UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

GDPR en privacy by design/default

Sibel Seker

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

2020
2021

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.

UHASSELT
KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

Faculteit Rechten

master in de rechten

Masterthesis

GDPR en privacy by design/default

Sibel Seker

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

Masterscriptie

“GDPR en privacy by design & default”

Prof. Dr. Ken Andries

Academiejaar 2020-2021

Sibel Seker

1437464

Dankwoord

Deze masterproef vormt het sluitstuk van mijn rechtenopleiding aan de Universiteit Hasselt. Een masterproef schrijven is niet gemakkelijk en vraagt veel tijd en inspanning. Zonder enkele personen in mijn omgeving, had ik deze scriptie nooit kunnen voltooien. Graag neem ik even de tijd om deze personen te bedanken.

Eerst en vooral wil ik mijn promotor Prof. dr. Ken Andries bedanken. Hij was een zeer goede begeleider en stuurde mij in de juiste richting daar waar nodig was. Zijn feedback was cruciaal om het juiste onderzoek te verrichten.

Een speciaal woord van dank gaat uit naar mijne echtgenoot Coskun Uzbas. Daar waar ik vaak hele dagen doorwerkte, bood hij zijn hulp aan op mentaal, financieel en huishoudelijk vlak.

Vervolgens wil ik mijn familieleden bedanken. Mijn ouders en schoonouder stonden altijd klaar om te helpen en zonder hun steun zou deze masterproef er niet geweest zijn.

Tot slot wil ik mijn geode vriendin Sultana Azizi bedanken voor de grote steun in deze moeilijke tijden.

Sibel Seker
12 mei 2021

Woordenlijst met afkortingen

AEPD	Spanish Data Protection Agency
AVG	Algemene Verordening gegevensbescherming
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
CalOPPA	California Online Privacy Protection Act
CNIL	Commission nationale de l'informatique et des libertés
DPbDD	Data protection by design and default
DPIA	Data protection impact assessment
DPO	Data protection officer
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EVRM	Europees Verdrag voor de Rechten van de Mens
GDPR	General Data Protection Regulation
GEB	Gegevensbeschermingseffectbeoordeling
ICO	Information Commissioners Office
KPI	Kritieke prestatie indicatoren
PET	Privacy enhancing technology
PbD	Privacy by design
VWEU	Verdrag betreffende de werking van de Europese Unie

Inhoudsopgave

1. Inleiding

Vandaag de dag is het internet een onmiskenbaar instrument geworden. We houden contact met familie en vrienden, delen filmpjes met elkaar, doen aankopen via websites enzovoort. Dit is de uitvinding die ons allemaal dichterbij brengt en waarmee we op een verre afstand in contact blijven zonder ons zorgen te maken over onze persoonlijke gegevens. We hebben deze gegevens namelijk in vertrouwen ingegeven. Het internet is tenslotte een veilige haven als je maar een gebruiker bent. Of toch niet?

Nog maar enkele jaren geleden kwam het Cambridge Analytica schandaal naar boven. Cambridge Analytica was een Brits databedrijf dat onder andere datamining, data-analyse en direct marketing bundelde met strategische communicatie voor verkiezingscampagnes. Facebook pleegde echter een inbreuk door een te laks beleid te hebben en persoonsgegevens onvoldoende te beschermen. Meer dan 50 miljoen mensen werden gedupeerd. Namen, e-mailadressen, telefoonnummers en wachtwoorden werden zo openlijk blootgesteld. Facebook is bovendien niet het enige bedrijf dat persoonsgegevens onvoldoende beschermt.[1]

Het is duidelijk dat de economische integratie gezorgd heeft voor aanzienlijke toename van de grensoverschrijdende stromen van gegevens. Zowel ondernemingen als autoriteiten krijgen steeds meer zicht op onze persoonsgegevens. Door het internet, de snelle technologische ontwikkelingen en de globalisering, kampen we met nieuwe uitdagingen in onze huidige maatschappij. Dankzij de technologie kunnen bedrijven en overheden meer dan ooit gebruik maken van onze gegevens. Zulke ontwikkelingen vereisen een krachtig en streng kader om persoonsgegevens extra te beschermen. De Algemene Verordening Gegevensbescherming moet dit krachtig kader bieden. Het is bijgevolg interessant om de privacy en gegevensbescherming in de EU in haar hele context te onderzoeken. Dit zal onderzocht worden in het tweede hoofdstuk.[2]

