. De verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Uniewetgeving of nationale wetgeving, mits 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 (zie ook /04.10); h. De verwerking noodzakelijk is voor doelen van preventieve of arbeidsgeneeskunde, voor beoordeling van arbeidsgeschiktheid, medische diagnosen, verstrekken van gezondheidszorg of sociale diensten, op grond van Uniewetgeving of nationale wetgeving en onder de voorwaarden van het vierde lid (zie ook /04.10); i. de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid op grond van Uniewetgeving of nationale wetgeving waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim, of: j. de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doelen[59], op grond van Uniewetgeving of nationale wetgeving, waarbij 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 belangen van de betrokkene.
/04.10	De voorwaarden b, g en h van /04.09 zijn niet van toepassing indien de verwerking geschiedt door[60]: a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is;

[58] De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.
[59] Avg art. 83, lid 1.
[60] Uitvoeringswet Avg art. 23.

U.01 Doelbinding gegevensverwerking	
	b. verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht en financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover dat noodzakelijk is voor: 1. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt, of: 2. de uitvoering van de overeenkomst van verzekering; c. scholen voor zover dat met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is; d. een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming of de gecertificeerde instelling, bedoeld in artikel 1.1 van de Jeugdwet en de rechtspersoon, bedoeld in artikel 256, eerste lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover dat noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken; e. Onze Minister voor zover dat in verband met de tenuitvoerlegging van vrijheidsstraffen of vrijheidsbenemende maatregelen noodzakelijk is; f. bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn voor zover dat noodzakelijk is voor: 1. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene, of: 2. de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.
/04.11	Het verbod om bijzondere persoonsgegevens te verwerken, is vanuit het algemeen belang (punt g) niet van toepassing indien[61]: a. dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; b. de gegevens worden verwerkt door de Autoriteit of een ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht en dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, voor de uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad, of: c. dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en de Autoriteit ontheffing heeft verleend. De Autoriteit kan bij de verlening van ontheffing beperkingen en voorschriften opleggen. Hierbij wordt de evenredigheid met het nagestreefde doel gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens geëerbiedigd, en worden passende en specifieke maatregelen getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

[61] Uitvoeringswet Avg art. 28.

U.01 Doelbinding gegevensverwerking	
/05 Strafrechtelijke veroordelingen en strafbare feiten	
/05.01	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 alleen worden verwerkt[62]: a. indien 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 of de Wet justitiële en strafvorderlijke gegevens. b. indien de verwerkingsverantwoordelijke deze gegevens ten eigen behoeve verwerkt ter: 1. beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren, of: 2. 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. c. indien deze ten behoeve van derden worden verwerkt: 1. door verwerkingsverantwoordelijken die optreden krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus; 2. door een verwerkingsverantwoordelijke die tevens rechtspersoon is en in dezelfde groep is verbonden als bedoeld in artikel 2:24b van het Burgerlijk Wetboek, of: 3. door een verwerkingsverantwoordelijke die hiervoor toestemming heeft verkregen van de Autoriteit.
/05.02	De verwerking vindt alleen plaats onder toezicht van de overheid of indien de verwerking is toegestaan bij wet- en regelgeving die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid[63].
/05.03	De verwerking van de gegevens over personeel in dienst van de verwerkingsverantwoordelijke, vindt plaats overeenkomstig regels die zijn vastgesteld in overeenstemming met de procedure als bedoeld in de Wet op de ondernemingsraden[64].
/05.04	Het verbod om persoonsgegevens te verwerken, is niet van toepassing voor zover dit noodzakelijk is in aanvulling op de verwerking van strafrechtelijke gegevens voor de doeleinden waarvoor deze gegevens worden verwerkt[65].
/05.05	De verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en

[62] Uitvoeringswet Avg art. 31.
[63] Avg art. 10.
[64] Uitvoeringswet Avg art. 31 lid 2.
[65] Uitvoeringswet Avg art. 31 lid 3.

U.01 Doelbinding gegevensverwerking	
	strafbare feiten of daarmee verband houdende veiligheidsmaatregelen is toegestaan indien dit geschied 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[66].
/06 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 bepaald[67]: a. Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer (BSN), zonder dat daarvoor nadere regelgeving vereist is. b. Het burgerservicenummer (BSN) als uniek persoonsnummer voldoet aan artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb). c. Voor instellingen die geen beroep kunnen doen op artikel 10 Wabb 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 er andere identificerende nummers in gebruik, bijvoorbeeld het onderwijsnummer, dat overeenkomt met het burgerservicenummer, tenzij de deelnemer geen burgerservicenummer heeft.
/07 Geautomatiseerde besluitvorming	
/07.01	Een betrokkene wordt niet onderworpen aan een geautomatiseerde individuele besluitvorming, tenzij het besluit: 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.
/07.03	In de bij punten a) en c) in /07.01 bedoelde gevallen 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 menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.
/07.03	Bij de bij punten a) en c) in /07.01 bedoelde besluiten zijn niet gebaseerd op de

[66] Uitvoeringswet Avg art. 31 lid 4.
[67] Uitvoeringswet Avg art. 44.

U.01 Doelbinding gegevensverwerking	
	bijzondere categorieën van persoonsgegevens, tenzij /04.01 punt a) of g), van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen.
/08 Wetenschappelijk of historisch onderzoek of met een statistisch oogmerk en archivering in het algemeen belang	
/08.01	De verwerking van (bijzondere) persoonsgegevens ten behoeve van wetenschappelijk onderzoek of statistiek en archivering in het algemeen belang vindt plaats zover[68, 69]: a. het onderzoek een algemeen belang dient, b. de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is, c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost, en: d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.
/08.02	Verwerking van persoonsgegevens ten behoeve van wetenschappelijk onderzoek of archivering vindt alleen plaats, indien passende technische en organisatorische maatregelen zijn getroffen om de rechten en vrijheden van de betrokkene te beschermen: • het waarborgen van de doelbinding[70] (bijvoorbeeld door pseudonimisering) en: • de betrokkene niet meer kan worden geïdentificeerd[71].

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 ook voor meerdere doelen verzameld en verwerkt worden; die doelen hoeven niet per se verband te houden met elkaar[72]. Voor al deze doelen afzonderlijk geldt dat ze tijdig moeten worden vastgesteld, gerechtvaardigd zijn, welbepaald en uitdrukkelijk omschreven.

/01.04 Een voldoende SMART omschrijving houdt in[73]:

a. Specifiek: de doelstelling is eenduidig;
b. Meetbaar: er zijn meetbare/observeerbare voorwaarden waardoor het doel bereikt kan worden;
c. Acceptabel: het doel is acceptabel voor de doelgroep en/of management en iemand neemt zijn verantwoordelijkheid voor het juist realiseren van dit doel;
d. Realistisch: de doelstelling is haalbaar;
e. Tijdsgebonden: er is bepaald wanneer (in de tijd) het doel bereikt moet zijn.

[68] Invulling van art. 9 lid 2, deel j.
[69] Uitvoeringswet Avg art. 27.
[70] Avg art. 5 lid 1, onderdeel b.
[71] Avg art. 5 lid 1, onderdeel e.
[72] Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp, Ministerie van Justitie, 2002, p. 20.
[73] NOREA PIA, versie 1.1. juli 2015, p.23.

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[74] en daarmee aan de vereisten van /02 voldoen.

/02.02 Voor de private sector zijn doorgaans de onderdelen a, b, d en f een basis voor verwerking van persoonsgegevens. Ook onderdeel c kan een basis zijn voor verwerking van persoonsgegevens in de private sector, wanneer er sprake is van een wettelijke verplichting voor een private partij[75].

/02.02 Voor de overheid is met name verwerking op basis van een wettelijke verplichting (onderdeel c) en verwerking in het belang van uitvoering van een taak van algemeen belang (onderdeel e) relevant. Deze beide rechtsgrondslagen voor de overheid moeten[76] worden vastgesteld bij het wettelijke recht dat op de verwerkingsverantwoordelijke van toepassing is. 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 verandert het wettelijk kader, zoals dat gold onder de richtlijn en de Wbp, niet[77].

/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[78] 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[79].

