Richtsnoeren

Richtsnoeren 4/2019 inzake artikel 25

Gegevensbescherming door ontwerp en door standaardinstellingen

Versie 2.0

Vastgesteld op 20 oktober 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versiegeschiedenis

Versie 1.0	13 november 2019	Vaststelling van de richtsnoeren voor openbare raadpleging
Versie 2.0	20 oktober 2020	Vaststelling van de richtsnoeren door het EDPB na openbare raadpleging

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, onder e), 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 (hierna "AVG" genoemd),

Gezien de EER-Overeenkomst en met name bijlage XI en Protocol 37 daarvan, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018,

Gezien artikel 12 en artikel 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

Samenvatting

In een steeds sterker gedigitaliseerde wereld speelt naleving van voorschriften inzake gegevensbescherming door ontwerp en door standaardinstellingen een zeer belangrijke rol bij de bevordering van privacy en gegevensbescherming in de samenleving. Daarom is het essentieel dat verwerkingsverantwoordelijken deze verantwoordelijkheid serieus nemen en de AVG-verplichtingen uitvoeren wanneer zij verwerkingsactiviteiten ontwerpen.

Deze richtsnoeren bieden algemene hulp bij de in artikel 25 van de AVG beschreven verplichte gegevensbescherming door ontwerp en door standaardinstellingen (hierna "DPbDD" genoemd). DPbDD is een verplichting voor alle verwerkingsverantwoordelijken, ongeacht de omvang en complexiteit van de verwerking. Om de voorschriften inzake DPbDD te kunnen uitvoeren is het essentieel dat de verwerkingsverantwoordelijke de beginselen van gegevensbescherming en de rechten en vrijheden van betrokkenen begrijpt.

De belangrijkste verplichting is de uitvoering van *passende* maatregelen en de nodige waarborgen om te zorgen voor *doeltreffende uitvoering* van de *beginselen van gegevensbescherming* en zo de *rechten en vrijheden van betrokkenen door ontwerp en door standaardinstellingen* te waarborgen. In artikel 25 worden zowel elementen van ontwerp als van standaardinstellingen beschreven waarmee rekening moet worden gehouden. Die elementen worden in deze richtsnoeren verder uitgewerkt.

Krachtens artikel 25, lid 1, moeten verwerkingsverantwoordelijken DPbDD vroegtijdig in aanmerking nemen bij het plannen van een nieuwe verwerkingsactiviteit. Verwerkingsverantwoordelijken moeten DPbDD voor én tijdens de verwerking uitvoeren door de doeltreffendheid van de gekozen maatregelen en waarborgen regelmatig te evalueren. DPbDD is ook van toepassing op bestaande systemen die persoonsgegevens verwerken.

De richtsnoeren omvatten tevens een leidraad voor de doeltreffende uitvoering van de in artikel 5 genoemde beginselen inzake verwerking van persoonsgegevens, met een overzicht van belangrijke ontwerp- en standaardinstellingselementen en praktijksituaties ter illustratie. De verwerkingsverantwoordelijke moet nadenken over de geschiktheid van de voorgestelde maatregelen in de context van de betreffende verwerking.

Het EDPB doet aanbevelingen over de wijze waarop verwerkingsverantwoordelijken, verwerkers en producenten kunnen samenwerken om DPbDD te bewerkstelligen. Het moedigt de verwerkingsverantwoordelijken uit de sector, de verwerkers en de producenten aan DPbDD bij de marketing van hun producten richting verwerkingsverantwoordelijken en betrokkenen te gebruiken als middel om een concurrentievoordeel te behalen. Ook moedigt het alle verwerkingsverantwoordelijken aan gebruik te maken van certificeringen en gedragscodes.

1 TOEPASSINGSGEBIED

1. In de richtsnoeren ligt de nadruk op de uitvoering van DPbDD door verwerkingsverantwoordelijken op basis van de verplichting uit artikel 25 van de AVG.[1] Voor andere actoren, zoals verwerkers en producenten van producten, diensten en toepassingen (hierna "producenten" genoemd), die niet rechtstreeks aan bod komen in artikel 25, kunnen deze richtsnoeren ook nuttig zijn om producten te ontwikkelen die aan de AVG voldoen, en diensten op te zetten die verwerkingsverantwoordelijken in staat stellen om aan hun gegevensbeschermingsverplichtingen te voldoen.[2] In overweging 78 van de AVG wordt toegevoegd dat rekening moet worden gehouden met DPbDD in het kader van openbare aanbestedingen. Hoewel alle verwerkingsverantwoordelijken DPbDD in hun verwerkingen moeten opnemen, bevordert deze bepaling de vaststelling van de beginselen van gegevensbescherming, waarbij overheidsinstanties het goede voorbeeld moeten geven. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de DPbDD-verplichtingen voor de door zijn verwerkers en subverwerkers uitgevoerde verwerking en moet hier dus rekening mee houden bij het inhuren van deze partijen.

2. Het in artikel 25 beschreven voorschrift is dat verwerkingsverantwoordelijken gegevensbescherming moeten opnemen in de verwerking van persoonsgegevens, door ontwerp en als standaardinstelling. Dit geldt gedurende de gehele verwerkingscyclus. De eis van DPbDD geldt ook voor verwerkingssystemen die al bestonden voordat de AVG in werking trad. Verwerkingsverantwoordelijken moeten voortdurend zorgen dat de verwerking strookt met de AVG. Zie punt 2.1.4 van deze richtsnoeren voor meer informatie over hoe een systeem in overeenstemming met DPbDD kan worden gehouden. De kern van de bepaling is te zorgen voor een *passende* en *doeltreffende* gegevensbescherming, zowel door *ontwerp* als door *standaardinstellingen*, wat betekent dat verwerkingsverantwoordelijken moeten kunnen aantonen dat zij bij de verwerking over passende maatregelen en waarborgen beschikken om ervoor te zorgen dat de gegevensbeschermingsbeginselen en de rechten en vrijheden van betrokkenen doeltreffend zijn.

3. In hoofdstuk 2 van de richtsnoeren wordt ingegaan op een interpretatie van de voorschriften uit artikel 25 en worden de wettelijke verplichtingen onderzocht die door deze bepaling worden

[1] De interpretaties die hierin worden verstrekt, zijn eveneens van toepassing op artikel 20 van Richtlijn (EU) 2016/680 en artikel 27 van Verordening 2018/1725.

[2] In overweging 78 van de AVG wordt deze behoefte duidelijk vermeld: "*Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen de producenten van de producten, diensten en toepassingen te worden gestimuleerd om bij de ontwikkeling en de uitwerking van dergelijke producten, diensten en toepassingen rekening te houden met het recht op bescherming van persoonsgegevens en, met inachtneming van de stand van de techniek, erop toe te zien dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming*".

ingevoerd. Voorbeelden van de manier waarop DPbDD in het kader van specifieke gegevensbeschermingsbeginselen kan worden toegepast, worden verstrekt in hoofdstuk 3.

4. In de richtsnoeren wordt, in hoofdstuk 4, ook de mogelijkheid behandeld om een certificeringsmechanisme tot stand te brengen om aan te tonen dat artikel 25 wordt nageleefd. In hoofdstuk 5 wordt ingegaan op de manier waarop het artikel kan worden gehandhaafd door de toezichthoudende autoriteiten. Tot slot bevatten de richtsnoeren verdere aanbevelingen voor belanghebbenden om DPbDD met succes uit te voeren. Het EDPB erkent de uitdagingen die het voor kleine en middelgrote ondernemingen (hierna "kmo's" genoemd) oplevert wanneer zij aan de verplichtingen inzake DPbDD moeten voldoen, en neemt in hoofdstuk 6 aanvullende aanbevelingen voor kmo's op.

2 ANALYSE VAN ARTIKEL 25, LEDEN 1 EN 2, "GEGEVENSBESCHERMING DOOR ONTWERP EN DOOR STANDAARDINSTELLINGEN"

5. Het doel van dit hoofdstuk is de voorschriften voor gegevensbescherming door ontwerp uit artikel 25, lid 1, en voor gegevensbescherming door standaardinstellingen uit artikel 25, lid 2, te onderzoeken en hiervoor richtsnoeren te verstrekken. Gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen zijn complementaire concepten die elkaar versterken. Betrokkenen zullen meer profijt hebben van gegevensbescherming door standaardinstellingen als er ook sprake is van gegevensbescherming door ontwerp – en vice versa.

6. DPbDD is een vereiste voor alle verwerkingsverantwoordelijken, van kleine bedrijven tot multinationale ondernemingen. Daarom kan de complexiteit van DPbDD verschillen afhankelijk van de desbetreffende verwerkingshandeling. DPbDD kan echter in alle gevallen, ongeacht de omvang van de organisatie, voordelen opleveren voor de verwerkingsverantwoordelijke en de betrokkene.

2.1 Artikel 25, lid 1: Gegevensbescherming door ontwerp

2.1.1 De verplichting van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen en noodzakelijke waarborgen in de verwerking in te bouwen

7. Overeenkomstig artikel 25, lid 1, moet de verwerkingsverantwoordelijke *passende* technische en organisatorische *maatregelen* treffen die zijn ontworpen om de gegevensbeschermingsbeginselen uit te voeren en de *nodige waarborgen* in de verwerking inbouwen ter naleving van de voorschriften en ter bescherming van de rechten van de betrokkenen. Zowel de passende maatregelen als de noodzakelijke waarborgen dienen hetzelfde doel, namelijk de rechten van betrokkenen beschermen en ervoor zorgen dat de bescherming van persoonsgegevens in de verwerking is ingebouwd.

8. *Technische en organisatorische maatregelen* en noodzakelijke *waarborgen* kunnen in ruime zin worden opgevat als elke methode die of elk middel dat een verwerkingsverantwoordelijke bij de verwerking kan toepassen. *Passend* houdt in dat de maatregelen en noodzakelijke waarborgen geschikt moeten zijn voor het beoogde doel, oftewel dat hiermee de

gegevensbeschermingsbeginselen op een *doeltreffende* manier worden uitgevoerd[3]. De vereiste van geschiktheid hangt dus nauw samen met de vereiste van doeltreffendheid.

9. Een technische of organisatorische maatregel of waarborg kan alles zijn van de toepassing van geavanceerde technische oplossingen tot de basisopleiding van personeel. Voorbeelden van mogelijk geschikte maatregelen en waarborgen, afhankelijk van de context en de risico's van de betreffende verwerking, zijn: pseudonimisering van persoonsgegevens[4]; opslag van beschikbare persoonsgegevens in een gestructureerde, voor de meeste machines leesbare vorm; betrokkenen de mogelijkheid geven in te grijpen in de verwerking; informatie verstrekken over de opslag van persoonsgegevens; systemen voor malwaredetectie; werknemers opleiden op het gebied van basale "cyberhygiëne"; beheersystemen voor privacy en informatiebeveiliging invoeren; verwerkers contractueel verplichten specifieke praktijken voor minimale gegevensverwerking in te voeren enz.

10. Normen, beste praktijken en gedragscodes die worden erkend door verenigingen en andere organen die categorieën verwerkingsverantwoordelijken vertegenwoordigen, kunnen van pas komen bij het vaststellen van passende maatregelen. De verwerkingsverantwoordelijke moet echter controleren of de maatregelen geschikt zijn voor de betreffende verwerking.

2.1.2 Ontworpen om de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de rechten en vrijheden van betrokkenen te beschermen

11. De *gegevensbeschermingsbeginselen* (hierna "de beginselen" genoemd) staan in artikel 5. De *rechten en vrijheden van betrokkenen* zijn de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens (hierna "de rechten" genoemd). De bescherming van deze rechten wordt in artikel 1, lid 2, beschreven als het doel van de AVG[5]. De precieze bewoording hiervan is te vinden in het Handvest van de grondrechten van de Europese Unie. Het is cruciaal dat de verwerkingsverantwoordelijke de betekenis van *de beginselen* en *de rechten* begrijpt, aangezien deze de basis vormen voor de bescherming die de AVG biedt, in het bijzonder via de DPbDD-verplichting.

12. Bij de uitvoering van de passende technische en organisatorische maatregelen moeten de maatregelen en waarborgen worden *ontworpen* met inachtneming van de doeltreffende uitvoering van elk van de bovengenoemde beginselen en de daaruit voortkomende bescherming van de rechten.

Werken aan doeltreffendheid

13. Doeltreffendheid staat centraal bij het concept van gegevensbescherming door ontwerp. De vereiste om de beginselen op een doeltreffende manier uit te voeren betekent dat verwerkingsverantwoordelijken de maatregelen en waarborgen moeten uitvoeren die voor de bescherming van deze beginselen noodzakelijk zijn, om zo de rechten van betrokkenen te beschermen. Iedere uitgevoerde maatregel moet de beoogde resultaten opleveren voor de door de verwerkingsverantwoordelijke voorziene verwerking. Uit deze beschouwing komen twee dingen voort.

14. Ten eerste betekent dit dat er op grond van artikel 25 geen specifieke technische en organisatorische maatregelen verplicht zijn. De maatregelen en waarborgen moeten veeleer specifiek worden gekozen met het oog op de uitvoering van gegevensbeschermingsbeginselen bij de desbetreffende verwerking. Daarbij moeten de maatregelen en waarborgen zo worden ontworpen dat zij robuust zijn en dat de

[3] "Doeltreffendheid" komt hieronder aan bod in punt 2.1.2.
[4] Gedefinieerd in artikel 4, lid 5, van de AVG.
[5] Zie overweging 4 van de AVG.

verwerkingsverantwoordelijke verdere maatregelen kan invoeren naar aanleiding van eventuele toenamen van risico's[6]. Of maatregelen al dan niet doeltreffend zijn, hangt dus af van de context van de verwerking in kwestie en een beoordeling van bepaalde elementen die in acht moeten worden genomen bij het bepalen van de middelen van de verwerking. De bovengenoemde elementen komen in punt 2.1.3 aan bod.