Opmerkelijk is dat de Europese wetgever verwerkingsverantwoordelijken verplicht om passende technische en organisatorische maatregelen te nemen via het concept van 'privacy by design en default'. Deze verplichting moet de beginselen inzake de gegevensverwerking en de rechten en vrijheden van personen waarborgen. Het derde hoofdstuk zal bijgevolg worden toegewijd aan dit concept. Het eerste deel zal zich specifiek focussen op de privacy by design en het tweede op de privacy by default.[3]

Nieuwe regels brengen nieuwe vragen en uitdagingen met zich mee. De regels inzake privacy by design en default kunnen onder andere uitdagingen vormen voor producenten en data-analisten. Het

[1] M. KAMINSKY, "Facebook Faces Class Action Over Security Breach That Affected 50 Million Users", https://www.forbes.com/sites/michellefabio/2018/09/30/facebook-faces-class-action-over-security-breach-that-affected-50-million-users/?sh=6b9984777b6c.
[2] Overweging 6 AVG.
[3] Artikel 25 AVG.

is hierom dat in het vierde hoofdstuk kort wordt ingegaan op deze uitdagingen.

De AVG bepaalt bovendien in haar verordening dat lidstaten zelf toezichthoudende overheden moeten aanduiden.[4] Deze instanties kunnen inbreuken zwaar beboeten en verdere schendingen voorkomen. In het laatste hoofdstuk zal bijgevolg onderzocht hoe de toezichthoudende autoriteiten dit in Engeland en in Frankrijk regelen. Ook zal de privacywetgeving van de Amerikaanse Staat California interessant zijn voor dit onderzoek. California is namelijk de eerste Staat in Amerika waar een specifieke privacywet werd ingevoerd.[5]

Deze masterproef zal uiteindelijk worden afgesloten met een laatste deel waarin een algemene conclusie wordt geformuleerd.

1.1 Onderwerp

Dit onderzoek richt zich op de General Data Protection Regulation of de Algemene Verordening Gegevensbescherming. Beginnend met de analyse van de factoren die geleid hebben tot het huidig wetgevend kader, zal dit worden aangevuld met een korte bespreking van de GDPR. Vervolgens zal het concept van 'privacy by design en default' worden uiteengezet en gekeken worden welke uitdagingen dit met zich meebrengt. Bovendien zal besproken worden hoe privacyorganen, zoals het ICO en de CNIL de privacywetgeving afdwingen. Tot slot is het wenselijk om de GDPR te vergelijken met privacyregelgeving buiten de EU. Hiervoor wordt de 'GDPR' van de staat California kort geanalyseerd om te kunnen concluderen of de AVG consumentvriendelijker is.

1.2 Probleemstelling

De privacyrichtlijn van 1995 was sterk verouderd en achterhaald. Door nieuwe technologieën maken ondernemingen en overheden steeds meer gebruik van persoonsgegevens die bovendien onderling steeds vaker werden uitgewisseld. De wetgever werd zich bewust van digitalisering, technologische ontwikkelingen en de nieuw opkomende elektronische communicatie waardoor een 'vernieuwing' van de richtlijn noodzakelijk werd. Hierdoor werd in 2016 de nieuwe privacywetgeving, nl. de GDPR of de GDPR goedgekeurd en trad deze in werking in 2018. Desondanks de GDPR al enkele jaren aanwezig is en het aan de hand van artikel 25 verplichtingen stelt aan verwerkingsverantwoordelijken, heeft de gegevensbeschermingsautoriteit al veel bedrijven teruggefloten. Waarom hebben bedrijven moeilijkheden met 'GDPR-compliant' zijn? Biedt de bepaling van 'privacy by design en default' onvoldoende duidelijkheid?

1.3 Onderzoeksvragen

De centrale onderzoeksvraag van deze scriptie luidt als volgt: 'In welke mate biedt de GDPR en de privacy by design en default voldoende bescherming?' De centrale onderzoeksvraag zal beantwoord worden door middel van 3 deelvragen.