/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 inzake beperking van grondrechten, waarbij de beperking van het privéleven[80] voorzienbaar moet zijn bij wet. Het begrip 'voorzienbaar bij wet' wordt hierbij opgevat als een materieel wetsbegrip, dat niet beperkt is tot wetten in

[74] Avg overweging 44.
[75] Avg overweging 46.
[76] Avg art. 6 lid 3.
[77] Avg overweging 46.
[78] Avg art. 6 lid 1 Avg.
[79] Avg overweging 46.
[80] Avg art. 8 lid 2.

formele zin[81]. In de kern gaat het er om dat het voor het individu kenbaar 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. Artikel 6, eerste lid, onder e van de Avg 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, doordat die betrekking heeft op het algemeen belang volgens punt e): "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:

- 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 die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX van de Avg.

Het Nederlands recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel[82].

/02.02 Gelet op de materiële overeenstemming tussen de Avg en de Wbp kan worden aangenomen dat de bestaande wet- en regelgeving waarmee invulling wordt gegeven aan de publieke taak voor wat betreft de rechtsgrondslagen voor verwerking van gegevens in de regel aan de Avg voldoet. Wel zal de formulering in wettelijke bepalingen in sectorale regelgeving, waar deze verwijst naar de Wbp, aangepast moeten worden[83].

/02.02 Bij onderdeel f is voor de overheid van belang dat dit onderdeel niet geldt voor overheidsinstanties in het kader van de uitoefening van hun taak.
Overheidsinstanties zullen in de uitoefening van hun taak geen gebruik kunnen maken van de grondslag 'gerechtvaardigd belang', maar zullen 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 overheidsinstantie 'typisch bedrijfsmatige handelingen' verricht waarbij persoonsgegevens worden verwerkt, zoals bijvoorbeeld de verwerking van persoonsgegevens die noodzakelijk is voor de beveiliging van overheidsgebouwen. Voor handelingen die buiten de uitoefening van de taak vallen, mag er

[81] Avg overweging 41.
[82] Avg art. 6.
[83] Uitvoeringswet Avg, Mvt paragraaf 4.2.2.

wel een grondslag worden aangenomen in het gerechtvaardigd belang van de organisatie. De overheid onderscheidt zich hierin niet wezenlijk van een private partij[84].

Toelichting /03 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 één 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[85]:

- 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 De verwerkingsverantwoordelijke mag gegevens verder verwerken voor een ander doel, mits dat dat andere doel niet onverenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld[86]. De verwerkingsverantwoordelijke dient zelf vast te stellen of het andere doel verenigbaar is met het oorspronkelijke doel.
Op grond van de Avg blijft ook verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden onverminderd mogelijk. Artikel 5, eerste lid, onder b van de Avg bepaalt namelijk dat verdere verwerking met het oog op voornoemde doeleinden niet als onverenigbaar met de oorspronkelijke doeleinden worden beschouwd. Voorwaarde voor de verdere verwerking is wel dat de verantwoordelijke voorziet in passende waarborgen voor de bescherming van de persoonsgegevens van de betrokkenen. Bij de mogelijke voorzieningen die de verantwoordelijke in dit kader kan treffen, kan bijvoorbeeld worden gedacht aan het pseudonimiseren van de desbetreffende persoonsgegevens.

/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

[84] Avg overweging 47.
[85] Avg overweging 50.
[86] Avg art. 5 lid 1b.

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[87]. De verwerkingsverantwoordelijke hoeft in geval van toestemming niet te toetsen aan het verenigbaarheidsvereiste.

/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. In Nederland heeft dit zijn weerslag gekregen in artikel 39 van de Uitvoeringswet Avg. De verdere verwerking hoeft ook in dat geval niet verenigbaar te zijn met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. De verwerkingsverantwoordelijke hoeft dan ook niet te toetsen aan het vereiste van verenigbaarheid[88]. De verdere verwerking door de verwerkingsverantwoordelijke is dan gebaseerd op de lidstaatrechtelijke bepaling (een specifieke wettelijke bepaling dus).
Zoals gezegd, dient verdere verwerking voor een niet-verenigbaar doel met terughoudendheid te worden toegepast. Een belangrijke beperking is dan ook dat de nationaalrechtelijke grondslag voor de verdere verwerking voor een niet- verenigbaar doel in een democratische samenleving een noodzakelijke en evenredige maatregel moet vormen ter waarborging van de doelstellingen, die in artikel 23, eerste lid, van de Avg zijn opgesomd. Het gaat daarbij om doelstellingen van algemeen belang, die hieronder nog nader aan de orde zullen komen. Het is allereerst aan de wetgever om te bepalen of deze belangen aan de orde zijn en zo ja of zij in het concrete geval een voldoende rechtvaardig vormen voor het toestaan van niet-verenigbaar gebruik.

/03.01 Indien de verdere verwerking wordt verricht op basis van mogelijkheid 3, doordat de verwerkingsverantwoordelijke hiertoe wettelijk is verplicht of indien 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, 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 die 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 specificaties kunnen vaststellen 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 of, indien zulks is gerechtvaardigd om redenen van algemeen belang, waaronder gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming en

[87] Avg art. 7 en 8.
[88] Avg art. 6, tweede deel lid 4.

het beheer van gezondheidszorgdiensten, een privaatrechtelijke persoon, zoals een beroepsvereniging, moet zijn[89].

/03.01 De verwerking van persoonsgegevens dient ook als rechtmatig te worden beschouwd indien 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 indien 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[90].

/03.01 De volgende specifieke uitzonderingsgronden zijn[91]:

a. de nationale veiligheid;
b. 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.

Toelichting /04 Bijzondere persoonsgegevens

/04.02 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 er passende waarborgen worden vastgesteld[92].

/04.03 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[93].

[89] Avg overweging 45.
[90] Avg overweging 46.
[91] Avg art. 23 Avg.
[92] Avg overweging 56.
[93] Avg overweging 55.

/04.05 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[94].

/04.06 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[95].

/04.06 Foto's worden niet systematisch beschouwd als verwerking van bijzondere categorieën van 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[96].

/04.07 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[97].

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 bijvoorbeeld een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitrodiagnostiek[98].

/04.07 Bijzondere categorieën van persoonsgegevens waarvoor betere bescherming is vereist, mogen alleen voor gezondheidsdoeleinden worden verwerkt indien dat nodig is om die doeleinden te verwezenlijken in het belang van natuurlijke personen en de samenleving als geheel, met name bij het beheer van gezondheidszorgdiensten en -stelsels of sociale diensten en stelsels van sociale diensten, met inbegrip van de verwerking door de beheersautoriteiten en de centrale nationale gezondheidsinstanties van die gegevens met het oog op kwaliteitscontrole, beheersinformatie en het algemeen nationaal en lokaal toezicht op het gezondheidszorgstelsel of het stelsel van sociale diensten, en bij het waarborgen van de continuïteit van de gezondheidszorg of de sociale diensten en

[94] Avg overweging 34.
[95] Avg art. 4, lid 14.
[96] Avg overweging 51.
[97] Avg art. 4 lid 15 Avg
[98] Avg overweging 35.

grensoverschrijdende gezondheidszorg of voor doeleinden inzake gezondheids-beveiliging, -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 dient de Avg te voorzien in geharmoniseerde voorwaarden voor de verwerking van bijzondere categorieën van 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. De lidstaten moet worden toegestaan andere voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid te handhaven of in te voeren. Wanneer deze voorwaarden van toepassing zijn op de grensoverschrijdende verwerking van deze persoonsgegevens, mag dit evenwel geen belemmering vormen voor het vrije verkeer van gegevens binnen de Unie[99].

/04.07 Het kan om redenen van algemeen belang op het gebied van de volksgezondheid nodig zijn om bijzondere categorieën van 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 gezondheids-toestand, de behoeften aan gezondheidszorg, middelen ten behoeve van de gezondheids-zorg, 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 te leiden dat persoonsgegevens door derden zoals werkgevers, of verzekeringsmaatschappijen en banken voor andere doeleinden worden verwerkt[100].

Toelichting /05 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 persoons-gegevens 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 rechts-handeling van de Unie. De Avg mag derhalve niet van toepassing zijn op de met die doeleinden verrichte verwerkingsactiviteiten. Overeenkomstig de Avg door overheids-

[99] Avg overweging 53.
[100] Avg overweging 54.

instanties 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[101].

/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[102].