15. Ten tweede moeten verwerkingsverantwoordelijken kunnen aantonen dat de beginselen in acht zijn genomen.

16. De uitgevoerde maatregelen en waarborgen moeten het gewenste effect hebben in termen van gegevensbescherming, en de verwerkingsverantwoordelijke moet over documentatie beschikken van de uitgevoerde technische en organisatorische maatregelen[7]. Hiertoe kan de verwerkingsverantwoordelijke passende kernprestatie-indicatoren (KPI's) vaststellen om de doeltreffendheid aan te tonen. Een KPI is een door de verwerkingsverantwoordelijke gekozen meetbare waarde die aantoont hoe doeltreffend de verwerkingsverantwoordelijke zijn doelstelling inzake gegevensbescherming verwezenlijkt. KPI's kunnen *kwantitatief* zijn, zoals het percentage valse positieven of valse negatieven, afname van klachten of vermindering van de reactietijd wanneer betrokkenen hun rechten uitoefenen, of *kwalitatief*, zoals beoordelingen van prestaties, gebruik van indelingsschema's of deskundige beoordelingen. In plaats van KPI's kunnen verwerkingsverantwoordelijken de doeltreffende uitvoering van de beginselen ook aantonen door de gedachte achter hun beoordeling van de doeltreffendheid van de gekozen maatregelen en waarborgen uiteen te zetten.

2.1.3 Elementen waarmee rekening moet worden gehouden

17. Artikel 25, lid 1, bevat een overzicht van elementen waarmee de verwerkingsverantwoordelijke rekening moet houden bij het vaststellen van de maatregelen voor een specifieke verwerkingsactiviteit. In de onderstaande punten worden richtsnoeren gegeven voor de manier waarop deze elementen kunnen worden toegepast in het ontwerpproces, met inbegrip van het ontwerp van de standaardinstellingen. Deze elementen dragen allemaal bij aan de vaststelling of een maatregel passend is om de beginselen doeltreffend uit te voeren. De afzonderlijke elementen vormen dus geen doel op zich, maar zijn factoren waarmee rekening moet worden gehouden om de doelstelling te verwezenlijken.

2.1.3.1 "stand van de techniek"

18. Het concept "stand van de techniek" komt voor in het EU-acquis over verschillende onderwerpen, bijvoorbeeld milieubescherming en productveiligheid. In de AVG wordt naar de "stand van de

[6] "Fundamentele beginselen die gelden voor verwerkingsverantwoordelijken (d.w.z. rechtmatigheid, minimale gegevensverwerking, doelbinding, transparantie, gegevensintegriteit, juistheid van de gegevens) blijven gelijk, ongeacht de verwerking en het risico voor de betrokkenen. De nodige aandacht voor de aard en de omvang van die verwerking maakte steeds integraal deel uit van de toepassing van deze beginselen, zodat deze inherent schaalbaar zijn." Groep gegevensbescherming artikel 29. "Verklaring over de rol van een risicogebaseerde benadering bij rechtskaders met betrekking tot gegevensbescherming." WP 218 van 30 mei 2014, blz. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Zie de overwegingen 74 en 78.

techniek"[8] verwezen in artikel 32, voor veiligheidsmaatregelen,[9] [10] maar ook in artikel 25, waardoor deze benchmark wordt uitgebreid naar alle technische en organisatorische maatregelen die in de verwerking zijn ingebed.

19. In het kader van artikel 25 legt de verwijzing naar "stand van de techniek" verwerkingsverantwoordelijken bij het bepalen van de passende technische en organisatorische maatregelen een verplichting op **om rekening te houden met de huidige vooruitgang in technologie** die op de markt beschikbaar is. Dit betekent dat verwerkingsverantwoordelijken op de hoogte moeten zijn en blijven van technologische ontwikkelingen, de gegevensbeschermingsrisico's en -mogelijkheden die technologie met zich kan meebrengen voor de verwerkingsactiviteit, en de methode om de maatregelen en waarborgen uit te voeren en bij te werken die een *doeltreffende uitvoering* van de beginselen en rechten van de betrokkenen verzekeren, met inachtneming van het veranderende technologische landschap.

20. De "stand van de techniek" is een dynamisch concept dat niet op enig moment statisch kan worden vastgesteld, maar *voortdurend* moet worden beoordeeld in de context van technologische vooruitgang. In het licht van technologische ontwikkelingen kan een verwerkingsverantwoordelijke vaststellen dat een maatregel die in het verleden een adequaat niveau van bescherming bood, niet langer toereikend is. Nalaten om op de hoogte te blijven van technologische veranderingen zou dus kunnen leiden tot niet-naleving van artikel 25.

21. Het criterium van de "stand van de techniek" geldt niet alleen voor technologische, maar ook voor organisatorische maatregelen. Een gebrek aan passende organisatorische maatregelen kan de doeltreffendheid van een gekozen technologie verminderen of zelfs volledig ondermijnen. Voorbeelden van organisatorische maatregelen zijn: vaststelling van intern beleid; actuele opleiding over technologie, beveiliging en gegevensbescherming; en beleid inzake de governance en het beheer van IT-beveiliging.

22. Bestaande en erkende kaders, normen, certificeringen, gedragscodes enz. uit verschillende domeinen kunnen een rol spelen bij het aanduiden van de "stand van de techniek" binnen het betreffende toepassingsgebied. Als er dergelijke normen zijn en deze een hoge mate van bescherming bieden voor de betrokkene die strookt met – of zelfs verder gaat dan – de wettelijke voorschriften, moeten verwerkingsverantwoordelijken deze in acht nemen bij het ontwerp en de uitvoering van gegevensbeschermingsmaatregelen.

2.1.3.2 "uitvoeringskosten"

23. De verwerkingsverantwoordelijke kan rekening houden met de uitvoeringskosten bij het kiezen en toepassen van passende technische en organisatorische maatregelen en noodzakelijke waarborgen

[8] Zie het "Kalkar"-besluit van het Duits Constitutioneel Gerechtshof in 1978: https://germanlawarchive.iuscomp.org/?p=67. Dit kan de basis vormen voor een methodologie voor een objectieve definiëring van het concept. Op basis daarvan zou het technologieniveau van de "stand van de techniek" worden geïdentificeerd tussen het technologieniveau van "bestaande wetenschappelijke kennis en onderzoek" en de meer gevestigde "algemeen aanvaarde technologieregels". De "stand van de techniek" kan bijgevolg worden geïdentificeerd als het technologieniveau van diensten, technologieën of producten die op de markt bestaan en het doeltreffendst zijn om de vastgestelde doelstellingen te bereiken.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

die voor doeltreffende uitvoering van de beginselen zorgen ter bescherming van de rechten van de betrokkenen. De kosten verwijzen naar middelen in het algemeen, ook tijd en personele middelen.

24. Het kostenelement houdt in dat de verwerkingsverantwoordelijke geen onevenredige hoeveelheid middelen hoeft te besteden wanneer er andere maatregelen bestaan die minder middelen in beslag nemen, maar ook doeltreffend zijn. De kosten van de uitvoering vormen echter slechts een factor waarmee rekening kan worden gehouden bij de uitvoering van gegevensbescherming door ontwerp, geen reden om deze vorm van gegevensbescherming niet uit te voeren.

25. De gekozen maatregelen moeten er dus voor zorgen dat de beginselen, ongeacht het kostenaspect, niet worden geschonden bij de verwerking van persoonsgegevens binnen door de verwerkingsverantwoordelijke voorziene verwerkingsactiviteiten. Verwerkingsverantwoordelijken moeten in staat zijn de totale kosten zo te beheren dat zij alle beginselen op een doeltreffende manier kunnen uitvoeren en dus de rechten kunnen beschermen.

2.1.3.3 "aard, omvang, context en doel van de verwerking"

26. Verwerkingsverantwoordelijken moeten bij de vaststelling van noodzakelijke maatregelen rekening houden met de aard, de omvang, de context en het doel van de verwerking.

27. Deze factoren moeten in lijn met hun functie in andere bepalingen van de AVG, zoals de artikelen 24, 32 en 35, worden geïnterpreteerd, met het oog op het inbouwen van gegevensbeschermingsbeginselen in de verwerking.

28. Kortom, het concept van de **aard** kan worden opgevat als de inherente[11] kenmerken van de verwerking. De **omvang** verwijst naar de grootte en het bereik van de verwerking. De **context** houdt verband met de omstandigheden van de verwerking, die een invloed kunnen uitoefenen op de verwachtingen van de betrokkene, terwijl het **doel** betrekking heeft op de doelstellingen van de verwerking.

2.1.3.4 "qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden"

29. In de AVG wordt een coherente risicogebaseerde benadering gehanteerd in veel bepalingen van de artikelen 24, 25, 32 en 35, teneinde passende technische en organisatorische maatregelen te identificeren om individuen en hun persoonsgegevens te beschermen en aan de voorschriften van de AVG te voldoen. De te beschermen activa zijn steeds hetzelfde (de individuen, via de bescherming van hun persoonsgegevens), met dezelfde risico's (voor de rechten van de individuen) en met inachtneming van dezelfde voorwaarden (aard, omvang, context en doel van de verwerking).

30. Bij het uitvoeren van de risicoanalyse voor de naleving van artikel 25 moet de verwerkingsverantwoordelijke de risico's voor de rechten van betrokkenen identificeren die schending van de beginselen met zich meebrengt, en bepalen hoe waarschijnlijk en hoe ernstig deze zijn, teneinde maatregelen uit te voeren waarmee de vastgestelde risico's op doeltreffende wijze worden beperkt. Een systematische en grondige evaluatie van de verwerking is essentieel bij de uitvoering van risicobeoordelingen. Bijvoorbeeld: een verwerkingsverantwoordelijke beoordeelt de specifieke risico's

[11] Voorbeelden zijn bijzondere categorieën persoonsgegevens, automatische besluitvorming, scheve machtsverhoudingen, onvoorspelbare verwerking, belemmeringen voor de betrokkene bij het uitoefenen van de rechten enz.

van een gebrek aan vrijelijk gegeven toestemming – een schending van het beginsel van rechtmatigheid – bij een verwerking van persoonsgegevens van kinderen en jongeren tot 18 jaar als kwetsbare groep waarbij geen andere rechtsgrond bestaat, en voert passende maatregelen uit om de vastgestelde risico's in verband met deze groep betrokkenen aan te pakken en op doeltreffende wijze te beperken.

31. De "Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling van het EDPB"[12], die gericht zijn op het bepalen of het waarschijnlijk is dat een verwerkingsactiviteit tot een hoger risico leidt voor de betrokkene, bevatten ook richtlijnen over de manier waarop gegevensbeschermingsrisico's kunnen worden beoordeeld en de manier waarop een gegevensbeschermingsrisicobeoordeling kan worden uitgevoerd. Deze richtsnoeren kunnen ook nuttig zijn tijdens de risicobeoordeling in alle bovenvermelde artikelen, waaronder artikel 25.

32. De risicogebaseerde benadering sluit het gebruik van referentiekaders, beste praktijken en normen niet uit. Deze kunnen een nuttig pakket van instrumenten vormen waarmee verwerkingsverantwoordelijken soortgelijke risico's in soortgelijke situaties (aard, omvang, context en doel van de verwerking) kunnen aanpakken. Niettemin blijft de verplichting uit artikel 25 (evenals de artikelen 24 en 32 en artikel 35, lid 7, onder c)) om rekening te houden met "*de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden*" bestaan. Om die reden moeten verwerkingsverantwoordelijken, hoewel zij door dergelijke instrumenten worden ondersteund, steeds per geval een gegevensbeschermingsrisicobeoordeling uitvoeren van de verwerking in kwestie en de doeltreffendheid van de voorgestelde passende maatregelen en waarborgen nagaan. Het kan vervolgens nodig zijn een nieuwe gegevensbeschermingseffectbeoordeling toe te voegen of een bestaande bij te werken.

2.1.4 Tijdsaspect

2.1.4.1 Bij de bepaling van de verwerkingsmiddelen

33. Gegevensbescherming door ontwerp moet worden uitgevoerd "*bij de bepaling van de verwerkingsmiddelen*".

34. De "*verwerkingsmiddelen*" variëren van de algemene tot de gedetailleerde ontwerpelementen van de verwerking, met inbegrip van de architectuur, de procedures, de protocollen, de opmaak en de algemene indruk.

35. Met "*bij de bepaling van de verwerkingsmiddelen*" wordt verwezen naar de periode waarin de verwerkingsverantwoordelijke beslist op welke manier de verwerking zal worden uitgevoerd, hoe de verwerking zal worden vormgegeven en welke mechanismen er bij de verwerking zullen worden gebruikt. Tijdens dit besluitvormingsproces moet de verwerkingsverantwoordelijke passende maatregelen en waarborgen inschatten om de beginselen en rechten van de betrokkenen op doeltreffende wijze in de verwerking in te bouwen, en moet hij rekening houden met elementen zoals de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context, het doel en de risico's.