De eerste deelvraag heeft betrekking op het huidig regime van de bescherming van gegevensverwerking. Er zal gekeken worden naar de ontstaansgeschiedenis en naar de huidige

[4] Art. 51 AVG
[5] X, "The California Privacy Rights Act of 2020", 2020, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/.

wetgeving van de Europese Unie, waarbij ook een koppeling naar het nationaal recht van België wordt gemaakt.

De tweede deelvraag handelt over het GDPR-compliant worden en de problemen die het met zich meebrengt. Het concept van 'privacy by design en default' zal hier besproken worden, waarna de uitdagingen van deze bepaling worden toegelicht.

De derde deelvraag heeft betrekking op de evaluatie van de wetgeving. De GDPR beschermt persoonsgegevens door middel van nieuwe en strengere regels. De vraag is echter of deze regels gekwalificeerd kunnen worden als consumentvriendelijker. Voor deze onderzoeksvraag zal niet enkel naar de regelgeving binnen de EU worden gekeken, maar ook hierbuiten.

1.4 Relevantie

Dit onderzoek is relevant aangezien het twee belangrijke redenen betreft.

Gezien de GDPR op 2018 in werking trad en er tot op heden nog steeds inbreuken worden gepleegd, is het zinvol om de bepaling van privacy by design en default te onderzoeken. Door een heldere analyse van dit concept krijgen verwerkingsverantwoordelijken meer duidelijkheid over de implementatie ervan, zodat onwenselijkheden in de toekomst worden vermeden.

Bovendien betreft de bescherming van persoonsgegevens een globale kwestie. Het bespreken van een de 'Amerikaanse GDPR', de privacywetgeving van California, kan ons een andere visie opleveren.

1.5 Beperkingen

Dit onderzoek beperkt zich in eerste instantie tot de General Data Protection Regulation en de nationale wetgeving. Er zal niet zozeer worden ingegaan op andere Verordeningen. Omwille van de grote omvang beperk ik mij dus tot het onderzoeken binnen deze grenzen. Echter, om te kunnen besluiten of de Europese wetgeving consumentvriendelijk is, zal er rechtsvergelijkend onderzoek gedaan worden met de privacywetgeving van California, Verenigde Staten van Amerika. Een rechtsvergelijkend perspectief met andere continenten zoals Azië wordt buiten beschouwing gehouden.

1.6 Onderzoeksmethode

Het onderzoek wordt opgedeeld in 4 hoofdstukken. Alle delen zullen worden behandeld aan de hand van een klassiek literatuur- en bronnenonderzoek. Voornamelijk zal er gefocust worden op primaire bronnen zoals de Algemene Verordening Gegevensbescherming. Aangezien dit onderzoek gericht is op een recent geïntroduceerde concept van 'privacy by design en default', zal er in mindere mate gefocust worden op Europese rechtspraak.

Aangezien in het laatste hoofdstuk het Verenigd Koninkrijk, Frankrijk en de Amerikaanse staat California ter sprake komt, zal dit hoofdstuk hoofdzakelijk bestaan uit Europese en Amerikaanse onlinebronnen.

2. Privacy en gegevensbescherming

2.1. Europees regelgevend kader

2.1.1 Inleiding

Om een duidelijk beeld te vormen over de totstandkoming van de regelgeving die vandaag de dag bestaat, zal als inleidend gedeelte het Europees regelgevend kader inzake de privacy en gegevensbescherming kort worden besproken.

2.1.2 EVRM, VWEU, en het Handvest van de grondrechten van de EU

Artikel 8 EVRM geeft ieder individu het recht op bescherming en eerbiediging van zijn privé- en familieleven, de eigen woning en het briefgeheim. Dankzij de evolutie in de rechtspraak van het Europees Hof, valt de bescherming van persoonsgegevens nu ook onder artikel 8 van het Europees Verdrag van de Rechten van de Mens. Dit wil zeggen dat dat onwettige inmenging in de privacy een inbreuk vormt op een grondrecht.[6] De Raad van Europa nam de bescherming van personen ten opzichte van de geautomatiseerde verwerking van gegevens uitdrukkelijk op in Conventie 108, waarbij de verplichtingen betreffende de verwerking van persoonsgegevens in richtlijn 95/46/EG werden vastgelegd.[7] Het verdrag werd geratificeerd door alle EU-lidstaten.[8] Het recht op gegevensbescherming werd ook in artikel 16 van het VWEU vermeld.[9] In 2000 werd de bescherming van persoonsgegevens afzonderlijk opgenomen in artikel 8 van het Handvest van de Europese Unie als fundamenteel grondrecht.[10]