Toelichting /06 Nationaal identificerend nummer

/06.01 Artikel 87 van de Avg geeft een grondslag om bij lidstatelijk recht specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer. Artikel 38 van de Uitvoeringswet Avg regelt het gebruik van wettelijk voorgeschreven nummers.
Artikel 44 van de Uitvoeringswet Avg regelt dat een nummer dat ter 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.
Voor de overheid is het gebruik van een uniek persoonsnummer, het burgerservicenummer (BSN) geregeld in artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb). 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 artikel 10 Wabb 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 er andere identificerende nummers in gebruik, bijvoorbeeld het onderwijsnummer, dat overeenkomt met het burgerservicenummer, tenzij de deelnemer geen burgerservicenummer heeft.
Noch in de bepaling zoals deze was opgenomen in de Wbp, noch in sectorspecifieke voorschriften worden veranderingen voorzien ten aanzien van het burgerservicenummer[103].

[101] Avg overweging 19.
[102] Avg overweging 50.
[103] Uitvoeringswet Avg, Mvt, paragraaf 4.10.

Toelichting /07 Geautomatiseerde individuele besluitvorming

/07 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.

/07 De negatieve kenmerken van een bepaalde groep mogen niet tegengeworpen worden aan een individu. Het individu hoeft deze kenmerken namelijk helemaal niet te hebben.

/07 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[104].

Toelichting /08 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[105]. Deze bepalingen werken rechtstreeks in de Nederlandse rechtsorde, en behoeven geen omzetting naar Nederlands recht.

/08 Voor de verwerking van bijzondere 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 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.
Indien de uitdrukkelijke toestemming van de betrokkene niet kan worden verkregen of een onevenredige inspanning kost, kan de verwerking alsnog plaatsvinden[106]. Ook is verwerking mogelijk als de verwerking moet een algemeen belang dienen, de verwerking moet noodzakelijk zijn voor het wetenschappelijk of historisch onderzoek of het statistisch doel en tot slot moet bij de uitvoering worden voorzien in waarborgen die verzekeren dat de

[104] Avg overweging 38.
[105] Avg art. 5 lid 1 b en e.
[106] Avg art. 27.

persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad[107]. Verder zal de verwerking vanzelfsprekend ook moeten voldoen aan de overige van toepassing zijnde voorwaarden die door de Avg en door deze wet zijn gesteld.

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[108].
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 of de verwerker hebben de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevens verwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.			
Doelstelling	Het verstrekken van inzicht 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 van persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.			
Referentie	Avg	Uitvoeringswet Avg		
	Art. 30			
/01 Register				
/01.01	Elke verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten 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[109]: 1) de naam en de contactgegevens van: a) de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, b) in voorkomend geval: i) van de vertegenwoordiger van de verwerkingsverantwoordelijke, en: ii) van de functionaris voor gegevensbescherming; 2) de verwerkingsdoeleinden; 3) een beschrijving van de categorieën van betrokkenen; 4) een beschrijving van de categorieën van persoonsgegevens;			

[107] Avg art. 27
[108] Avg overweging 82.
[109] Avg art. 30 lid 1.

U.02 Register van verwerkingsactiviteiten	
	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 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[110]: 1) de naam en de contactgegevens van: a) de verwerkers b) iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt. In voorkomend geval: i) de vertegenwoordiger van de verwerkingsverantwoordelijke of ii) de verwerker 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 elektronische vorm opgesteld.
/01.06	Het register hoeft niet te worden bijgehouden, indien: 1) De onderneming of organisaties minder dan 250 personen in dienst heeft, 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) er 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	Het registers van de verwerkingsverantwoordelijke en van de verwerker geven één samenhangend beeld.
/02.01	Op verzoek van de AP wordt middels de registers een actueel beeld gegeven.

[110] Avg art. 30 lid 1.

U.02 Register van verwerkingsactiviteiten	
/02.02	De onderlinge samenhang (gegevensstromen) en afhankelijkheden tussen: 1) de bedrijfsprocessen; 2) organisaties en organisatieonderdelen; 3) de verwerkingen; 4) de locaties waar persoonsgegevens opgeslagen; 5) de gegevensuitwisselingen (binnen en buiten de eigen organisatie); 6) de systemen zijn benoemd en beschreven.
/02.03	Bij wijzigingen in bestaande en nieuwe verwerkingen worden de resultaten vanuit de gegevensbeschermingseffectbeoordeling (GEB) 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 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, het dreigingsbeeld, veranderingen op organisatorisch vlak, veranderingen in de stand der techniek, of veranderingen van de verwerkingen, kunnen wijzigingen in de verwerking zelf, of de waarborgen voor de veilige verwerking. Het register dient te worden bijgehouden met de relevante informatie om inzicht te verschaffen 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 de verwerking, juistheid en nauwkeurigheid van de persoonsgegevens te bewaken en die, bij onjuistheid en onnauwkeurigheid van de gegevens of bij ongewenste verwerking, de gegevens te recitificeren, te vervolledigen, te wissen, de verwerking te beperken en toestemming tot verwerking in te trekken.

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 op verzoek van betrokkene gebeurd wordt deze over de status van de afhandeling geïnformeerd.			
Doelstelling	Het zorgdragen voor een gegevensverwerking die correct en in overeenstemming met de wens van betrokkenen is.			
Risico	Wanneer de gegevens onjuist en onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, worden verkeerde conclusies over de betrokkene getrokken met negatieve consequenties tot gevolg of naar het oordeel van betrokkene ongewenste verwerking van zijn of haar persoonsgegevens.			
Referentie	Avg	Uitvoeringswet Avg		
	Art. 7 lid 3, 11 lid 2, 12, 16, 17, 18, 19, 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 op de juiste werking van de getroffen maatregelen en brengt hierover rapportages uit aan hogere management.			
/02 Gecorrigeerd, gestaakt of overgedragen				
/02.01	Op verzoek van betrokkene worden onjuiste persoonsgegevens gerectificeerd[111].			
/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[112].			
/02.03	Op verzoek van de betrokkene worden de hem betreffende persoonsgegevens gewist wanneer een van de volgende gevallen van toepassing is[113]: 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 verwerkings-verantwoordelijke rust; f. de persoonsgegevens van kinderen jonger dan 16 jaar zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.			

[111] Avg art. 16, lid 1.
[112] Avg art. 16, lid 1.

U.03 Kwaliteitsmanagement	
/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[114].
/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[115].
/02.06	Op verzoek van betrokkene wordt de verwerking beperkt, indien: 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 is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan; c. de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of: d. de betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverant-woordelijke zwaarder wegen dan die van de betrokkene.

[113] Avg art. 17 lid 1.
[114] Avg art. 21 lid 1.
[115] Avg art. 17 lid 2.

U.03 Kwaliteitsmanagement	
/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[116], indien 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.
/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[117].
/03.02	De verwerkingsverantwoordelijke informeert op verzoek van de betrokkene aan wie hij de mededeling van correctie heeft gedaan[118].
/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.
/03.04	Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt[119].
/03.05	De verwerkingsverantwoordelijke reageert schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is[120].

[116] Avg art. 20.
[117] Avg art. 19.
[118] Avg art. 19.
[119] Avg art. 12 lid 3.
[120] Avg art. 12 lid 1.

U.03 Kwaliteitsmanagement	
/03.05	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 klacht in te dienen bij een AP en beroep bij de rechter in te stellen[121].
/03.06	Indien de verwerkingsverantwoordelijke kan aantonen dat hij de betrokkene niet kan identificeren, stelt hij de betrokkenen daarvan indien mogelijk in kennis. Betrokkene kan aanvullende gegevens verstrekken om identificatie mogelijk te maken[122].