[12] "Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling en om te bepalen of de verwerking "waarschijnlijk een hoog risico inhoudt" voor de toepassing van Verordening 2016/679" van de Groep gegevensbescherming artikel 29. WP 248 rev. 01 van 4 oktober 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711, goedgekeurd door het EDPB.

Dit omvat ook het moment waarop de gegevensverwerkingssoftware, -hardware en -diensten worden aanbesteed en uitgevoerd.

36. In een vroeg stadium nadenken over DPbDD is essentieel voor een geslaagde uitvoering van de beginselen en voor bescherming van de rechten van de betrokkenen. Vanuit een kosten-batenperspectief is het bovendien in het belang van de verwerkingsverantwoordelijke om in een zo vroeg mogelijk stadium over DPbDD na te denken, aangezien het lastig en kostbaar kan zijn om later plannen die reeds zijn gemaakt en verwerkingsactiviteiten die reeds zijn ontworpen, weer te wijzigen.

2.1.4.2 Bij de verwerking zelf (instandhouding en herziening van gegevensbeschermingsvoorschriften)

37. Wanneer de verwerking van start is gegaan, heeft de verwerkingsverantwoordelijke de doorlopende verplichting om DPbDD in stand te houden, oftewel te zorgen voor voortdurende doeltreffende uitvoering van de beginselen ter bescherming van de rechten, op de hoogte te blijven van de stand van de techniek, het risiconiveau opnieuw te beoordelen enz. De aard, de omvang en de context van verwerkingsactiviteiten, evenals het bijbehorende risico, kunnen in de loop van de verwerking veranderen, wat betekent dat de verwerkingsverantwoordelijke de verwerkingsactiviteiten telkens opnieuw moet beoordelen via regelmatige evaluaties en beoordelingen van de doeltreffendheid van de gekozen maatregelen en waarborgen.

38. De verplichting om de verwerkingsactiviteit te onderhouden, te evalueren en, indien nodig, te actualiseren geldt ook voor reeds bestaande systemen. Dat betekent dat legacysystemen die zijn ontworpen vóór de inwerkingtreding van de AVG, moeten worden geëvalueerd en onderhouden ter waarborging van de uitvoering van maatregelen en waarborgen waarmee de beginselen en de rechten van betrokkenen op een doeltreffende manier worden uitgevoerd en beschermd, zoals in deze richtsnoeren beschreven.

39. Deze verplichting heeft ook betrekking op alle verwerkingen die worden uitgevoerd via gegevensverwerkers. De activiteiten van verwerkers moeten regelmatig door de verwerkingsverantwoordelijke worden geëvalueerd en beoordeeld om ervoor te zorgen dat ze de ononderbroken naleving van de beginselen mogelijk maken en de verwerkingsverantwoordelijke in staat stellen zijn verplichtingen in dit verband na te komen.

2.2 Artikel 25, lid 2: Gegevensbescherming door standaardinstellingen

2.2.1 Door standaardinstellingen worden alleen persoonsgegevens verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking

40. Een “standaardinstelling” zoals doorgaans gedefinieerd in informatica (computerwetenschappen), verwijst naar de reeds bestaande of vooraf geselecteerde waarde van een configureerbare instelling die is toegekend aan een applicatie, computerprogramma of apparaat. Dergelijke instellingen worden ook “voorinstellingen” of “fabrieksinstellingen” genoemd, met name bij elektronische apparaten.

41. De term “door standaardinstellingen” duidt bij de verwerking van persoonsgegevens dus op het maken van keuzen in verband met de configuratiewaarden of verwerkingsopties die zijn ingesteld of voorgeschreven in een verwerkingssysteem, zoals een applicatie, dienst of apparaat, of in een handmatige verwerkingsprocedure, en die van invloed zijn op de hoeveelheid persoonsgegevens die wordt verzameld, de mate waarin deze worden verwerkt, hoe lang deze worden bewaard en in hoeverre deze toegankelijk zijn.

42. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om dusdanige standaardinstellingen voor de verwerking te kiezen en door te voeren dat er standaard uitsluitend verwerkingen worden uitgevoerd die strikt noodzakelijk zijn voor het gestelde, wettige doel. Daarvoor moeten verwerkingsverantwoordelijken vertrouwen op hun beoordeling van de noodzakelijkheid van de verwerking met betrekking tot de rechtsgronden uit artikel 6, lid 1. Dit houdt in dat de verwerkingsverantwoordelijke standaard niet meer gegevens verzamelt dan nodig is, de verzamelde gegevens niet in grotere mate verwerkt dan nodig is voor het beoogde doel, en de gegevens niet langer dan nodig bewaart. De basiseis is dat gegevensbescherming via de standaardinstellingen in de verwerking is ingebouwd.

43. De verwerkingsverantwoordelijke moet vooraf bepalen voor welke welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelstellingen de persoonsgegevens worden verzameld en verwerkt.[13] De maatregelen moeten in beginsel passend zijn om ervoor te zorgen dat alleen de persoonsgegevens worden verwerkt die noodzakelijk zijn voor elke specifieke doelstelling van de verwerking. De EDPS-richtsnoeren om de noodzakelijkheid en evenredigheid van maatregelen die het recht op gegevensbescherming beperken voor persoonsgegevens te beoordelen, kunnen ook nuttig zijn om te beslissen welke gegevens moeten worden verwerkt om een specifieke doelstelling te bereiken.[14] [15] [16]

44. Als de verwerkingsverantwoordelijke software van derden of in de handel verkrijgbare software gebruikt, moet hij een risicobeoordeling voor het betreffende product uitvoeren en ervoor zorgen dat functies die geen rechtsgrond hebben of niet stroken met het beoogde doel van de verwerking, uitgeschakeld zijn.

45. Dezelfde overwegingen gelden voor organisatorische maatregelen die de verwerkingsactiviteiten ondersteunen. Deze moeten zodanig worden ontworpen dat ze vanaf het begin alleen de minimale hoeveelheid persoonsgegevens verwerken die noodzakelijk is voor de specifieke activiteiten. In het bijzonder moet hiermee rekening worden gehouden bij het verlenen van toegang tot de gegevens aan personeelsleden met verschillende functies en verschillende toegangsbehoeften.

46. Passende “technische en organisatorische maatregelen” in het kader van gegevensbescherming door standaardinstellingen wordt dus op dezelfde manier opgevat als hierboven in punt 2.1.1 besproken, maar specifiek toegepast op de uitvoering van het beginsel van minimale gegevensverwerking.

47. De bovengenoemde verplichting om uitsluitend persoonsgegevens te verwerken die noodzakelijk zijn voor elke specifieke doelstelling, geldt voor de onderstaande elementen.

[13] Artikel 5, lid 1, onder b) tot en met e), van de AVG.

[14] EDPS. “Richtsnoeren om de noodzakelijkheid en evenredigheid van maatregelen die het recht op gegevensbescherming beperken te beoordelen”. 25 februari 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Zie ook: EDPS. “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit” https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Zie voor meer informatie over noodzakelijkheid: Groep gegevensbescherming artikel 29. “Advies 06/2014 over het begrip “gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke” in artikel 7 van Richtlijn 95/46/EG”. WP 217 van 9 april 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_nl.pdf

2.2.2 Dimensies van de verplichting van minimale gegevensverwerking

48. In artikel 25, lid 2, worden de dimensies van de verplichting van minimale gegevensverwerking voor standaardverwerking beschreven. Hier staat dat de verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.

2.2.2.1 "hoeveelheid verzamelde persoonsgegevens"

49. Verwerkingsverantwoordelijken moeten zowel het volume van de persoonsgegevens als de soorten, de categorieën en het detailniveau van de persoonsgegevens in acht nemen die vereist zijn voor de verwerkingsdoeleinden. Bij hun keuzen inzake ontwerp moeten zij rekening houden met de verhoogde risico's voor de beginselen van integriteit en vertrouwelijkheid, minimale gegevensverwerking en opslagbeperking wanneer er grote hoeveelheden gedetailleerde persoonsgegevens worden verzameld, en deze vergelijken met de verlaging van de risico's wanneer er kleinere hoeveelheden en/of minder gedetailleerde informatie over de betrokkenen wordt verzameld. In elk geval mag de verzameling van persoonsgegevens die niet noodzakelijk zijn voor het specifieke verwerkingsdoel, niet in de standaardinstellingen worden opgenomen. Met andere woorden, indien bepaalde categorieën van persoonsgegevens niet noodzakelijk zijn of indien gedetailleerde gegevens niet nodig zijn omdat minder granulaire gegevens volstaan, worden er geen bijkomende persoonsgegevens verzameld.

50. Dezelfde standaardeisen gelden voor diensten: ongeacht het platform of apparaat mogen uitsluitend de voor het gestelde doel noodzakelijke persoonsgegevens worden verzameld.

2.2.2.2 "de mate waarin zij worden verwerkt"

51. Verwerkingsactiviteiten[17] die op persoonsgegevens worden uitgevoerd, worden beperkt tot wat noodzakelijk is. Vele verwerkingsactiviteiten kunnen bijdragen aan een verwerkingsdoel. Het feit dat bepaalde persoonsgegevens nodig zijn om een doel te verwezenlijken, betekent echter niet dat alle soorten en frequenties van verwerkingsactiviteiten op de gegevens mogen worden uitgevoerd. Verwerkingsverantwoordelijken moeten er zorg voor dragen dat zij de grenzen van de "verenigbare doeleinden" uit artikel 6, lid 4, niet verleggen, en zij moeten voor ogen houden wat verwerking inhoudt binnen de redelijke verwachtingen van de betrokkenen.

2.2.2.3 "de termijn waarvoor zij worden opgeslagen"

52. Verzamelde persoonsgegevens mogen niet worden opgeslagen als dit voor de verwerking niet nodig is en er geen ander verenigbaar doel en geen rechtsgrond is krachtens artikel 6, lid 4. Als gegevens worden bewaard, moet de verwerkingsverantwoordelijke objectief kunnen rechtvaardigen dat dit noodzakelijk is overeenkomstig het beginsel van verantwoordingsplicht.

53. De verwerkingsverantwoordelijke beperkt de bewaartermijn tot wat noodzakelijk is voor het doel. Indien persoonsgegevens niet meer nodig zijn met het oog op de verwerking, worden deze in beginsel vernietigd of geanonimiseerd. De lengte van de bewaartermijn hangt dus af van het doel van de betreffende verwerking. Deze verplichting houdt rechtstreeks verband met het beginsel van opslagbeperking uit artikel 5, lid 1, onder e), en moet een standaardinstelling vormen, d.w.z. dat de

[17] Krachtens artikel 4, lid 2, van de AVG omvat dit 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.

verwerkingsverantwoordelijke systematische procedures voor gegevensvernietiging of -anonimisering moet inbouwen in de verwerking.

54. Anonimisering[18] van persoonsgegevens vormt een alternatief voor vernietiging, mits er rekening wordt gehouden met alle relevante contextuele elementen en mits de waarschijnlijkheid en ernst van het risico, inclusief het risico op hernieuwde identificatie, regelmatig worden beoordeeld.[19]

2.2.2.4 "de toegankelijkheid daarvan"

55. De verwerkingsverantwoordelijke moet op basis van een beoordeling van de noodzaak beperken wie er toegang hebben tot persoonsgegevens en welke soorten toegang er worden verleend, en ervoor zorgen dat persoonsgegevens wanneer dit noodzakelijk is, bijvoorbeeld in kritische situaties, toegankelijk zijn voor degenen voor wie dit noodzakelijk is. Toegangscontroles moeten tijdens de verwerking worden geëerbiedigd voor de hele gegevensstroom.

56. In artikel 25, lid 2, wordt verder bepaald dat persoonsgegevens niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk mogen worden gemaakt. De verwerkingsverantwoordelijke moet de toegankelijkheid in beginsel beperken en de betrokkene de mogelijkheid geven in te grijpen alvorens persoonsgegevens over de betrokkene te publiceren of op een andere manier beschikbaar te stellen voor een onbeperkt aantal natuurlijke personen.

57. Het beschikbaar maken van persoonsgegevens voor een onbeperkt aantal natuurlijke personen kan leiden tot verdere verspreiding van de gegevens dan oorspronkelijk bedoeld. Dit is met name relevant in de context van het internet en zoekmachines. Verwerkingsverantwoordelijken moeten betrokkenen daarom in beginsel een mogelijkheid geven in te grijpen alvorens persoonsgegevens op het open internet beschikbaar worden gemaakt. Dit is met name van belang wanneer het om kinderen en kwetsbare groepen gaat.

58. Afhankelijk van de rechtsgrond voor de verwerking kan de mogelijkheid tot ingrijpen verschillen op basis van de context van de verwerking. Voorbeelden zijn vragen om toestemming om de persoonsgegevens openbaar toegankelijk te maken of privacy-instellingen hanteren waardoor de betrokkenen de openbare toegang zelf kunnen beheren.

59. Zelfs indien persoonsgegevens openbaar beschikbaar worden gesteld met toestemming en medeweten van een betrokkene, betekent dit niet dat alle andere verwerkingsverantwoordelijken die toegang hebben tot de persoonsgegevens, deze zelf voor hun eigen doeleinden vrij mogen verwerken. Zij hebben hiervoor een eigen rechtsgrond nodig.[20]

[18] Groep gegevensbescherming artikel 29. "Advies 05/2014 over anonimiseringstechnieken". WP 216 van 10 april 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf

[19] Zie artikel 4, lid 1, van de AVG, overweging 26 van de AVG en "Advies 5/2014 over anonimiseringstechnieken" van de Groep gegevensbescherming artikel 29. Zie ook het onderdeel over "opslagbeperking" in deel 3 van dit document, waarin wordt aangegeven dat de verwerkingsverantwoordelijke moet zorgen voor de doeltreffendheid van de uitgevoerde anonimiseringstechniek(en).

[20] Zie zaak Satakunnan Markkinapörssi Oy en Satamedia Oy tegen Finland nr. 931/13.

3 GEGEVENSBESCHERMINGSBEGINSELEN UITVOEREN BIJ DE VERWERKING VAN PERSOONSGEGEVENS VIA GEGEVENSBESCHERMING DOOR ONTWERP EN DOOR STANDAARDINSTELLINGEN

60. In alle fasen van het ontwerp van de verwerkingsactiviteiten, inclusief inkoop, aanbestedingen, uitbesteding, ontwikkeling, ondersteuning, onderhoud, testen, opslag, vernietiging enz., moet de verwerkingsverantwoordelijke de verschillende elementen van DPbDD in acht en in overweging nemen. Deze worden in dit hoofdstuk aan de hand van voorbeelden toegelicht in het kader van de uitvoering van de beginselen.[21] [22] [23]

61. Verwerkingsverantwoordelijken moeten de beginselen uitvoeren om DPbDD te verwezenlijken. Het betreft de volgende beginselen: transparantie, rechtmatigheid, behoorlijkheid, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, en verantwoordingsplicht. Deze beginselen worden beschreven in artikel 5 en overweging 39 van de AVG. Voor een volledig begrip van de manier waarop DPbDD moet worden uitgevoerd, wordt benadrukt hoe belangrijk het is de betekenis van elk van de beginselen te begrijpen.

62. Bij de presentatie van voorbeelden van de wijze waarop DPbDD kan worden geoperationaliseerd, hebben we een lijst gemaakt met **belangrijke DPbDD-elementen** voor elk van de beginselen. De voorbeelden belichten het specifieke gegevensbeschermingsbeginsel in kwestie, maar kunnen ook gedeeltelijk samenvallen met andere hiermee nauw samenhangende beginselen. Het EDPB benadrukt dat de belangrijke elementen en de voorbeelden die hieronder worden beschreven, uitputtend noch bindend zijn. Zij zijn slechts bedoeld als richtsnoeren voor elk van de beginselen. Verwerkingsverantwoordelijken moeten beoordelen hoe zij de naleving van de beginselen kunnen garanderen in het kader van de concrete verwerkingsactiviteit in kwestie.

63. Hoewel dit gedeelte gericht is op de uitvoering van de beginselen, moet de verwerkingsverantwoordelijke ook *passende* en *doeltreffende* methoden toepassen om de rechten van betrokkenen te beschermen, ook overeenkomstig hoofdstuk III van de AVG als dit nog niet op grond van de beginselen zelf verplicht is.

64. Het beginsel van verantwoordingsplicht is overkoepelend: op grond van dit beginsel moet de verwerkingsverantwoordelijke verantwoordelijk zijn voor het kiezen van de noodzakelijke technische en organisatorische maatregelen.

3.1 Transparantie[24]

[21] Meer voorbeelden zijn te vinden in: Noorse gegevensbeschermingsautoriteit, “Softwareontwikkeling via gegevensbescherming door ontwerp en door standaardinstellingen”. 28 november 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Meer informatie over de manier waarop het concept transparantie kan worden opgevat, is terug te vinden in: Groep gegevensbescherming artikel 29, “Richtsnoeren over transparantie in het kader van Verordening 2016/679”. WP 260 rev. 01 van 11 april 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – goedgekeurd door het EDPB.

65. De verwerkingsverantwoordelijke moet naar de betrokkene toe duidelijk en open zijn over de manier waarop de persoonsgegevens worden verzameld, gebruikt en gedeeld. Transparantie gaat over het in staat stellen van betrokkenen om hun rechten uit de artikelen 15 tot en met 22 te begrijpen en waar nodig uit te oefenen. Het beginsel is vervat in de artikelen 12, 13, 14 en 34. Maatregelen en waarborgen die worden getroffen ter ondersteuning van het beginsel van transparantie, moeten de uitvoering van deze artikelen ook ondersteunen.

66. Belangrijke ontwerp- en standaardinstellingselementen voor het beginsel van transparantie zijn onder meer:

- Duidelijkheid – informatie wordt in duidelijke en eenvoudige taal, beknopt en begrijpelijk verstrekt.
- Semantiek – communicatie heeft een duidelijke betekenis voor het betrokken doelpubliek.
- Toegankelijkheid – informatie is eenvoudig toegankelijk voor de betrokkene.
- Contextueel – informatie wordt op het relevante tijdstip en in de passende vorm verstrekt.
- Relevantie – informatie is relevant en toepasselijk voor de specifieke betrokkene.
- Universeel ontwerp – informatie is toegankelijk voor alle betrokkenen, inclusief het gebruik van machinaal leesbare talen om de leesbaarheid en duidelijkheid te bevorderen.
- Begrijpelijk – betrokkenen hebben een goed begrip van wat zij kunnen verwachten met betrekking tot de verwerking van hun persoonsgegevens, in het bijzonder wanneer de betrokkenen kinderen of andere kwetsbare groepen zijn.
- Meerdere kanalen – informatie wordt verstrekt via verschillende kanalen en media, niet alleen tekstuele, om de waarschijnlijkheid dat de informatie effectief bij de betrokkene terechtkomt, te vergroten.
- Gelaagd – informatie wordt zo gestructureerd dat de spanning tussen volledigheid en begrijpelijkheid wordt weggenomen en er tegelijk aan de redelijke verwachtingen van betrokkenen wordt voldaan.

Voorbeeld[25]

Een verwerkingsverantwoordelijke ontwerpt een privacybeleid op zijn website om aan de vereisten inzake transparantie te voldoen. Het privacybeleid moet geen grote hoeveelheid informatie bevatten die voor de gemiddelde betrokkene lastig te begrijpen is. Het moet helder en beknopt worden geschreven, zodat het voor de gebruiker van de website gemakkelijk te begrijpen is op welke manier zijn of haar persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke verstrekt daarom informatie op een gelaagde manier, waarbij de belangrijkste punten worden gemarkeerd. Gedetailleerdere informatie moet gemakkelijk te vinden zijn. Er worden vervolgkeuzemenu's en links naar andere pagina's verstrekt, waar de verschillende punten en concepten uit het beleid nader worden toegelicht. De verwerkingsverantwoordelijke zorgt er ook voor dat de informatie via meerdere kanalen wordt aangeboden, met video's waarin de belangrijkste punten van de schriftelijke informatie worden toegelicht. Synergie tussen de verschillende pagina's is essentieel om te zorgen dat de gelaagde benadering niet voor meer verwarring zorgt, maar deze juist wegneemt.

Het privacybeleid moet eenvoudig toegankelijk zijn voor de betrokkenen. Het wordt daarom beschikbaar gesteld en zichtbaar gemaakt op alle webpagina's van de desbetreffende internetsite, zodat de betrokkene steeds met één muisklik toegang kan krijgen tot de informatie. De verstrekte

[25] De Franse gegevensbeschermingsautoriteit heeft talrijke voorbeelden gepubliceerd van beste praktijken om gebruikers in te lichten, evenals andere transparantiebeginselen: https://design.cnil.fr/en/

informatie wordt bovendien opgesteld overeenkomstig de beste praktijken en normen van universeel ontwerp, zodat deze voor iedereen toegankelijk is.

Bovendien moet de noodzakelijke informatie ook in de juiste context en op het geschikte moment worden verstrekt. Aangezien de verwerkingsverantwoordelijke veel verwerkingsactiviteiten uitvoert met de op de website verzamelde gegevens, is enkel een privacybeleid op de website niet voldoende om aan de eisen inzake transparantie te voldoen. De verwerkingsverantwoordelijke stelt daarom een informatiestroom op waarmee de betrokkene relevante informatie ontvangt binnen de passende contexten, bijvoorbeeld via informatiefragmenten of pop-ups. Wanneer de betrokkene bijvoorbeeld wordt gevraagd om persoonsgegevens in te voeren, informeert de verwerkingsverantwoordelijke de betrokkene over de manier waarop de persoonsgegevens worden verwerkt en de reden waarom deze persoonsgegevens noodzakelijk zijn voor de verwerking.

3.2 Rechtmatigheid

67. De verwerkingsverantwoordelijke moet een geldige rechtsgrond vaststellen voor de verwerking van persoonsgegevens. Maatregelen en waarborgen moeten de vereiste ondersteunen dat de hele levenscyclus van de verwerking in overeenstemming is met de relevante rechtsgronden van verwerking.

68. Belangrijke ontwerp- en standaardinstellingselementen voor rechtmatigheid zijn onder meer:
- Relevantie – de juiste rechtsgrond wordt op de verwerking toegepast.
- Differentiatie[26] – de gebruikte rechtsgrond voor iedere verwerkingsactiviteit wordt gedifferentieerd.
- Gespecificeerd doel – de passende rechtsgrond houdt duidelijk verband met het specifieke doel van de verwerking.[27]
- Noodzakelijkheid – om rechtmatig te zijn moet de verwerking onvoorwaardelijk en noodzakelijk zijn voor het doel.
- Autonomie – de betrokkene krijgt binnen de kaders van de rechtsgrond de hoogst mogelijke mate van autonomie toegekend wat controle over de persoonsgegevens betreft.
- Toestemming verkrijgen – toestemming moet vrijelijk worden gegeven en specifiek, geïnformeerd en ondubbelzinnig zijn.[28] Er moet bijzondere aandacht worden besteed aan het vermogen van kinderen en jongeren om geïnformeerd toestemming te geven.
- Intrekken van toestemming – wanneer toestemming de rechtsgrond is, is het mogelijk de toestemming voor de verwerking weer in te trekken. Het intrekken van toestemming is net zo eenvoudig als het geven ervan. Zo niet, dan voldoet het toestemmingsmechanisme van de verwerkingsverantwoordelijke niet aan de AVG.[29]
- Belangenafweging – wanneer gerechtvaardigd belang de rechtsgrond is, voert de verwerkingsverantwoordelijke een gewogen belangenafweging uit en besteedt hij daarbij

[26] EDPB. "Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen". Versie 2.0 van 8 oktober 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[27] Zie het gedeelte hieronder over doelbinding.

[28] Zie Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679.https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Zie Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, blz. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

bijzondere aandacht aan het machtsverschil, met name bij kinderen tot 18 jaar en andere kwetsbare groepen. Er worden maatregelen en waarborgen ingesteld om de negatieve gevolgen voor de betrokkenen te beperken.

- Bepaling vooraf – de rechtsgrond wordt vastgesteld voordat de verwerking plaatsvindt.
- Beëindiging – indien de rechtsgrond niet langer van toepassing is, wordt de verwerking dienovereenkomstig beëindigd.
- Aanpassing – indien er een geldige wijziging is van de rechtsgrond voor de verwerking, wordt de feitelijke verwerking overeenkomstig de nieuwe rechtsgrond aangepast.[30]
- Toewijzing van verantwoordelijkheid – indien gezamenlijke verwerkingsverantwoordelijkheid is voorzien, verdelen de partijen hun respectieve verantwoordelijkheden ten aanzien van de betrokkene op een duidelijke en transparante wijze en ontwerpen zij de maatregelen voor de verwerking in overeenstemming met deze verdeling.

Voorbeeld

Een bank is van plan een dienst aan te bieden om de doeltreffendheid van het beheer van leningsaanvragen te verbeteren. Het idee achter de dienst is dat de bank, door toestemming van de klant te vragen, gegevens over de klant rechtstreeks van belastingdiensten kan verwerven. In dit voorbeeld wordt niet ingegaan op de verwerking van persoonsgegevens uit andere bronnen.

Deze persoonsgegevens over de financiële situatie van de betrokkene moeten worden verkregen om op verzoek van de betrokkene stappen te kunnen ondernemen alvorens een leenovereenkomst te sluiten.[31] Het wordt echter niet noodzakelijk geacht om deze persoonsgegevens rechtstreeks van de belastingdiensten te verkrijgen, want de klant kan een overeenkomst sluiten door de informatie van de belastingdiensten zelf aan te leveren. Hoewel de bank een gerechtvaardigd belang kan hebben om de documentatie rechtstreeks van de belastingdiensten te verkrijgen, bijvoorbeeld met het oog op de waarborging van de efficiëntie van de verwerking van de lening, levert het verlenen van dergelijke directe toegang tot de persoonsgegevens van aanvragers aan banken een risico op ten aanzien van het gebruik of potentiële misbruik van de toegangsrechten.

Bij de uitvoering van het rechtmatigheidsbeginsel is de verwerkingsverantwoordelijke zich ervan bewust dat hij in deze situatie de grond “noodzakelijk voor contract” niet kan gebruiken voor het deel van de verwerking dat betrekking heeft op het rechtstreeks verzamelen van persoonsgegevens van de belastingdiensten. Het feit dat deze specifieke verwerking het risico inhoudt dat de betrokkene minder betrokken is bij de verwerking van zijn gegevens, is ook een relevante factor bij het beoordelen van de rechtmatigheid van de verwerking zelf. De bank concludeert dat er voor dit deel van de verwerking een andere rechtsgrond nodig is. In de lidstaat waar de verwerkingsverantwoordelijke is gevestigd, zijn er nationale wetten op grond waarvan de bank rechtstreeks informatie mag verkrijgen van de belastingdiensten indien de betrokkene hier vooraf toestemming voor geeft.