Toelichting / 01 Juistheid en nauwkeurigheid

/01.01 De verwerkingsverantwoordelijke treft de nodige maatregelen om de juistheid en nauwkeurigheid van persoonsgegevens te borgen. 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 zorgdragen voor juistheid en nauwkeurigheid van de persoonsgegevens, is daarmee een inspannings-verplichting 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:

a. Het inregelen van de (technische) mogelijkheid om te kunnen corrigeren;
b. Er is vastgesteld en bekrachtigd 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;
c. Het identificeren en beperken van personen en afdelingen die toegang hebben tot de persoonsgegevens, waarbij tevens zekerheid wordt verkregen over de wijze waarop de juistheid van gegevens bij toegang is gewaarborgd en dat gegevens niet voor andere doeleinden worden gebruikt dan de vereiste doelstelling.
d. Het identificeren en beperken van partijen aan wie persoonsgegevens mogen worden verstrekt, waarbij tevens zekerheid word verkregen over de wijze waarop de juistheid van gegevens bij verstrekking is gewaarborgd en dat gegevens niet voor andere doeleinden worden gebruikt dan de vereiste doelstelling.
e. Het identificeren van de gevolgen van het onjuist gebruik van persoonsgegevens en of hoe deze gevolgen kunnen worden ondervangen.
f. Bij het aanstellen van een verwerker is:
   - aangetoond 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;
   - dfe geheimhoudingsplicht geborgd door deze vast te stellen en vast te leggen in de verwerkersovereenkomst.

Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:

[121] Avg art. 12 lid 4
[122] Avg art. 11 en 12; zie ook Avg overweging 57

a. 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:
b. 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[123].

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[124].

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

a. voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b. 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;
c. om redenen van algemeen belang op het gebied van volksgezondheid;
d. 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;
e. voor de instelling, uitoefening of onderbouwing van een rechtsvordering[125].

/02.03 Het recht op wissing is niet van toepassing als de verwerking nodig is:

a. voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b. voor het nakomen van een in een 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 verwerkingsverant-woordelijke is verleend;
c. om redenen van algemeen belang op het gebied van volksgezondheid;
d. met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig, voor zover het recht op wissing de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
e. voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

/02.06 Het recht de verwerking te beperken geldt, indien de verwerking (inclusief profilering) plaatsvindt voor[126]:

a. de vervulling van een taak van algemeen belang,

[123] Avg art. 12 lid 5.
[124] Avg art. 23, lid 1.
[125] Avg art. 17 lid 3.
[126] Avg art. 21 lid 1.

b. de vervulling van een taak van het openbaar gezag,
c. 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,
d. direct marketing, of:
e. wetenschappelijk of historisch onderzoek of statistische doeleinden, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Toelichting /03 Geïnformeerd

/03.06 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[127].

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 de Avg).

U.04 Beveiligen van de verwerking van persoonsgegevens				
Criterium	De verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen om een verwerking van persoonsgegevens op een passend niveau te beveiligen[128].			
Doelstelling	Persoonsgegevens 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	Uitvoeringswet Avg		
	Art. 32.	§ 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[129].			
/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.			

[127] Avg art. 12 lid 6 en overwegingen 58, 59.
[128] Avg art. 32.
[129] Avg art. 32 lid 3.

U.04 Beveiligen van de verwerking van persoonsgegevens	
/01.04	De maatregelen waarborgen een passend beveiligingsniveau en bevatten onder meer[130]: 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[131].
/02.03	Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurde certificering kan worden gebruikt om aan te tonen dat dat de maatregelen passend zijn.

Toelichting/01 Technische en organisatorische maatregelen

/01.01 Dergelijke maatregelen kunnen onder meer bestaan in het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens[132]. 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[133].

/01.01 Fysieke persoonsgegevens worden ook fysiek beschermd, denk hierbij aan bijvoorbeeld gebouw-zonering 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.

[130] Avg art. 32. Dit is 'het informatiebeveiligingsartikel'
[131] Avg art. 32 lid 2.
[132] Avg overweging 78.
[133] Het ontvangen van een back-up en de opslag van persoonsgegevens zijn 'verwerkingen' van persoonsgegevens.

/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 van 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 er 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:

a. Welke technische, organisatorische en fysieke beveiligingsmaatregelen genomen zijn;
b. Welk normenstelsel de organisatie volgt;
c. Op welke wijze de eventuele aanwijzingen (richtsnoeren, beleidsregels) van de AP over het beveiligen van persoonsgegevens ingeregeld zijn;
d. De wijze waarop geheimhouding van de medewerkers geregeld is;
e. Welke acties de verantwoordelijke verwerker neemt bij datalekken;
f. De wijze waarop de verwerker zich periodiek verantwoordt over de nakoming van afspraken;
g. Hoe controle op de naleving van de beveiligingsmaatregelen is ingeregeld;
h. Het geven van instructies en trainingen over de manier waarop persoonsgegevens beschermd worden;
i. Een calamiteitenplan;
j. 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;
k. De opname van de technische en organisatorische maatregelen in de verwerkersovereenkomst, met voortdurende controle op de uitvoering ervan en direct ingrijpen als er niet aan wordt voldaan;
l. De maatregelen worden periodiek getoetst en worden aangepast als ze niet meer voldoende bescherming bieden;
m. Toekenning en deling van de verantwoordelijkheden en bevoegdheden met de omgang van persoonsgegevens;
n. 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 privacybeschermingstechnieken 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[134], hierbij zijn de gegevens niet meer te herleiden tot de oorspronkelijke gegevens. Een vergelijkbare techniek is pseudonimisering.

[134] Borking, J., *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies*, Kluwer, Den Haag, 2010. CBP Richtsnoeren voor het beveiligen van persoonsgegevens 2013, p.13.

De Avg definieert pseudonimisering als[135]: "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er 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".

/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 in de Avg is niet bedoeld om andere gegevensbeschermingsmaatregelen uit te sluiten[136].

/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[137].
- De verwerkingsverantwoordelijke dient, met name met betrekking tot onlinediensten en online-identificatoren, alle redelijke maatregelen te nemen om de identiteit te controleren van een betrokkene die om inzage verzoekt[138].

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[139].

/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.[140]

/02.01 Er hoeft niet voor de zwaarste technische beveiliging gekozen te worden, *maar voor de meest adequate*. De NEN-ISO 27001/27002 en de afgeleide overheidsnormen (zoals de Baseline Informatiebeveiliging Rijksdienst (BIR) en de Baseline Informatiebeveiliging Gemeenten (BIG)) zijn momenteel de standaard voor 'adequate' beveiliging[141]. Of deze echt adequaat is, ligt ook weer aan de scope en de applicability bepaling. Van belang is te weten dat de BIR en de BIG de NEN-ISO normen *niet vervangen*, maar een praktische uitvoerings-handleiding vormen. Er moet altijd tegen de volledige NEN-ISO normen worden gecontroleerd.

/02.01 Om aan de hand van de risicoanalyse het passend beschermingsniveau vast te stellen wordt er voldaan aan de volgende kwaliteitseisen[142]:

---

[135] Avg art. 4 lid 5.
[136] Avg art. 4 lid 5.
[137] Avg overweging 39.
[138] Avg overweging 64.
[139] Avg overweging 83.
[140] Avg art. 28 lid 1.
[141] Zwenne, G.J. en Knol. PC., *Tekst en Commentaar Telecommunicatie- en Privacyrecht*, Kluwer, Deventer, 2013, p.726.
[142] Borking, J., *Privacyrecht is code*. *Over het gebruik van Privacy Enhancing Technologies*, Kluwer, Den Haag, 2010, p.117 en CBP, *Richtsnoeren voor het beveiligen van persoonsgegevens*, Den Haag, 2013, p.13.

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 moet in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
c. *Exclusiviteit (de vertrouwelijkheid 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 nemen en maatregelen toe te passen die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (zie B.03, §2.1.3).

/02.01 Als met geringe extra kosten meer beveiliging kan worden bewerkstelligd, dan moeten deze als 'passend' worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zouden 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. Er moet daarbij 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 gegevens. Sommige gegevens zijn naar hun aard vertrouwelijker (zoals bijzondere persoonsgegevens zoals ras, religie, seksuele voorkeur maar bijvoorbeeld biometrische gegevens en inloggegevens), andere gegevens worden vertrouwelijk als ze in een bepaalde context worden geplaatst (bijv. uithuisplaatsing v/e minderjarige, gegevens over de financiële situatie van een persoon). Een bijkomende vuistregel: hoe groter verzameling van persoonsgegevens van een specifieke betrokkene is, des te vertrouwelijker deze gegevens kunnen worden.

/02.02 Het niveau van de technische, organisatorische en fysieke maatregelen wordt periodiek geëvalueerd en indien nodig geactualiseerd, zodat het niveau passend blijft[143].

/02.02 Indien sprake is van bijzondere persoonsgegevens, uniek identificerende gegevens (zoals BSN-nummers, vingerafdrukken, biometrische gegevens) of gegevens over kwetsbare groepen, personen of gebruikersnamen, wachtwoorden en andere inloggegevens, dan vraagt dit om extra aandacht in de risicoanalyse/maatregelen[144].