De bank verstrekt daarom informatie over de verwerking in het online-aanvraagplatform, zodanig dat de betrokkenen gemakkelijk kunnen begrijpen welke verwerking verplicht is en welke optioneel. De verwerkingsopties staan standaard niet toe dat gegevens rechtstreeks bij andere bronnen dan de betrokkene zelf worden opgevraagd, en de optie voor rechtstreekse informatie-opvraging wordt zodanig aangeboden dat dit de betrokkene niet ontmoedigt om zich te onthouden. Toestemming die

[30] Is de oorspronkelijke rechtsgrond toestemming, zie dan Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[31] Zie artikel 6, lid 1, onder b), van de AVG.

wordt verleend om gegevens rechtstreeks van andere verwerkingsverantwoordelijken te verzamelen, is een tijdelijk recht op toegang tot een specifiek informatiepakket.

De verleende toestemming wordt elektronisch en op een documenteerbare manier verwerkt, en betrokkenen krijgen een eenvoudige manier aangeboden om te controleren waarvoor zij toestemming hebben verleend en om hun toestemming in te trekken.

De verwerkingsverantwoordelijke heeft deze DPbDD-vereisten vooraf beoordeeld en neemt al deze criteria op in de eisenspecificatie voor de inschrijving voor het platform. De verwerkingsverantwoordelijke is zich ervan bewust dat het, indien hij de DPbDD-vereisten niet opneemt in de inschrijving, te laat of zeer kostbaar kan zijn om nadien gegevensbescherming uit te voeren.

3.3 Behoorlijkheid

69. Behoorlijkheid is een overkoepelend beginsel op grond waarvan persoonsgegevens niet mogen worden verwerkt op een manier die op een niet te rechtvaardigen manier nadelig, onwettig discriminerend, onverwacht of misleidend is voor de betrokkene. Maatregelen en waarborgen ter uitvoering van het beginsel van behoorlijkheid ondersteunen ook de rechten en vrijheden van betrokkenen, in het bijzonder het recht op informatie (transparantie), het recht op tussenkomst (inzage, wissing, gegevensoverdracht, rectificatie) en het recht op beperking van de verwerking (het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming en non-discriminatie van betrokkenen bij die procedures).

70. Belangrijke ontwerp- en standaardinstellingselementen voor behoorlijkheid zijn onder meer:
    - Autonomie – betrokkenen krijgen de hoogst mogelijke mate van autonomie om te bepalen hoe hun persoonsgegevens worden gebruikt of verwerkt en in welke mate en onder welke voorwaarden dat gebeurt.
    - Interactie – betrokkenen kunnen communiceren met de verwerkingsverantwoordelijke en hun rechten uitoefenen ten aanzien van de door deze verwerkingsverantwoordelijke verwerkte persoonsgegevens.
    - Verwachting – de verwerking komt overeen met de redelijke verwachtingen van de betrokkenen.
    - Non-discriminatie – de verwerkingsverantwoordelijke discrimineert de betrokkenen niet op onbehoorlijke wijze.
    - Niet-exploitatie – de verwerkingsverantwoordelijke buit de behoeften of de kwetsbaarheden van de betrokkenen niet uit.
    - Keuze van de consument – de verwerkingsverantwoordelijke mag zijn gebruikers niet op onbehoorlijke wijze “vasthouden”. Wanneer een dienst die persoonsgegevens verwerkt, door eigendomsrechten is beschermd, kan er sprake zijn van onbehoorlijk vasthouden als de betrokkenen hun recht van gegevensoverdraagbaarheid niet goed kunnen uitoefenen overeenkomstig artikel 20.
    - Machtsevenwicht – machtsevenwicht is een belangrijke doelstelling voor de relatie tussen verwerkingsverantwoordelijke en betrokkene. Machtsverschillen moeten worden vermeden. Wanneer dit niet mogelijk is, moeten zij worden erkend en moeten er passende tegenmaatregelen worden genomen.
    - Geen risico-overdracht – verwerkingsverantwoordelijken dragen de risico’s van het bedrijf niet op de betrokkenen over.

- Geen misleiding – informatie over en opties voor gegevensverwerking worden op een objectieve en neutrale manier aangeleverd, zonder misleidende of manipulerende bewoordingen of vormgevingen.
- Eerbiediging van rechten – de verwerkingsverantwoordelijke eerbiedigt de grondrechten van betrokkenen, voert passende maatregelen en waarborgen uit en tast deze rechten niet aan, tenzij dit uitdrukkelijk is gerechtvaardigd op grond van de wet.
- Ethisch – de verwerkingsverantwoordelijke heeft oog voor het bredere effect van de verwerking op de rechten en waardigheid van het individu.
- Eerlijk – de verwerkingsverantwoordelijke stelt informatie beschikbaar over de manier waarop hij persoonsgegevens verwerkt, doet wat hij belooft en misleidt de betrokkenen niet.
- Menselijke tussenkomst – de verwerkingsverantwoordelijke integreert *gekwalificeerde* menselijke tussenkomst die de vertekeningen blootlegt die machines kunnen veroorzaken, overeenkomstig het recht om niet te worden onderworpen aan een geautomatiseerde individuele besluitvorming uit artikel 22.[32]
- Eerlijke algoritmen – Er wordt regelmatig beoordeeld of de algoritmen werken in overeenstemming met de doelen, waarbij de algoritmen worden aangepast om ontdekte vertekening te beperken en behoorlijkheid te waarborgen bij de verwerking. Er wordt informatie verstrekt aan betrokkenen over de verwerking van persoonsgegevens op basis van algoritmen die hen analyseren of voorspellingen over hen maken, bijvoorbeeld met betrekking tot arbeidsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag, locatie of verplaatsingen.[33]

Voorbeeld 1

Een verwerkingsverantwoordelijke beheert een zoekmachine die voornamelijk door gebruikers gegenereerde persoonsgegevens verwerkt. De verwerkingsverantwoordelijke haalt voordeel uit het feit dat hij grote hoeveelheden persoonsgegevens ter beschikking heeft en die persoonsgegevens kan gebruiken voor gerichte advertenties. De verwerkingsverantwoordelijke wil daarom invloed uitoefenen op de betrokkenen, zodat zij uitgebreidere verzameling en gebruikmaking van hun persoonsgegevens toelaten. Daarvoor moet toestemming worden verkregen door verwerkingsopties aan de betrokkene voor te leggen.

Bij de uitvoering van het behoorlijkheidsbeginsel is de verwerkingsverantwoordelijke zich er, rekening houdend met de aard, de omvang, de context en het doel van de verwerking, van bewust dat hij deze opties niet kan aanbieden op een manier die de betrokkene aanzet om toe te laten dat de verwerkingsverantwoordelijke meer persoonsgegevens verzamelt dan wanneer de opties op een gelijke en neutrale manier werden aangeboden. Dit wil zeggen dat hij de verwerkingsopties niet mag aanbieden op een manier die het voor betrokkenen moeilijk maakt om hun gegevens niet te delen, of die het voor betrokkenen moeilijk maakt om hun privacy-instellingen aan te passen en de verwerking te beperken. Dit zijn voorbeelden van manipulatieve patronen, die in strijd zijn met de geest van artikel 25. De standaardopties voor de verwerking mogen niet invasief zijn, en de keuze voor de verdere verwerking moet worden aangeboden op een manier die de betrokkene niet onder druk zet

[32] Zie Richtsnoeren over geautomatiseerde individuele besluitvorming en profilering voor de toepassing van verordening 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] Zie overweging 71 van de AVG.

om toestemming te geven. De verwerkingsverantwoordelijke biedt de opties om wel of geen toestemming te geven daarom als twee in gelijke mate zichtbare keuzemogelijkheden aan en geeft daarbij de gevolgen van elke keuze voor de betrokkene correct weer.

Voorbeeld 2

Een andere verwerkingsverantwoordelijke verwerkt persoonsgegevens voor de verlening van een streamingdienst waarbij gebruikers de keuze hebben tussen een gewoon abonnement van standaardkwaliteit en een premiumabonnement van hoge kwaliteit. Als onderdeel van het premiumabonnement krijgen abonnees prioritaire klantendienstverlening.

Op grond van het behoorlijkheidsbeginsel mag de prioritaire klantendienstverlening die aan premiumabonnees wordt toegekend, de mogelijkheid van gewone abonnees om hun rechten uit te oefenen niet discrimineren overeenkomstig artikel 12 van de AVG. Dit wil zeggen dat, ook al krijgen de premiumabonnees prioritaire dienstverlening, die prioritering niet mag leiden tot een gebrek aan passende maatregelen om zonder onnodige vertraging, en in elk geval binnen een maand na de ontvangst van de verzoeken, te antwoorden op verzoeken van gewone abonnees.

Prioritaire klanten mogen betalen voor een betere dienstverlening, maar alle betrokkenen moeten gelijke en ongedifferentieerde toegang hebben om hun rechten en vrijheden overeenkomstig artikel 12 te kunnen uitoefenen.

3.4 Doelbinding[34]

71. De verwerkingsverantwoordelijke moet gegevens verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, en mag de gegevens niet op een met die doeleinden onverenigbare wijze verder verwerken.[35] Het ontwerp van de verwerking moet daarom worden vormgegeven op basis van wat noodzakelijk is om de doeleinden te bereiken. Vindt verdere verwerking plaats, dan moet de verwerkingsverantwoordelijke er eerst voor zorgen dat de doeleinden van deze verwerking verenigbaar zijn met de oorspronkelijke doeleinden en de verwerking dienovereenkomstig ontwerpen. Of een nieuw doeleinde verenigbaar is of niet, wordt beoordeeld overeenkomstig artikel 6, lid 4.

72. Belangrijke ontwerp- en standaardinstellingselementen voor doelbinding zijn onder meer:
- Bepaling vooraf – de rechtsgrond wordt vastgesteld vóór het ontwerp van de verwerking.
- Specificiteit – het doel van de verwerking van persoonsgegevens is welbepaald en uitdrukkelijk omschreven.
- Doelgerichtheid – het doel van de verwerking stuurt het ontwerp van de verwerking en legt de grenzen van de verwerking vast.
- Noodzakelijkheid – het doel bepaalt welke persoonsgegevens noodzakelijk zijn voor de verwerking.

[34] De Groep gegevensbescherming artikel 29 heeft richtsnoeren uitgebracht om het doelbindingsbeginsel in het kader van Richtlijn 95/46/EG toe te lichten. Hoewel het Advies niet door het EDPB is vastgesteld, kan het wel relevant zijn, aangezien de formulering in de AVG dezelfde is. Groep gegevensbescherming artikel 29. "Advies 03/2013 over doelbinding". WP 203 van 2 april 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Artikel 5, lid 1, onder b), van de AVG.

- Verenigbaarheid – elk nieuw doeleinde moet verenigbaar zijn met het oorspronkelijke doeleinde waarvoor de gegevens werden verzameld, en moet relevante veranderingen in het ontwerp sturen.
- Verdere verwerking beperken – de verwerkingsverantwoordelijke verbindt geen gegevensreeksen met elkaar en voert geen verdere verwerkingen uit voor nieuwe onverenigbare doeleinden.
- Beperkingen van hergebruik – de verwerkingsverantwoordelijke treft technische maatregelen, waaronder hashing en versleuteling, om de mogelijkheid van herbestemming van persoonsgegevens te beperken. Ook treft de verwerkingsverantwoordelijke organisatorische maatregelen, zoals beleid en contractuele verplichtingen, die hergebruik van persoonsgegevens beperken.
- Evaluatie – de verwerkingsverantwoordelijke evalueert regelmatig of de verwerking noodzakelijk is voor de doeleinden waarvoor de gegevens werden verzameld, en toetst het ontwerp regelmatig aan doelbinding.

Voorbeeld

De verwerkingsverantwoordelijke verwerkt persoonsgegevens van zijn klanten. Het doel van de verwerking is een overeenkomst uitvoeren, d.w.z. goederen aan het juiste adres kunnen leveren en betaling ontvangen. De persoonsgegevens die worden opgeslagen, zijn de aankoopgeschiedenis, de naam, het adres, het e-mailadres en het telefoonnummer.

De verwerkingsverantwoordelijke overweegt een product voor het beheer van klantenrelaties (CRM) aan te kopen dat alle klantengegevens over verkoop, marketing en klantenservice op één plaats bijeenbrengt. Het product biedt de mogelijkheid om alle telefoonoproepen, activiteiten, documenten, e-mails en marketingcampagnes op te slaan om een 360-gradenbeeld van de klant te krijgen. Bovendien kan het CRM-product automatisch de koopkracht van de klant analyseren door openbare informatie te gebruiken. Het doel van de analyse is om gerichtere reclameactiviteiten te creëren. Deze activiteiten zijn geen onderdeel van het oorspronkelijke wettige doeleinde van de verwerking.

Om in overeenstemming te zijn met het beginsel van doelbinding verzoekt de verwerkingsverantwoordelijke de aanbieder van het product om de verschillende verwerkingsactiviteiten in kaart te brengen die gebruikmaken van persoonsgegevens voor doeleinden die relevant zijn voor de verwerkingsverantwoordelijke.

Nadat hij de resultaten hiervan heeft ontvangen, beoordeelt de verwerkingsverantwoordelijke of het nieuwe marketingdoeleinde en het doeleinde van gerichte reclame verenigbaar zijn met de oorspronkelijke doeleinden die zijn vastgesteld toen de gegevens werden verzameld, en of er voldoende rechtsgrond is voor de betreffende verwerking. Als de beoordeling geen positief resultaat oplevert, mag de verwerkingsverantwoordelijke de betreffende functionaliteiten niet in gebruik nemen. De verwerkingsverantwoordelijke kan er ook voor kiezen geen beoordeling uit te voeren en de beschreven functionaliteiten van het product simpelweg niet te gebruiken.

3.5 Minimale gegevensverwerking

73. Uitsluitend persoonsgegevens die toereikend zijn, ter zake dienend en beperkt tot wat **noodzakelijk** is voor het doeleinde, worden verwerkt.[36] Bijgevolg moet de verwerkingsverantwoordelijke vooraf bepalen welke kenmerken en parameters van verwerkingssystemen en hun ondersteunende functies toelaatbaar zijn. Minimale gegevensverwerking verwezenlijkt en operationaliseert het noodzakelijkheidsbeginsel. Bij de verdere verwerking moet de verwerkingsverantwoordelijke regelmatig overwegen of de verwerkte persoonsgegevens nog toereikend, ter zake dienend en noodzakelijk zijn, of dat de gegevens moeten worden verwijderd of geanonimiseerd.

74. Verwerkingsverantwoordelijken moeten eerst en vooral bepalen of ze de persoonsgegevens wel hoeven te verwerken voor hun doeleinden. De verwerkingsverantwoordelijke moet nagaan of de betreffende doeleinden ook kunnen worden verwezenlijkt wanneer er minder persoonsgegevens worden verwerkt, of met behulp van minder gedetailleerde of geaggregeerde persoonsgegevens, of helemaal zonder persoonsgegevens te verwerken[37]. Deze controle moet plaatsvinden voordat er gegevens worden verwerkt, maar kan ook op ieder moment in de verwerkingscyclus worden uitgevoerd. Dit is ook in overeenstemming met artikel 11.

75. Minimale gegevensverwerking kan ook verwijzen naar de mate van identificatie. Indien het voor het doel van de verwerking niet nodig is dat de definitieve gegevensreeks verwijst naar een geïdentificeerd of een identificeerbaar individu (bijvoorbeeld bij statistieken), maar voor de oorspronkelijke verwerking wel (bv. vóór de aggregatie van gegevens), dan moet de verwerkingsverantwoordelijke de persoonsgegevens verwijderen of anonimiseren zodra identificatie niet langer nodig is. Indien verdere identificatie nodig blijft voor andere verwerkingsactiviteiten, moeten persoonsgegevens worden gepseudonimiseerd om de risico's voor de rechten van de betrokkenen te beperken.

76. Belangrijke ontwerp- en standaardinstellingselementen voor minimale gegevensverwerking zijn onder meer:
    - Gegevensvermijding – vermijd de verwerking van persoonsgegevens volledig wanneer dit mogelijk is voor het betreffende doel.
    - Beperking – beperk de hoeveelheid verzamelde gegevens tot wat noodzakelijk is voor het doel.
    - Beperking van toegang – geef de gegevensverwerking zo vorm dat zo weinig mogelijk mensen toegang tot persoonsgegevens nodig hebben om hun werkzaamheden uit te voeren, en beperk de toegang dienovereenkomstig.
    - Relevantie – persoonsgegevens zijn relevant voor de desbetreffende verwerking, en de verwerkingsverantwoordelijke kan deze relevantie aantonen.
    - Noodzakelijkheid – elke categorie van de persoonsgegevens is noodzakelijk voor de gespecificeerde doeleinden en wordt uitsluitend verwerkt indien het niet mogelijk is het doel met andere middelen te bereiken.
    - Aggregatie – gebruik waar mogelijk geaggregeerde gegevens.
    - Pseudonimisering – pseudonimiseer persoonsgegevens zodra het niet langer noodzakelijk is om over rechtstreeks identificeerbare persoonsgegevens te beschikken, en bewaar identificatiesleutels afzonderlijk.
    - Anonimisering en vernietiging – indien persoonsgegevens niet of niet langer noodzakelijk zijn voor het doel, worden deze geanonimiseerd of vernietigd.
    - Gegevensstroom – de gegevensstroom is voldoende doeltreffend, zodat er niet meer kopieën worden gemaakt dan noodzakelijk.

[36] Artikel 5, lid 1, onder c), van de AVG.

[37] Dit staat in overweging 39 van de AVG: "Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt."

- "Stand van de techniek" – de verwerkingsverantwoordelijke past actuele en geschikte technologieën voor gegevensvermijding en minimale gegevensverwerking toe.

Voorbeeld 1

Een boekenwinkel wil de inkomsten verhogen door boeken online te verkopen. De eigenaar van de boekenwinkel wil een gestandaardiseerd formulier opstellen voor de bestelprocedure. Om ervoor te zorgen dat klanten alle gewenste informatie invullen, maakt de eigenaar van de boekenwinkel alle velden in het formulier verplicht (vult de klant niet alle velden in, dan kan de bestelling niet worden geplaatst). De eigenaar van de webshop gebruikt aanvankelijk een standaardcontactformulier, waarin om informatie als de geboortedatum, het telefoonnummer en het thuisadres van de klant wordt gevraagd. Niet alle velden in het formulier zijn echter noodzakelijk voor het doel, namelijk het kopen en leveren van boeken. In dit specifieke geval zijn de geboortedatum en het telefoonnummer van de betrokkene, als deze vooraf voor het product betaalt, niet noodzakelijk voor de aankoop van het product. Dit betekent dat deze velden in het bestelformulier voor het product niet verplicht mogen zijn, tenzij de verwerkingsverantwoordelijke duidelijk kan aantonen dat de informatie om andere redenen noodzakelijk is en deze redenen uiteen kan zetten. Bovendien zijn er situaties waarbij een adres niet noodzakelijk is. Wanneer een klant een e-boek bestelt, kan hij het product bijvoorbeeld rechtstreeks op zijn apparaat downloaden.

De eigenaar van de webshop beslist daarom om twee webformulieren te maken: een voor het bestellen van boeken, met een veld voor het adres van de klant, en een voor het bestellen van e-boeken, zonder een veld voor het adres van de klant.

Voorbeeld 2

Een openbaarvervoersbedrijf wenst statistische informatie te verzamelen op basis van routes van reizigers. Dit is nuttig om juiste keuzen te maken over wijzigingen in tijdschema's van het openbaar vervoer en over goede routebepalingen van de treinen. De reizigers moeten elke keer wanneer zij een vervoersmiddel betreden of verlaten, hun ticket door een kaartlezer halen. Nadat de verwerkingsverantwoordelijke een risicobeoordeling heeft uitgevoerd met betrekking tot de rechten en vrijheden van reizigers in verband met de verzameling van hun reisroutes, stelt hij vast dat het, wanneer reizigers in dunbevolkte gebieden wonen of werken, dankzij de identificatiecode van het ticket mogelijk is hen te identificeren op basis van losse routes. Aangezien het niet noodzakelijk is voor het doel van optimalisatie van de tijdschema's van het openbaar vervoer en de routebepaling van de treinen, bewaart de verwerkingsverantwoordelijke de identificatiecode van het ticket daarom niet. Op het moment dat de reis voorbij is, bewaart de verwerkingsverantwoordelijke alleen de individuele reisroutes, zodat het niet mogelijk is reizen te identificeren die verbonden zijn aan één enkel ticket, maar alleen informatie over afzonderlijke reisroutes.

Indien er alsnog een risico kan bestaan dat een persoon enkel door zijn reisroute in het openbaar vervoer wordt geïdentificeerd, treft de verwerkingsverantwoordelijke statistische maatregelen om het risico te beperken, zoals het weglaten van het begin en het einde van de route.

Voorbeeld 3

Een koerier wenst de doeltreffendheid van zijn leveringen te beoordelen wat levertijden, planning van werkbelasting en brandstofverbruik betreft. Om dit doel te bereiken moet de koerier een aantal persoonsgegevens verwerken die zowel met de werknemers (chauffeurs) als met de klanten (adressen, te leveren artikelen enz.) verband houden. Deze verwerkingsactiviteit houdt risico's in, met betrekking tot zowel toezicht op werknemers, waarvoor specifieke wettelijke waarborgen nodig zijn, als het volgen van de gewoonten van klanten via de kennis van de geleverde artikelen in de loop der tijd. Deze risico's kunnen aanzienlijk worden verminderd met passende pseudonimisering van werknemers en klanten. Met name wanneer pseudonimiseringssleutels regelmatig worden gewisseld en macrogebieden in aanmerking worden genomen in plaats van gedetailleerde adressen, wordt er een doeltreffende vorm van minimale gegevensverwerking nagestreefd en kan de verwerkingsverantwoordelijke zich uitsluitend richten op het leveringsproces en het doel van middelenoptimalisatie, zonder de drempel van het toezicht op gedragingen van individuen (klanten of werknemers) te overschrijden.

Voorbeeld 4

Een ziekenhuis verzamelt gegevens over zijn patiënten in een ziekenhuisinformatiesysteem (elektronisch patiëntendossier). Het ziekenhuispersoneel moet toegang tot patiëntendossiers hebben om goede beslissingen te kunnen nemen met betrekking tot de zorg en behandeling van de patiënten, alsook voor de documentatie van alle uitgevoerde handelingen in het kader van diagnosen, zorg en behandeling. Standaard wordt er enkel toegang verleend aan de zorgverleners die met de behandeling van de betreffende patiënt zijn belast binnen de afdeling waaraan de patiënt is toegewezen. De groep mensen met toegang tot een patiëntendossier wordt uitgebreid als er andere afdelingen of diagnostische eenheden bij de behandeling worden betrokken. Nadat de patiënt is ontslagen en de facturering is afgerond, wordt de toegang beperkt tot een kleine groep medewerkers per afdeling die, na goedkeuring van de betreffende patiënt, reageren op verzoeken om medische informatie of op een uitgevoerd of gevraagd consult van een andere medische dienstverlener.

3.6 Juistheid

77. Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.[38]

78. De vereisten moeten worden gezien in verhouding tot de risico's en de gevolgen van het concrete gebruik van de gegevens. Onjuiste persoonsgegevens kunnen een risico vormen voor de rechten en vrijheden van de betrokkenen, bijvoorbeeld wanneer dit leidt tot een verkeerde diagnose of een onjuiste behandeling van een gezondheidsprotocol, of wanneer een foutieve afbeelding van een persoon ertoe leidt dat beslissingen worden genomen op een verkeerde basis, hetzij manueel, door gebruik van geautomatiseerde besluitvorming, of via kunstmatige intelligentie.

79. Belangrijke ontwerp- en standaardinstellingselementen voor juistheid zijn onder meer:
    - Gegevensbron – bronnen van persoonsgegevens zijn betrouwbaar wat de juistheid van de gegevens betreft.

[38] Artikel 5, lid 1, onder d), van de AVG.

- Mate van nauwkeurigheid – elk element van de persoonsgegevens is zo nauwkeurig als nodig is voor de gespecificeerde doelen.
- Meetbare juistheid – beperk het aantal valse positieven/negatieven, bijvoorbeeld vertekening bij automatische besluitvorming en kunstmatige intelligentie.
- Verificatie – afhankelijk van de aard van de gegevens, in verhouding tot hoe vaak deze kunnen wijzigen, gaat de verwerkingsverantwoordelijke de juistheid van persoonsgegevens bij de betrokkene na, voorafgaand aan en in verschillende fasen van de verwerking (bv. ten aanzien van leeftijdseisen).
- Wissing/rectificatie – de verwerkingsverantwoordelijke wist of rectificeert onjuiste gegevens onverwijld. Hiervoor draagt de verwerkingsverantwoordelijke in het bijzonder zorg wanneer de betrokkenen kinderen zijn of waren en zij later hun persoonsgegevens willen verwijderen.[39]
- Preventie van foutenvermeerdering – verwerkingsverantwoordelijken beperken de gevolgen van een gecumuleerde fout in de verwerkingsketen.
- Toegang – betrokkenen ontvangen informatie over en effectieve toegang tot persoonsgegevens overeenkomstig de artikelen 12 tot en met 15 van de AVG om de juistheid te controleren en waar nodig te rectificeren.
- Voortdurende juistheid – persoonsgegevens zijn in alle fasen van de verwerking juist, en in kritieke fasen worden er nauwkeurigheidstests uitgevoerd.
- Actueel – persoonsgegevens worden geactualiseerd indien dit nodig is voor het doel.
- Gegevensontwerp – gebruik van technologische en organisatorische ontwerpkenmerken om het aantal onjuistheden te verlagen, bijvoorbeeld vooraf bepaalde keuzemogelijkheden bieden in plaats van vrijetekstvelden.

Voorbeeld 1

Een verzekeraar wil kunstmatige intelligentie (KI) gebruiken om profielen te maken van klanten die verzekeringen kopen, als basis voor zijn besluitvorming bij het berekenen van het verzekeringsrisico. Bij het bepalen van de wijze waarop de KI-oplossingen moeten worden ontwikkeld, bepaalt hij de middelen voor de verwerking en houdt hij rekening met gegevensbescherming door ontwerp wanneer hij een KI-toepassing van een leverancier kiest en wanneer hij beslist over de trainingsmethode voor de KI.

Bij het bepalen van de trainingsmethode voor de KI moet de verwerkingsverantwoordelijke over juiste gegevens beschikken om nauwkeurige resultaten te behalen. Daarom moet de verwerkingsverantwoordelijke ervoor zorgen dat de gegevens die voor het trainen van de KI worden gebruikt, juist zijn.