[143] Een 'Information Security Management System (ISMS)' biedt een organisatie een procesbenadering voor het beheersen van de informatiebeveiliging. ISO/IEC 27001 is daarvoor de norm. Dat document 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 https://www.werkenmetnen7510.nl.

[144] De lidstaten kunnen de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer of enige andere identificator van algemene aard nader vaststellen (zie Avg art. 87).

2.2.5 U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens

Wie persoonsgegevens verstrekt aan een organisatie heeft het recht te weten waarvoor deze gegevens worden gebruikt, op welke wijze en door wie. De organisatie heeft hiertoe een informatie-plicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen wordt 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 toestemming kan geven voor de verwerking, tenzij er een uitzondering geldt[145].			
Doelstelling	Het garanderen van transparantie aan betrokkene over de gegevensverzameling en verwerking[146], zodat de betrokkene in staat wordt gesteld zijn rechten uit te kunnen oefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking[147].			
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	Uitvoeringswet Avg		
	Art. 13, 14 en 15	§ 4.2.1		
Indicatoren en maatregelen				
/01 Tijdig				
/01.01	De toestemming van de betrokkene wordt verkregen voorafgaand aan de verwerking[148], het doorgeven aan derden en het verder verwerken[149]. Dit geldt voor persoonsgegevens die via betrokkenen of anderen wordt of is 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[150].			
/02 Informatie				
/02.01	Het verzoek om toestemming bestaat in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden[151].			
/02.02	Wanneer persoonsgegevens bij de betrokkene worden verzameld, ontvangt de betrokkene de volgende informatie[152]: a. De identiteit en contactgegevens van de verantwoordelijke; b. In voorkomend geval, de contactgegevens van de functionaris gegevensbescherming c. de verwerkingsdoeleinden als ook de rechtsgrond van de gegevensverwerking; d. De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een			

[145] Avg art. 14.
[146] Avg art. 12 en overweging 60
[147] Avg overweging 60.
[148] Avg art. 6 lid 1.
[149] Avg art. 14 lid 3.
[150] Avg art. 14 lid 3.
[151] Avg art. 7 lid 2.
[152] Avg art. 13.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
	derde, indien de verwerking op deze rechtsgrond (art 6.1f) is gebaseerd; 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 er een adequaatheidsbesluit van de commissie bestaat, welke de passende waarborgen zijn en hoe deze kunnen worden ingezien. g. De periode dat ze worden opgeslagen, of de criteria ter bepaling van die termijn; h. Dat de betrokkene recht heeft op inzage, rectificatie of wissing, of beperking van de hem betreffende verwerking en het recht 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 (indien de verwerking is gebaseerd op de rechtsgrond toestemming); j. dat de betrokkene een klacht mag indienen bij een AP; k. of de verstrekking een wettelijke of contractuele verplichting is, danwel 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 er 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[153]: 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 gegevens-bescherming; c. de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking; d. de betrokken categorieën van persoonsgegevens; e. in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens; f. indien persoonsgegevens aan een ontvanger in een derde land of aan een internationale organisatie wordt doorgegeven wordt er informatie gegeven over hoe er een kopie van 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 verwerkingsverant-woordelijke of van een derde; i. dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om

[153] Avg art. 14.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	
	inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid; j. wanneer verwerking is gebaseerd is op toestemming van betrokkene, wordt gemeld dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan; k. dat de betrokkene het recht heeft 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 Toestemming	
/03.01	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[154].
/03.02	Bij aanbieden van een dienst aan een kind en het kind is jonger dan 16 jaar is de toestemming of machtiging tot toestemming verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt[155].
/04 Uitzondering	
/04.01	De verplichting tot het verstrekken van informatie geldt niet, indien: • de betrokkene reeds over de informatie beschikt; • het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen; • 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); • 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: • de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim, waaronder een statutaire geheimhoudingsplicht. • Wanneer de verwerking berust op een wettelijke bepaling, waarbij een specifieke uitzondering geldt. • Het betreft de verwerking van persoonsgegevens die deel uitmaken van archief-bescheiden die op grond van de Archiefwet niet voor vernietiging in aanmerking komen en zijn overgebracht naar een archiefbewaarplaats[156].

[154] Avg art. 14 lid 4.
[155] Avg art. 8.
[156] Zie Mvt Uitvoeringswet, toelichting bij artikel 41.

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[157].

/01.02 Bij informatieverkrijging van persoonsgegevens van een ander dan de betrokkene, kan bijvoorbeeld 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 er een vaste opvolging (keten) van actoren is.

/01.02 Doorgifte van persoonsgegevens tussen partijen in landen binnen de EU (en dus ook binnen Nederland) valt onder het algemene begrip van verwerken. De 'doorgever' van de gegevens (de verstrekker) blijft dus verantwoordelijk voor een goed gebruik door anderen van de persoonsgegevens. Voor doorgifte naar personen/organisaties in landen buiten de EU gelden andere/aanvullende eisen. Zie voor nadere informatie over doorgifte van persoonsgegevens: U07, §2.2.7.

/01.02 In de Avg is een plicht opgenomen voor de verstrekker (en dus niet alleen de ontvanger) om actief de betrokkene te informeren over de doorgifte van zijn/haar persoonsgegevens, vóórdat de doorgifte plaats vindt[158].

Toelichting /02 Informatie

/02.01 De informatie moet goed leesbaar en begrijpelijk is 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 Toestemming

/03.02 De verwerkingsverantwoordelijke doet, met inachtneming van de beschikbare technologie, redelijke inspanningen om daarbij te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend[159].

Toelichting /04 Uitzonderingen

/04.01 De verantwoordelijke moet kunnen aantonen dat de betrokkene reeds op de hoogte is, wil hij zich kunnen beroepen op deze uitzonderingsgrond.

/04.01 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[160].

/04.01 De volgende specifieke uitzonderingsgronden worden gesteld[161]:

[157] Avg art. 14 lid 4.

[158] Avg art. 14 lid 1, onderdeel e.

[159] Avg art. 8 lid 2.

[160] Mvt Wbp, Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr.3, pp.151, 152.

a. de nationale veiligheid;
b. 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.

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 ze niet meer herleidbaar zijn naar de betrokkenen[162].

U.06 Bewaren van persoonsgegevens				
Criterium	De organisatie hanteert voor persoonsgegevens een bewaartermijn die niet wordt overschreden door het treffen van de nodige maatregelen.			
Doelstelling	Borgen dat de 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	Uitvoeringswet Avg		
	Art. 5, lid 1, e	Art. 43		
Maatregelen/indicatoren				
/01 Bewaartermijn				
/01.01	Van alle persoonsgegevens is de bewaartermijn vastgesteld en bekrachtigd.			

[161] Avg art. 23.
[162] Avg overweging 27: "De Avg is niet van toepassing op de persoonsgegevens van overleden personen. De lidstaten kunnen regels vaststellen betreffende de verwerking van de persoonsgegevens van overleden personen."

U.06 Bewaren van persoonsgegevens	
/01.02	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[163].
/01.03	Indien in sectorspecifieke wetgeving een bewaartermijn is vastgelegd voor specifieke persoonsgegevens, dan geldt die bewaartermijn.
/01.04	Wanneer persoonsgegevens voor langere perioden worden opgeslagen worden zij louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden verwerkt[164] en er passende waarborgen zijn getroffen in overeenstemming met de Avg voor de rechten en vrijheden van de betrokkene ("opslagbeperking")[165].
/02 Nodige maatregelen	
/02.01	Als de bewaartermijnen verlopen, zijn de gegevens verwijderd, vernietigd of geanonimiseerd.
/02.02	De verantwoordelijke bepaald na elke verwerking van persoonsgegevens of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.

Toelichting /01 Bewaartermijn

/01.01 Soms vereist het bereiken van een doel juist dat persoonsgegeven bewaard blijven, bijv. iemands emailadres dient bewaard te blijven om te voorkomen dat diegene nog mailings krijgt.

/01.02 In sommige (sectorspecifieke) wetgeving is een bewaartermijn aangegeven voor bepaalde persoonsgegevens. Een voorbeeld hiervan is het bewaren van medische gegevens: in het Burgerlijk Wetboek is de termijn hiervoor vastgesteld op 15 jaar[166]. Denk ook aan gegevens over financiële transacties.