Aangenomen dat de verzekeraar een geldige rechtsgrond heeft om de KI te trainen met behulp van persoonsgegevens uit een grote subset van bestaande klanten, kiest de verwerkingsverantwoordelijke een grote verzameling van die klanten die representatief is voor de bevolking om vertekening te vermijden.

Vervolgens worden de klantgegevens verzameld uit het betreffende gegevensverwerkingssysteem, met inbegrip van gegevens over het soort verzekering, bijvoorbeeld zorgverzekering, woonverzekering, reisverzekering enz., evenals gegevens uit publieke registers waar zij wettige toegang toe hebben. Alle gegevens worden gepseudonimiseerd voordat zij worden overgedragen naar het systeem waarin het KI-model wordt getraind.

[39] Zie overweging 65.

Om ervoor te zorgen dat de gegevens die voor het trainen van de KI worden gebruikt, zo nauwkeurig mogelijk zijn, verzamelt de verwerkingsverantwoordelijke alleen gegevens uit gegevensbronnen met juiste en actuele informatie.

De verzekeraar test of de KI betrouwbaar is en verstrekt zowel tijdens de ontwikkeling ervan als voordat het product uiteindelijk wordt uitgegeven, niet-discriminerende resultaten. Wanneer de KI volledig getraind en operationeel is, gebruikt de verzekeraar de resultaten om de beoordelingen van het verzekeringsrisico te ondersteunen, maar zonder dat hij hierbij uitsluitend op de KI vertrouwt voor zijn beslissing om al dan niet een verzekering te verkopen, tenzij deze beslissing overeenkomstig de uitzonderingen uit artikel 22, lid 2, van de AVG wordt genomen.

Ook evalueert de verzekeraar regelmatig de resultaten van de KI om de betrouwbaarheid te waarborgen en, indien nodig, het algoritme aan te passen.

Voorbeeld 2

De verwerkingsverantwoordelijke is een gezondheidsinstelling die op zoek is naar methoden om de integriteit en juistheid van persoonsgegevens in haar cliëntenregisters te waarborgen.

In situaties waarin twee personen op hetzelfde moment bij de instelling aankomen en dezelfde behandeling ondergaan, bestaat er een risico dat zij met elkaar worden verward, als de enige parameter om hen te onderscheiden de naam is. Om de juistheid te waarborgen heeft de verwerkingsverantwoordelijke voor iedere persoon een unieke identificatiecode nodig, en dus meer informatie dan alleen de naam van de cliënt.

De instelling gebruikt verschillende systemen die persoonlijke informatie van cliënten bevatten, en moet ervoor zorgen dat de informatie met betrekking tot de cliënt in alle systemen en op elk moment correct, nauwkeurig en consistent is. De instelling heeft verschillende risico's geïdentificeerd die zich kunnen voordoen indien informatie wordt gewijzigd in één systeem, maar niet in de andere systemen.

De verwerkingsverantwoordelijke besluit het risico te verminderen door een hashingtechniek toe te passen die kan worden gebruikt om de integriteit van de gegevens in het behandelingsdagboek te waarborgen. Er worden onveranderlijke cryptografische tijdstempels ontwikkeld voor dossiers van het behandelingsdagboek en de bijbehorende cliënt, zodat wijzigingen kunnen worden herkend, met elkaar in verband kunnen worden gebracht en indien nodig kunnen worden gevolgd.

3.7 Opslagbeperking

80. De verwerkingsverantwoordelijke moet ervoor zorgen dat 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.[40]
Het is essentieel dat de verwerkingsverantwoordelijke precies weet welke persoonsgegevens het bedrijf verwerkt en waarom. Het doel van de verwerking vormt het belangrijkste criterium voor de bewaartermijn van de persoonsgegevens.

[40] Artikel 5, lid 1, onder e), van de AVG.

81. Maatregelen en waarborgen ter uitvoering van het beginsel van opslagbeperking vormen een aanvulling op de rechten en vrijheden van de betrokkenen, en in het bijzonder op het recht op wissing en het recht van bezwaar.

82. Belangrijke ontwerp- en standaardinstellingselementen voor opslagbeperking zijn onder meer:
- Verwijdering en anonimisering – de verwerkingsverantwoordelijke beschikt over heldere interne procedures en functionaliteiten voor verwijdering en/of anonimisering.
- Doeltreffendheid van anonimisering/verwijdering – de verwerkingsverantwoordelijke zorgt ervoor dat het niet mogelijk is om geanonimiseerde gegevens opnieuw te identificeren of verwijderde gegevens te herstellen, en hij test of dit mogelijk is.
- Automatisering – verwijdering van persoonsgegevens wordt geautomatiseerd.
- Opslagcriteria – de verwerkingsverantwoordelijke bepaalt welke gegevens en welke bewaartermijn noodzakelijk zijn voor het doel.
- Rechtvaardiging – de verwerkingsverantwoordelijke kan verantwoorden waarom de bewaartermijn noodzakelijk is voor het doeleinde en de betreffende persoonsgegevens en kan de motivering en de rechtsgrond voor de bewaartermijn uiteenzetten.
- Handhaving van beleid inzake bewaring – de verwerkingsverantwoordelijke handhaaft intern beleid inzake bewaring en voert tests uit om na te gaan of de organisatie dit beleid in de praktijk brengt.
- Back-ups/logbestanden – de verwerkingsverantwoordelijke bepaalt welke persoonsgegevens en bewaartermijn noodzakelijk zijn voor back-ups en logbestanden.
- Gegevensstroom – de verwerkingsverantwoordelijke let op de stroom van persoonsgegevens en de opslag van eventuele kopieën daarvan en probeert de tijdelijke opslag hiervan te beperken.

Voorbeeld

De verwerkingsverantwoordelijke verzamelt persoonsgegevens, met als doel van de verwerking om een lidmaatschap te registreren voor de betrokkene. De persoonsgegevens moeten worden verwijderd wanneer het lidmaatschap wordt beëindigd en er geen rechtsgrond is voor verdere opslag van de gegevens.

De verwerkingsverantwoordelijke stelt allereerst een interne procedure op voor bewaring en vernietiging van gegevens. Op grond hiervan moeten werknemers de persoonsgegevens handmatig verwijderen nadat de bewaartermijn is afgelopen. De werknemer volgt de procedure en verwijdert en corrigeert regelmatig de gegevens van alle apparaten en van back-ups, logbestanden, e-mails en andere relevante opslagmedia.

Om de verwijdering doeltreffender en minder vatbaar voor fouten te maken zet de verwerkingsverantwoordelijke vervolgens in plaats daarvan een automatisch systeem op om de gegevens automatisch, op betrouwbare wijze en op regelmatigere basis te verwijderen. Het systeem wordt zo geconfigureerd dat het de gegeven procedure voor gegevensverwijdering volgt, die vervolgens met een vooraf bepaalde regelmatige interval plaatsvindt om persoonsgegevens van alle opslagmedia van het bedrijf te verwijderen. De verwerkingsverantwoordelijke evalueert en test de bewaarprocedure regelmatig en zorgt ervoor dat deze strookt met het actuele bewaarbeleid.

3.8 Integriteit en vertrouwelijkheid

83. Het beginsel van integriteit en vertrouwelijkheid omvat bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging, met behulp van passende technische of organisatorische maatregelen. Voor de beveiliging van persoonsgegevens zijn passende maatregelen nodig die zijn ontworpen om gegevensinbreuken te voorkomen en te beheren, om de gedegen uitvoering van gegevensverwerkingstaken en de naleving van de andere beginselen te waarborgen en om de doeltreffende uitoefening van de rechten van individuen mogelijk te maken.

84. In overweging 78 staat dat een van de DPbDD-maatregelen erin zou kunnen bestaan de verwerkingsverantwoordelijke in staat te stellen om *"beveiligingskenmerken te creëren en te verbeteren"*. Naast andere DPbDD-maatregelen wordt er in overweging 78 gewezen op een verantwoordelijkheid van de verwerkingsverantwoordelijken om voortdurend te beoordelen of zij op elk moment de passende middelen gebruiken voor de verwerking, en om te beoordelen of de gekozen maatregelen de bestaande kwetsbaarheden daadwerkelijk tegengaan. Verder moeten verwerkingsverantwoordelijken regelmatige evaluaties uitvoeren van de informatiebeveiligingsmaatregelen die persoonsgegevens omgeven en beschermen, en van de procedure voor de omgang met gegevensinbreuken.

85. Belangrijke ontwerp- en standaardinstellingselementen voor integriteit en vertrouwelijkheid zijn onder meer:
    - Beheersysteem voor informatiebeveiliging (ISMS) – over operationele middelen beschikken om beleidslijnen en procedures voor informatiebeveiliging te beheren.
    - Risicoanalyse – de risico's beoordelen aan de hand van de beveiliging van persoonsgegevens door na te denken over de gevolgen voor de rechten van individuen, en vastgestelde risico's tegengaan. Ontwikkel en onderhoud voor de risicobeoordelingen een uitgebreid, systematisch en realistisch dreigingsmodel en een analyse van het aanvalsoppervlak van de ontworpen software om de aanvalsvectoren de mogelijkheden om gebruik te maken van zwakke punten en kwetsbaarheden te beperken.
    - Beveiliging door ontwerp – denk bij het ontwerp en de ontwikkeling van het systeem zo vroeg mogelijk na over beveiligingseisen en integreer en verricht voortdurend relevante tests.
    - Onderhoud – evalueer en test software, hardware, systemen, diensten enz. regelmatig om kwetsbaarheden vast te stellen van de systemen die de verwerking ondersteunen.
    - Beheer van toegangscontrole – enkel bevoegde medewerkers voor wie dit noodzakelijk is, hebben toegang tot de persoonsgegevens die zij nodig hebben voor hun verwerkingstaken, en de verwerkingsverantwoordelijke maakt onderscheid tussen de verschillende toegangsrechten van de bevoegde medewerkers.
        - Beperking van toegang (personen) – geef de gegevensverwerking zo vorm dat zo weinig mogelijk mensen toegang tot persoonsgegevens nodig hebben om hun werkzaamheden te kunnen uitvoeren, en beperk de toegang dienovereenkomstig.
        - Beperking van toegang (inhoud) – houd, in het kader van elke verwerkingsactiviteit, de toegang beperkt tot de gegevenskenmerken van de betreffende dataset die nodig zijn voor die activiteit. Beperk de toegang bovendien tot de gegevens die betrekking hebben op de betrokkenen die binnen het mandaat van de betreffende medewerker vallen.
        - Segregatie van toegang – geef de gegevensverwerking zo vorm dat niemand volledige toegang tot alle verzamelde gegevens over een betrokkene nodig heeft, laat staan tot alle persoonsgegevens van een bepaalde categorie betrokkenen.
    - Beveiligde overdrachten – overdrachten zijn beveiligd tegen ongeoorloofde en onbedoelde toegang en wijzigingen.

- Beveiligde opslag – gegevensopslag is beveiligd tegen ongeoorloofde toegang en wijzigingen. Er zijn procedures om het risico van gecentraliseerde of gedecentraliseerde opslag te beoordelen en te bepalen op welke categorieën persoonsgegevens dit van toepassing is. Het is mogelijk dat voor bepaalde gegevens extra beveiligingsmaatregelen nodig zijn of dat bepaalde gegevens van andere moeten worden gescheiden.
- Pseudonimisering – persoonsgegevens en back-ups/logbestanden worden gepseudonimiseerd als een beveiligingsmaatregel om de risico's van potentiële gegevensinbreuken tot een minimum te beperken, bijvoorbeeld door middel van hashing of versleuteling.
- Back-ups/logbestanden – houd back-ups en logbestanden bij voor zover dit noodzakelijk is voor informatiebeveiliging, en gebruik controlesporen en toezicht op gebeurtenissen als routinebeveiligingscontrole. Deze zaken moeten worden beschermd tegen ongeoorloofde en onbedoelde toegang en wijzigingen en moeten regelmatig worden herzien. Incidenten moeten onverwijld worden afgehandeld.
- Rampenherstel/bedrijfscontinuïteit – speel in op de eisen voor rampenherstel en bedrijfscontinuïteit van het informatiesysteem om de beschikbaarheid van persoonsgegevens te herstellen na grote incidenten.
- Bescherming op basis van risico – bescherm alle categorieën persoonsgegevens met maatregelen die passen bij het risico van een beveiligingsinbreuk. Gegevens met bijzondere risico's moeten, indien mogelijk, apart van de rest van de persoonsgegevens worden bewaard.
- Beheer van reactie op veiligheidsincidenten – beschikken over routines, procedures en middelen om gegevensinbreuken op te sporen, in te dammen, te behandelen, te melden en er lering uit te trekken.
- Beheer van incidenten – de verwerkingsverantwoordelijke beschikt over processen voor de omgang met inbreuken en incidenten om het verwerkingssysteem robuuster te maken. Dit omvat meldingsprocedures, zoals het beheer van meldingen (aan de toezichthoudende autoriteit) en informatie (voor betrokkenen).

Voorbeeld

Een verwerkingsverantwoordelijke wil grote hoeveelheden persoonsgegevens uit een medische databank met elektronische (patiënten)dossiers verzamelen op een speciale databankserver binnen het bedrijf, om de verzamelde gegevens te verwerken met het oog op kwaliteitsborging. Het bedrijf heeft beoordeeld dat het routeren van de gegevens naar een server die toegankelijk is voor alle werknemers van het bedrijf, een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Aangezien slechts één afdeling binnen het bedrijf de verzamelde patiëntengegevens hoeft te verwerken, besluit de verwerkingsverantwoordelijke de toegang tot de speciale server te beperken tot medewerkers van die afdeling. Bovendien worden de gegevens, om het risico verder te verkleinen, gepseudonimiseerd voordat zij worden overgedragen.