/01.04 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.

/01.04 De maatregelen kunnen pseudonimisering omvatten, zodat de oorspronkelijke doelstellingen van in het kader van het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden alsnog kunnen worden behaald.

Toelichting /02 Nodige maatregelen

/02.01 De verantwoordelijke moet zich na elke verwerking van persoonsgegevens afvragen of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.

/02.01 De wet formuleert het iets anders dan in dit criterium en zegt: *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*. 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.

[163] Avg art. 5 lid 1, e.
[164] Avg art. 5 lid 1, e.
[165] Avg art. 89 lid 1.
[166] Art. 7:454 lid 3 BW.

/02.01 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.

/02.02 Indien aan de persoonsgegevens gekoppelde gegevens van belang zijn om langer te bewaren dienen de persoonsgegevens zodanig te worden geanonimiseerd dat het daarna niet meer mogelijk is deze geanonimiseerde gegevens weer herleidbaar te maken[167].

/02.02 Indien de persoonsgegevens zijn vastgelegd op een 'read only' gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, maar waarvan gegevens wel kunnen worden gekopieerd, zoals bijvoorbeeld 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[168].

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[169] [170]. Indien sprake is van meerdere verwerkingsverantwoordelijken bepalen zij gezamenlijk de doelstellingen en middelen van de verwerking en zijn zij gezamenlijke verwerkingsverantwoordelijken[171].

Bij de doorgifte wordt onderscheid gemaakt tussen doorgifte binnen de EU, waar de Avg geldt, en doorgifte naar buiten de EU. Indien doorgifte naar buiten de EU plaatsvindt, 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 er geen uitzonderingsgrond En: • Geldt er een door de Europese Commissie genomen adequaatheidsbesluit, of: • Zijn er passende waarborgen[172], of: • Geldt er een afwijking voor een specifieke situatie.
Doelstelling	Het 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 er exact wordt verwacht bij het doorgeven van persoonsgegevens, waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig

[167] Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp, Ministerie van Justitie, 2002, p.126.
[168] Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp, Ministerie van Justitie, 2002, p.37.
[169] Avg art. 28, lid 1.
[170] Avg art. 28, lid 10: Indien een verwerker in strijd met de Avg handelt, wordt die verwerker als verwerkingsverantwoordelijke beschouwd.
[171] Avg art. 27, lid 1.
[172] Avg art. 44.

U.07 Doorgifte persoonsgegevens				
	verder worden verwerkt en er een gebrek aan het nemen van verantwoordelijkheid en controle is.			
Referentie	Avg	Uitvoeringswet Avg		
	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 zij aan hun Avg-verplichtingen voldoen, met name met betrekking tot[173]: 1) de uitoefening van de rechten van de betrokkene (C.02, §2.3.2), en: 2) het informeren van de betrokkenen te bij ontvangst (U05). b) De regeling met de respectieve verantwoordelijkheden aan de betrokkene beschikbaar gesteld[174].			
/02 Afdoende garanties				
/02.01	De verwerking door een verwerker is in een overeenkomst of andere rechtshandeling vastgelegd, met[175] daarin: • het onderwerp en de duur van de verwerking, • 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. • het soort persoonsgegevens, inclusief: - de classificatie van de persoonsgegevens. • de categorieën van betrokkenen, en: • de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.			
/02.02	In de overeenkomst of andere rechtshandeling met de verwerker is bepaald dat: 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 (U.04, §2.2.4), inclusief: • welke medewerkers van de verwerker toegang tot de persoonsgegevens nodig hebben; • welke procedure wordt gevolgd in geval van een datalek; • in welke landen de persoonsgegevens worden opgeslagen;			

[173] Avg art. 26, lid 1.
[174] Avg art. 26, lid 3.
[175] Avg art. 28, lid 2.

U.07 Doorgifte persoonsgegevens	
	d. de vereisten aan de verwerkers ook bij het in dienst nemen van een andere verwerker geldt; e. er 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 verleent om 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 (U.06, §2.2.6); 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, indien 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.
/03 Vertegenwoordiger	
/03.01	Indien 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, tenzij: 1. Er sprake is van een incidentele verwerking die geen grootschalige verwerking van bijzondere categorieën van 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 passende technische en organisatorische maatregelen bieden (zie B03, §2.1.3) door de verwerker.
/03.03	Een verwerker laat een verwerking pas door een andere verwerker uitvoeren als er voorafgaand een specifieke of algemene schriftelijke toestemming is van de verwerkingsverantwoordelijke[176].
/04 Uitzonderingsgrond	
/04.01	De verwerking is 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

[176] art. 28, lid 1.

U.07 Doorgifte persoonsgegevens	
	internationale overeenkomst, zoals een verdrag inzake wederzijdse rechtsbijstand, tussen het verzoekende derde landen en de EU of een lidstaat[177].
/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 van persoonsgegevens aan een derde land of een internationale organisatie.
/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[178].
/06 Passende waarborgen	
/06.01	Wanneer door de Europese commissie geen adequaatheidsbesluit is genomen, dan zijn er passende waarborgen geboden, doordat er[179]: a. een juridisch bindend en afdwingbaar instrument is tussen overheidsinstanties of -organen; b. door de AP goedgekeurd bindende bedrijfsvoorschriften zijn (zie /05.02) c. er standaardbepalingen zijn inzake gegevensbescherming die door de Europese Commissie bedoelde onderzoeksprocedure zijn vastgesteld[180]; d. er standaardbepalingen zijn inzake gegevensbescherming die door een AP zijn vastgesteld en die door de Europese Commissie bedoelde onderzoeksprocedure zijn goedgekeurd[181]; e. er een goedgekeurde gedragscode 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; f. er een goedgekeurd certificeringsmechanisme 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. zijn er door de AP passende waarborgen, waarbij met name: • er 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: • er bepalingen zijn opgenomen in administratieve regelingen tussen overheidsinstanties of -organen, waaronder afdwingbare en effectieve rechten van betrokkenen.

[177] Avg art. 48.
[178] Avg art. 45.
[179] Avg art. 46.
[180] Avg art. 93, lid 2.
[181] Avg art. 93, lid 2.

U.07 Doorgifte persoonsgegevens	
/06.02	Als er bindende bedrijfsvoorschriften (/05.01 punt b))worden gebruikt om passende waarborgen te bieden, dan: a) zijn die juridisch bindend voor, van toepassing zijn op en worden 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) waarbij zijn de hier beknopt weergegeven elementen zijn vastgelegd (zie voor de volledige weergave artikel 47 lid 1): 1. de structuur en de contactgegeven; 2. de gegevensdoorgiften of reeks van doorgiften; 3. het intern en extern juridisch bindende karakter; 4. de toepassing van de algemene beginselen inzake gegevensbescherming; 5. de rechten van betrokkenen; 6. de aanvaarding van aansprakelijkheid voor alle inbreuken; 7. de wijze waarop informatie wordt verschaft over de bindende bedrijfsvoorschriften; 8. 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, op opleiding en op de behandeling van klachten; 9. de klachtenprocedures; 10. de bestaande procedures om te controleren of de bindende bedrijfsvoorschriften zijn nageleefd; 11. de procedures om die veranderingen in de regels te melden, te registreren en aan de AP te melden; 12. de procedure voor samenwerking met de AP; 13. de procedures om eventuele wettelijke voorschriften aan de AP te melden, en: 14. de passende opleiding inzake gegevensbescherming voor personeel.
/06.03	Wanneer de verwerking niet had mogen plaatsvinden wordt door de verwerkings-verantwoordelijke de doorgifte beëindigd en de AP en de betrokkenen hierover geïnformeerd[182].
/07 Afwijking voor een specifieke situatie	
/07.01	De doorgifte mag ook plaatsvinden als[183]: 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 overheidsinstanties ten behoeve van een openbare bevoegdheid wordt verricht;

[182] Avg art. 49.
[183] Avg art. 49.

U.07 Doorgifte persoonsgegevens	
	b. de doorgifte is noodzakelijk 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 is noodzakelijk 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; d. de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang, dat is erkend bij de wet- en regelgeving; e. de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering; f. de doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; g. de doorgifte is verricht 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. als de doorgifte aan derde landen of internationale organisaties is gebaseerd op internationale overeenkomsten die door de lidstaten zijn gesloten vóór 24 mei 2016, die overeenkomsten in overeenstemming zijn met het vóór die datum toepasselijke Unierecht en nog niet is gewijzigd, vervangen of ingetrokken[184].

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[185].

/01.01 Voorbeelden van dergelijke 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 certificerings-mechanisme 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.

[184] Avg art. 96.
[185] Avg art. 26, lid 3.

Toelichting /03 Vertegenwoordiger

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

/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 doe 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:

a. het gebruik van gegevens binnen concernverband, indien onderdelen van een concern zich binnen en buiten de EU bevinden; bindende bedrijfsvoorschriften zijn dan van toepassing.
b. de verstrekking aan derden die zich buiten de EU bevinden;
c. het ter beschikking stellen van de gegevens aan derden buiten de EU
d. 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: landsdelen die vallen onder de Canadian Personal Information Protection and Electronic Documents Act bieden een passend beschermingsniveau. Maar let op: Onder meer Québec valt hier *niet* onder, waardoor de gegevens aan een organisatie in Québec *niet* mogen worden doorgegeven, tenzij sprake is van een van de andere gronden voor rechtmatige doorgifte naar landen buiten de EU.

/05.01 In de Verenigde Staten van Amerika hebben alleen organisaties (in de VS) die zich hebben geconformeerd aan het EU-US Privacy shield verdrag een passend beschermingsniveau. Zij moeten zich hebben ingeschreven bij de Federal Trade Commission in het EU-US Privacy Shield register én dit ook actief de nodige maatregelen te hebben getroffen[186].

/01.02 Tot de Europese Economische Ruimte behoren de landen van de EU en 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.

[186] De stand van zaken rondom het niet onomstreden Privacy Shield is ingewikkelder dan hier verwoord en bovendien in beweging. Let in dit verband bijvoorbeeld op de Artikel 29-werkgroep.

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 een adequate technische- en organisatorische maatregelen moeten zijn ingericht, om de beheerprocessen vorm te geven.

Doelstelling
De doelstelling van de laag algemene control (beheersing) is er voor te zorgen en/of vast te stellen dat maatregelen ter waarborging van de privacy afdoende zijn ingericht.

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 een 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 (wie, wat)	Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.			
Doelstelling	Het garanderen van een rechtmatige, behoorlijke en transparantie verwerking van persoonsgegevens en het kunnen aantonen daarvan, naleving van de Avg, van andere de wet- en regelgeving betreffende de gegevensbescherming en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens.			
Risico	Als de verwerking van persoonsgegevens niet voldaan aan de Avg, zijn de risico's tweeledig; de betrokkene loopt persoonlijke privacyrisico's en de verwerkings-verantwoordelijke wordt geconfronteerd wordt 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	Uitvoeringswet Avg		
	Art. 5			
Indicatoren en maatregelen				
/01 Evaluatie				
/01.01	De verantwoordelijke en - indien aangesteld - de functionaris gegevensbescherming controleert of de gegevensverwerkingen voldoen aan de wettelijke verplichtingen. Hiertoe worden periodiek compliancy assessments uitgevoerd en de resultaten geregistreerd.			
/01.02	Als blijkt dat er toch niet voldaan wordt aan de eisen van de Avg, dan rapporteert de verantwoordelijke over te nemen maatregelen om de privacyschending te beëindigen. De evaluatierapportages worden beschikbaar gesteld aan het management.			

C.01 Intern toezicht	
/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 (§2.2.1), 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 (§2.2.1), de verwerking toereikend is, ter zake dienend en beperkt is tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).
/02.03	Aangetoond is dat, conform U.01 (§2.2.1), de verwerking ten aanzien van de betrokkene rechtmatig is (rechtmatigheid).
/02.04	Bij het aantonen van de rechtmatigheid (/02.03) wordt gebruik gemaakt van de overeenkomsten voor de doorgiften (U.07, §2.2.7).
/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 (§2.2.3), 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 (juistheid).
/02.07	Aangetoond is dat, conform B.03 (§2.1.3), de wijze van verwerken ten aanzien van de betrokkene behoorlijk is (behoorlijkheid).
/02.08	Aangetoond is dat, conform U.05 en C.02 (resp. §2.2.5 en §2.3.2), de persoonsgegevens op een wijze worden verwerkt die voor de betrokkene transparant is (transparantie).
/02.09	De verwerkingsverantwoordelijke toont compliancy aan door middel van een dossier (al dan niet door een functionaris gegevensbescherming bijgehouden)[187].
/02.10	Bij het aantonen van het compliant en het compleet zijn van het dossier wordt gebruik gemaakt van het register (U.02, §2.2.2).

Toelichting /01 Evaluatie

/01.01 Als de verantwoordelijke op de hoogte is van een schending van de privacyverplichtingen en hij laat hij om de nodige maatregelen te treffen om deze schending te beëindigen, dan is hij hierop aanspreekbaar en moet daarom tijdig de nodige maatregelen treffen. De 'nodige maatregelen' bestaan uit corrigerende maatregelen die het mogelijk maken binnen een passende termijn de schending van de privacy te beëindigen.

/01.01 Als de functionaris gegevensbescherming 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 privacyverplichtingen.

[187] art. 5, lid 2.

Toelichting /02 Rechtmatigheid aangetoond

/02.09 De uitkomst van het compliancyproces kan ook worden gebruikt voor publicatie over de behaalde resultaten in 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 (U.05, §2.2.5) en zijn er binnen de verwerkingen voorzieningen getroffen waarmee de betrokkene controle over zijn gegevens kan houden (U.03, §2.2.3).

C.02 Toegang gegevensverwerking voor b				
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[188], tenzij er een specifieke uitzonderingsgrond geldt.			
Doelstelling	Het bieden van transparantie over de gegevensverwerking, zodat, indien nodig, 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	Uitvoeringswet Avg		
	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.			
/01.02	De inzage over de verwerkte persoonsgegevens bevat de volgende informatie[189]: a) de verwerkingsdoeleinden; b) de betrokken categorieën van 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 indien dat niet mogelijk is, de criteria om die termijn te bepalen; e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het			

[188] Avg art. 12.
[189] Avg art. 15.

C.02 Toegang gegevensverwerking voor b	
	recht tegen die verwerking bezwaar te maken; f) dat de betrokkene het recht heeft klacht in te dienen bij een 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[190].
/02 Tijdig	
/02.01	De informatie is onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek verstrekt[191], tenzij: • 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.
/02.02	Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, dan: • 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[192]. Hierbij kan gebruik gemaakt worden van gestandaardiseerde iconen om het overzicht te houden[193].
/03.02	De informatie is schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt.
/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.

[190] Avg art. 14 lid 4.
[191] Avg art. 12 lid 3 en 4.
[192] Avg art. 12 lid 1.
[193] Avg art. 12 lid 7.

C.02 Toegang gegevensverwerking voor b	
/03.04	Het verstrekken van de informatie en het verstrekken van de communicatie is kosteloos, tenzij de verzoeken van een betrokkene kennelijk ongegrond, of: buitensporig zijn, met name vanwege hun repetitieve karakter, en dit kan worden aangetoond, mag de verwerkingsverantwoordelijke, ofwel: a) 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: b) weigeren gevolg te geven aan het verzoek.
/03.05	De verantwoordelijke heeft gegevens ter identificatie van de betrokkene om hem zijn rechten te laten doen gelden. Deze gegevens worden niet behouden, verkrijgen of verwerkt als er geen doeleinden (U.01, §2.2.1) zijn om nog persoonsgegevens van betrokkene te verwerken[194]. Als identificatie niet mogelijk is wordt de betrokkene daarvan indien mogelijk in kennis gesteld.
/04 Specifieke uitzonderingsgrond	
/04.01	De verantwoordelijke heeft geen informatie verstrekt als de verwerking berust op een wettelijke bepaling, waarbij een specifieke uitzondering geldt[195].

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, 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 Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverant-woordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

[194] Avg art. 11.
[195] Avg art. 23.

Toelichting /04 Specifieke uitzonderingsgrond

/04.01 De volgende specifieke uitzonderingsgronden worden gesteld[196]:

a. de nationale veiligheid;
b. 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.

/04.01 De specifieke uitzonderingsgronden worden in de Avg aangeduid als "beperkingen" (van een aantal artikelen in de Avg).