Om de toegang te regelen en mogelijke schade van malware te verminderen besluit het bedrijf het netwerk op te delen en toegangscontroles in te stellen voor de server. Daarnaast wordt er veiligheidsmonitoring en een indringerdetectie- en -preventiesysteem opgezet en wordt de server afgezonderd van routinegebruik. Er wordt een geautomatiseerd controlesysteem in werking gesteld om toezicht te houden op toegang en wijzigingen. Hieruit worden rapportage en automatische waarschuwingen gegenereerd wanneer bepaalde aan het gebruik gerelateerde gebeurtenissen worden geconfigureerd. De verwerkingsverantwoordelijke zorgt ervoor dat gebruikers uitsluitend toegang hebben als dit voor hen noodzakelijk is en zij over het passende toegangsniveau beschikken. Ongepast gebruik kan snel en eenvoudig worden vastgesteld.

Sommige gegevens moeten worden vergeleken met nieuwe gegevens en moeten daarom drie maanden worden opgeslagen. De verwerkingsverantwoordelijke besluit deze in aparte databanken op dezelfde server op te slaan en hiervoor zowel transparante versleuteling als versleuteling op kolomniveau te gebruiken. Sleutels voor ontcijfering van kolomgegevens worden opgeslagen in speciale beveiligingsmodules die enkel door bevoegd personeel kunnen worden gebruikt, maar hier niet uit kunnen worden gehaald.

Door de behandeling van komende incidenten wordt het systeem robuuster en betrouwbaarder. De verwerkingsverantwoordelijke begrijpt dat er preventieve en doeltreffende maatregelen moeten worden ingebouwd in alle huidige en toekomstige verwerkingsactiviteiten met betrekking tot persoonsgegevens en dat dit bijdraagt aan het voorkomen van dergelijke incidenten inzake gegevensinbreuken in de toekomst.

De verwerkingsverantwoordelijke treft deze veiligheidsmaatregelen om juistheid, integriteit en vertrouwelijkheid te waarborgen, maar ook om de verspreiding van malware door cyberaanvallen te voorkomen en de oplossing op die manier robuust te maken. Robuuste beveiligingsmaatregelen dragen bij aan het vertrouwen van de betrokkenen.

3.9 Verantwoordingsplicht[41]

86. Het beginsel van verantwoordingsplicht houdt in dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van alle bovengenoemde beginselen en deze kan aantonen.

87. De verwerkingsverantwoordelijke moet de naleving van de beginselen kunnen aantonen. Daarbij kan hij aantonen welke gevolgen de genomen maatregelen ter bescherming van de rechten van de betrokkenen hebben en waarom zij passend en doeltreffend worden geacht. Hij kan bijvoorbeeld aantonen waarom een maatregel geschikt is om het beginsel van opslagbeperking op doeltreffende wijze te waarborgen.

88. Om op verantwoorde wijze persoonsgegevens te kunnen verwerken moet de verwerkingsverantwoordelijke niet alleen de nodige kennis hebben, maar ook het vermogen om gegevensbescherming uit te voeren. Dat houdt in dat de verwerkingsverantwoordelijke zijn gegevensbeschermingsverplichtingen op grond van de AVG moet begrijpen en in staat moet zijn deze verplichtingen na te komen.

4 ARTIKEL 25, LID 3: CERTIFICERING

89. Overeenkomstig artikel 25, lid 3, kan een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme worden gebruikt als element om aan te tonen dat aan DPbDD is voldaan. Andersom kunnen documenten die aantonen dat aan DPbDD is voldaan, ook van pas komen in een certificeringsproces. Dit betekent dat, wanneer een verwerkingsactiviteit van een verwerkingsverantwoordelijke of een verwerker overeenkomstig artikel 42 is gecertificeerd, de toezichthoudende autoriteiten hiermee rekening moeten houden bij hun beoordeling inzake naleving van de AVG, in het bijzonder wat DPbDD betreft.

90. Wanneer een verwerkingsactiviteit van een verwerkingsverantwoordelijke of verwerker overeenkomstig artikel 42 is gecertificeerd, zijn de elementen die bijdragen aan het aantonen van de naleving van artikel 25, leden 1 en 2: de ontwerpprocessen, d.w.z. het proces voor het bepalen van de

[41] Zie overweging 74, waar staat dat verwerkingsverantwoordelijken de doeltreffendheid van hun maatregelen moeten aantonen.

middelen voor de verwerking; het bestuur; en de technische en organisatorische maatregelen ter uitvoering van de gegevensbeschermingsbeginselen. De criteria voor de certificering van gegevensbescherming worden bepaald door de certificeringsinstanties of de eigenaren van de certificeringsregelingen en vervolgens goedgekeurd door de bevoegde toezichthoudende autoriteit of het EDPB. Voor meer informatie over certificeringsmechanismen verwijzen we de lezer naar de richtsnoeren van het EDPB over certificering[42] en andere relevante richtsnoeren, zoals gepubliceerd op de website van het EDPB.

91. Zelfs wanneer een verwerkingsactiviteit overeenkomstig artikel 42 is gecertificeerd, heeft de verwerkingsverantwoordelijke nog steeds de verantwoordelijkheid om de naleving van de DPbDD-criteria uit artikel 25 voortdurend te monitoren en te verbeteren.

5 HANDHAVING VAN ARTIKEL 25 EN GEVOLGEN

92. De toezichthoudende autoriteiten kunnen de naleving van artikel 25 beoordelen volgens de procedures die in artikel 58 zijn vermeld. De bevoegdheden tot het nemen van corrigerende maatregelen zijn vermeld in artikel 58, lid 2, en omvatten waarschuwen, berispen, gelasten om de rechten van de betrokkene na te leven, de verwerking te beperken of te verbieden, administratieve geldboetes enz.

93. DPbDD vormt verder een factor bij het bepalen van de hoogte van geldboetes voor inbreuken op de AVG, zie artikel 83, lid 4.[43] [44]

6 AANBEVELINGEN

94. Hoewel dit in artikel 25 niet rechtstreeks aan bod komt, worden verwerkers en producenten ook erkend als belangrijke actoren die DPbDD mogelijk maken. Zij moeten zich ervan bewust zijn dat verwerkingsverantwoordelijken persoonsgegevens uitsluitend mogen verwerken met systemen en technologieën waarin gegevensbescherming is ingebouwd.

95. Bij het verwerken namens verwerkingsverantwoordelijken of het aanbieden van oplossingen aan verwerkingsverantwoordelijken moeten verwerkers en producenten hun deskundigheid gebruiken om vertrouwen op te bouwen en hun klanten, met inbegrip van kmo's, te begeleiden bij het ontwerpen of aankopen van oplossingen waarmee gegevensbescherming in de verwerking wordt ingebouwd. Dat houdt ook in dat het ontwerp van producten en diensten moet stroken met de behoeften van verwerkingsverantwoordelijken.

96. Bij de uitvoering van artikel 25 mag niet uit het oog worden verloren dat het belangrijkste ontwerpdoel de *doeltreffende uitvoering* van de beginselen en de *bescherming* van de rechten van betrokkenen in de passende maatregelen voor de verwerking is. Om de ingebruikname van DPbDD mogelijk te maken

[42] EDPB. "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation". Versie 3.0 van 4 juni 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

[43] In artikel 83, lid 2, onder d), van de AVG is bepaald dat bij het vaststellen van de oplegging van geldboetes voor inbreuken op de AVG naar behoren rekening moet worden gehouden met *"de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32"*.

[44] Meer informatie over boetes is te vinden in: Groep gegevensbescherming artikel 29. "Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679". WP 253 van 3 oktober 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – goedgekeurd door het EDPB.

en te ondersteunen raden wij verwerkingsverantwoordelijken, producenten en verwerkers de volgende zaken aan:

- Verwerkingsverantwoordelijken moeten aan gegevensbescherming denken vanaf de *eerste fasen* waarin zij een verwerkingsactiviteit plannen, zelfs al vóór het moment waarop zij de middelen van de verwerking bepalen.
- Wanneer de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming (DPO) heeft, moedigt het EDPB de actieve betrokkenheid van de DPO bij de aanbestedings- en ontwikkelingsprocedures aan, evenals bij de gehele levenscyclus van de verwerking.
- Een verwerkingsactiviteit kan *gecertificeerd* zijn. De mogelijkheid om een verwerkingsactiviteit te laten certificeren is van toegevoegde waarde voor een verwerkingsverantwoordelijke wanneer deze moet kiezen tussen verschillende verwerkingssoftware, -hardware, -diensten en/of -systemen van producenten of verwerkers. Producenten moeten er daarom naar streven DPbDD aan te tonen in de levenscyclus van hun ontwikkeling van een verwerkingsoplossing. Een certificeringszegel kan betrokkenen ook helpen te kiezen tussen verschillende goederen en diensten. De mogelijkheid om een verwerking te laten certificeren kan een concurrentievoordeel opleveren voor producenten, verwerkers en verwerkingsverantwoordelijken, en vergroot zelfs het vertrouwen van betrokkenen in de verwerking van hun persoonsgegevens. Wordt er geen certificering aangeboden, dan moeten verwerkingsverantwoordelijken op zoek gaan naar andere *waarborgen* dat producenten of verwerkers de DPbDD-vereisten naleven.
- Verwerkingsverantwoordelijken, verwerkers en producenten moeten hun verplichtingen in acht nemen om kinderen tot 18 jaar en andere kwetsbare groepen van specifieke bescherming te voorzien bij de naleving van DPbDD.
- Producenten en verwerkers moeten ernaar streven de uitvoering van DPbDD mogelijk te maken, om het de verwerkingsverantwoordelijke gemakkelijker te maken de verplichtingen uit artikel 25 na te komen. Verwerkingsverantwoordelijken mogen op hun beurt geen producenten of verwerkers kiezen die geen systemen aanbieden die de verwerkingsverantwoordelijke in staat stellen artikel 25 na te leven of hem daarbij ondersteunen, aangezien verwerkingsverantwoordelijken rekenschap moeten afleggen over de gebrekkige uitvoering daarvan.
- Producenten en verwerkers moeten een actieve rol spelen om ervoor te zorgen dat er wordt voldaan aan de criteria voor de “stand van de techniek”, en zij moeten verwerkingsverantwoordelijken in kennis stellen van alle wijzigingen aan de “stand van de techniek” die invloed kunnen hebben op de doeltreffendheid van de maatregelen die zij hebben ingevoerd. Verwerkingsverantwoordelijken moeten deze vereiste als een contractuele clausule opnemen om ervoor te zorgen dat zij op de hoogte blijven.
- Het EDPB raadt verwerkingsverantwoordelijken aan te eisen dat producenten en verwerkers aantonen hoe hun hardware, software, diensten of systemen de verwerkingsverantwoordelijke in staat stellen de verantwoordingsplicht na te leven in overeenstemming met DPbDD, bijvoorbeeld door gebruik te maken van kernprestatie-indicatoren om aan te tonen dat de maatregelen en waarborgen doeltreffend zijn als het gaat om de uitvoering van de beginselen en rechten.
- Het EDPB wijst op de behoefte aan een geharmoniseerde aanpak om de beginselen en rechten doeltreffend uit te voeren, en moedigt verenigingen of instanties die gedragscodes opstellen

in overeenstemming met artikel 40, aan om hierin ook sectorspecifieke richtsnoeren voor DPbDD op te nemen.

- Verwerkingsverantwoordelijken moeten billijk zijn voor de betrokkenen en transparant over de manier waarop zij doeltreffende uitvoering van DPbDD beoordelen en aantonen, net zoals zij naleving van de AVG aantonen in het kader van het verantwoordingsbeginsel.
- Privacybevorderende technologieën (PET's) die volwaardige maturiteit hebben bereikt, kunnen worden ingezet als maatregel overeenkomstig de DPbDD-vereisten als dit passend is binnen een risicogebaseerde aanpak. PET's dekken op zichzelf niet per definitie de verplichtingen uit artikel 25. Verwerkingsverantwoordelijken moeten beoordelen of de maatregel passend en doeltreffend is voor de uitvoering van de gegevensbeschermingsbeginselen en de rechten van betrokkenen.
- Voor bestaande legacysystemen gelden dezelfde DPbDD-verplichtingen als voor nieuwe systemen. Als legacysystemen niet al aan DPbDD voldoen en er geen veranderingen kunnen worden doorgevoerd om dit te bewerkstelligen, voldoet het legacysysteem simpelweg niet aan de verplichtingen uit de AVG en mag het niet worden gebruikt om persoonsgegevens te verwerken.
- Artikel 25 verlaagt de eisendrempel voor kmo's niet. De volgende zaken kunnen kmo's helpen te voldoen aan artikel 25:
    - Voer vroegtijdig risicobeoordelingen uit.
    - Begin met kleine verwerkingen en voer later de omvang en complexiteit op.
    - Probeer DPbDD-garanties te krijgen van producenten en verwerkers, zoals certificeringen en naleving van gedragscodes.
    - Kies partners met een goede staat van dienst.
    - Praat met gegevensbeschermingsautoriteiten.
    - Lees richtsnoeren van gegevensbeschermingsautoriteiten en het EDPB.
    - Houd u aan gedragscodes, indien deze beschikbaar zijn.
    - Win professionele hulp en advies in.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)