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[197].

C.03 Meldplicht Datalekken				
Criterium	De verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.			
Doelstelling	Het beperken en waar mogelijk voorkomen van de negatieve consequenties van een datalek.			
Risico	Negatieve consequenties die persoonlijke levenssfeer van de betrokkene treffen.			
Referentie	Avg	Uitvoeringswet Avg		
	Art. 33, Art. 34			
Indicatoren en maatregelen				
/01 Meldt een datalek				

[196] Avg art. 23.

[197] Avg art. 4. De Engelse tekst spreekt hier van "personal data breach". De meldplicht datalekken wordt behandeld in de artikelen 33 en 34 van de Avg. Zie ook Avg overweging 85.

C.03 Meldplicht Datalekken	
/01.01	Een datalek is, tenzij er een uitzondering van toepassing is (zie /04.01), op basis vn de Avg gemeld bij de AP.
/01.02	De melding aan de AP bevat ten minste[198]: 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 persoonsgegevens-registers 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, tenzij er een uitzonderingen van toepassing is (zie /04.02), gemeld aan de betrokkene.
/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[199]: 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	
/02.01	Een verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging, zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
/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.
/02.03	Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
/02.04	De melding aan de betrokkene gebeurt onverwijld.
/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.

[198] Avg art. 33a lid 3.
[199] Avg artikel 33, lid 3, onder b, c en d.

C.03 Meldplicht Datalekken	
/03.02	De documentatie stelt de AP in staat de naleving te controleren.
/03.03	De documentatie bevat de noodzakelijke gegevens, met daarbij de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.
/03.04	De documentatie bevat informatie over het feit dat de kennisgeving is gedaan zonder onredelijke vertraging moest kunnen 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[200].
/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. - De verantwoordelijke een aanbieder is van openbare elektronische communicatiediensten zoals bedoeld in de Telecommunicatiewet[201]. - De organisatie een financiële onderneming is in de zin van de Wet op het financieel toezicht[202].
/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: - 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 er 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 wettelijke bepaling, waarbij een specifieke uitzondering geldt[203], of: - 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[204].

[200] Overweging 87.
[201] Avg art. 95.
[202] Avg art. 34.
[203] Avg art. 23.
[204] Avg overweging 18.

Toelichting /01 Meldt een datalek

/01. Het gaat in de vAvg 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 Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, 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 Er moet desgevraagd meer documentatie voorhanden zijn die welke direct in verband staan 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 met persoonsgegevens heeft plaatsgevonden, en om de AP en de betrokkene daarvan onverwijld in kennis te stellen[205].

/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 de registratie van verwerkingsactiviteiten (U.02, paar. 2.2.2). Het advies is om de documentatie van datalekken binnen deze registratie van U.02 bij te houden. Hiermee wordt dubbele opslag en dubbel beheer van informatie over de gegevensverwerkingen voorkomen.

Toelichting /04 Uitzondering

/04.02 Met de uitzondering als de Telecommunicatiewet of de Wet op het financieel toezicht van toepassing is wordt een dubbele meldplicht voorkomen.

/04.02 De volgende specifieke uitzonderingsgronden worden gesteld[206]:

a. de nationale veiligheid;
b. 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;

[205] Avg overweging 87.
[206] Avg art. 23.

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:

a. de doeleinden van de verwerking of van de categorieën van verwerking,
b. de categorieën van 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 wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.

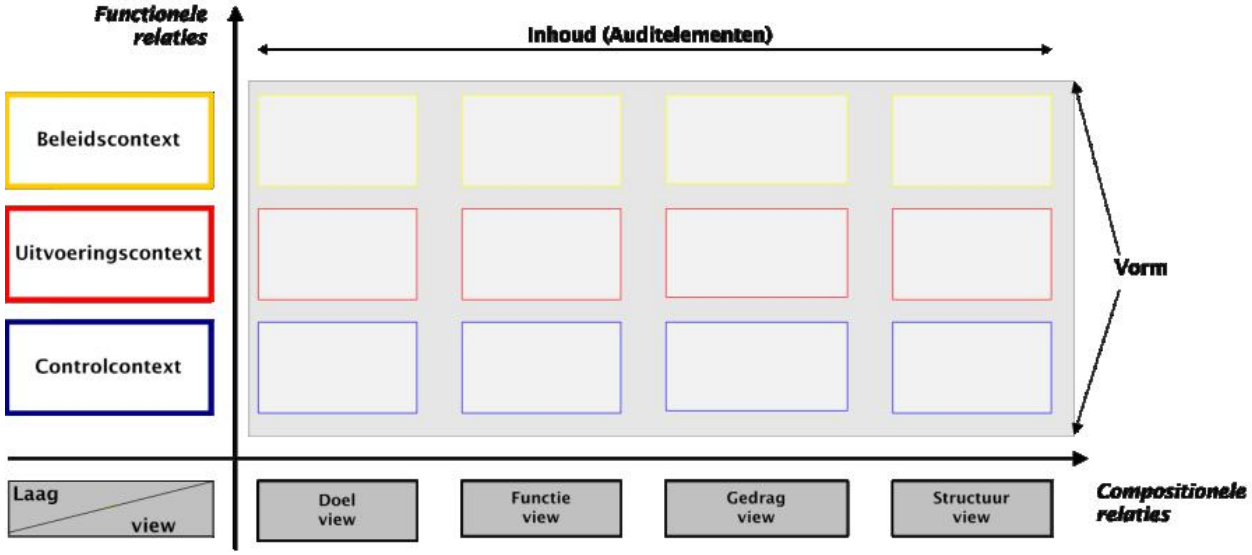
/04.02 Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten[207].

[207] Avg overweging 18.

Bijlage 1: Korte toelichting van de SIVA-methode

Het raamwerk

De Privacy Baseline is gebaseerd op de SIVA-methode[208]. De SIVA-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 criteria weer te geven.
Het voordeel van deze methode is dat duidelijk wordt aangegeven wie wat binnen een norm moet doen, terwijl de SIVA-methode tevens goed laat zien wat de context is van de normen.



Het SIVA-raamwerk

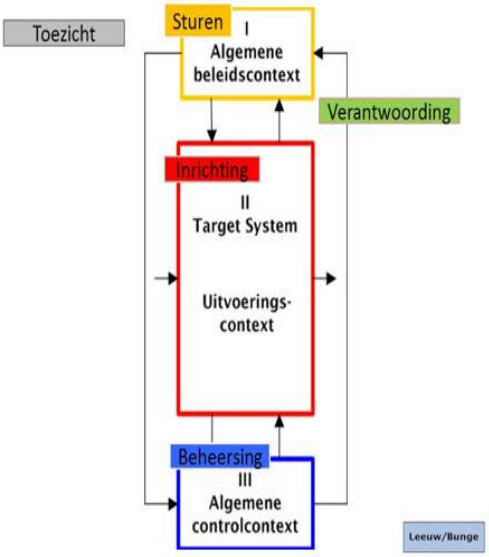
Het SIVA-raamwerk bestaat uit vier componenten (domeinen), te weten *Structuur*, *Inhoud*, *Vorm* en *Analysevolgorde.* Deze componenten zijn hulpmiddelen en worden als volgt omschreven:

- Structuur: De omgeving, in dit geval de verwerking van persoonsgegevens, is verdeeld in een aantal domeinen. Dit bevordert de volledigheid, relevantie, duidelijkheid en samenhang van de aspecten die worden onderzocht.
- Inhoud: Vanuit verschillende invalshoeken worden per domein basiselementen geïdentificeerd.
- Vorm: Per element worden het criterium geformuleerd door middel van een formuleringsvoorschrift (template).
- Analysevolgorde: Een iteratief analyseproces van de bij structuur genoemde lagen.

[208] 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.

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[209]. Deze structuur is nodig voor het verkrijgen van een compleet overall beeld, waarbinnen de criteria voor de Privacy Baseline konden worden geïdentificeerd.



Inhoud

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, doel-stellingen, 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: 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*.

Vorm

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

Predicaat	(object-1,	object-2,	object-3)
Actietype	(Wie	Wat	Waarom)

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.

[209] 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).

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.*

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 er 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 voor 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.					
…	…					

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 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 in de toelichtingen onder het kader nadere uitleg bij de maatregelen.