2.1.3 Richtlijn en e-privacybescherming

Tot 2016 was Richtlijn 95/46/EG het belangrijkste instrument in de Europese Unie die bepalingen bevatte inzake de bescherming van persoonsgegevens.[11] De Richtlijn werd in België omgezet in de wet van 11 december 1998.[12] Recentelijk werd deze vervangen door de GDPR of de AVG.[13]

De e-Privacyrichtlijn trad in werking op 12 juli 2002 en werd gewijzigd in 2009.[14] De richtlijn regelt de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer specifiek

---

[6] Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 4 november 1950, *BS* 19 augustus 1955.

[7] Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.

[8] Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, *BS* 30 december 1993.

[9] Art. 16, 1ste lid VWEU.

[10] Art. 8, 1ste lid Handvest van de grondrechten van de Europese Unie van 7 december 2000, *Pb.L.* 18 december 2000, afl. 346, 10.

[11] Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.

[12] Wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *BS* 3 februari 1999.

[13] Verord.Raad nr. 2016/679, 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, *Pb.L.* 4 mei 2016, afl. 119, 1.

[14] Richtl.EP en Raad nr. 2002/58/EG, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37.

in de elektronische communicatiediensten. Op 1 januari 2017 werd voorgesteld om deze richtlijn nogmaals te herzien. De e-Privacyverordening is tot op heden nog steeds niet in werking getreden. Dit omdat de EDPB verbeterpunten heeft aangehaald met betrekking tot het voorstel. De verordening zou er eind 2021 of begin 2022 moeten zijn.[15]

2.1.4 GDPR of Algemene Verordening Gegevensbescherming

In januari 2012 werd een voorstel ingediend om Richtlijn 95/46/EG te herzien.[16] Na een lang proces werd in mei 2016 de privacyrichtlijn vernieuwd en uitgevaardigd onder de General Data Protection Regulation.[17] De GDPR of de AVG dat op 25 mei 2018 in werking trad, is een verordening dat regels omvat inzake het beheer en de bescherming van persoonlijke gegevens van EU-onderdanen. Opvallend koos de Europese wetgever deze keer niet voor een richtlijn, maar voor een krachtiger instrument, een verordening. Bijgevolg zijn de bepalingen van de verordening rechtstreeks van toepassing, zonder dat er eerst een omzetting moet plaatsvinden.[18]

De hervorming van de vorige regelgeving was een gevolg van verschillende factoren. Allereerst, was er het wenselijk karakter om nationale wetgeving te harmoniseren op vlak van bescherming van de persoonsgegevens van EU-onderdanen. De Europese wetgever wou de burger meer transparantie bieden en controle geven over zijn/haar persoonlijke gegevens.[19] Een tweede reden voor de hervorming waren de vele technologische ontwikkelingen en de globalisering van de digitale economie.[20] Zoals eerder vermeld, werden de regels inzake bescherming van persoonsgegevens geregeld door Richtlijn 95/45/EC.[21] Deze richtlijn dateert van 1995 en was sterk verouderd en achterhaald. Door nieuwe technologieën maakten ondernemingen en overheden steeds meer gebruik van persoonsgegevens die bovendien steeds vaker worden uitgewisseld. De wetgever werd zich bewust van digitalisering, technologische ontwikkelingen en die nieuw opkomende elektronische communicatie waardoor een vernieuwing van de richtlijn noodzakelijk werd.[22] Het finaal doel van de GDPR of de AVG is het bieden van meer rechtszekerheid voor zowel natuurlijke personen als ondernemingen en overheden. [23]

Desondanks de GDPR al in 2016 werd uitgevaardigd, is het GDPR-compliant zijn nog steeds een discussiepunt in veel bedrijven, waar vaak te veel aandacht wordt besteed aan formele vereisten zoals het aanpassen van contracten en algemene voorwaarden en te weinig aandacht wordt besteed aan praktische aspecten. De vereiste aanpassingen van bedrijfsprocessen moeten namelijk ook

[15] Autoriteit Persoonsgegevens, "EDPB: voorstel ePrivacy Verordening moet beter", geraadpleegd op 29 maart 2021, https://autoriteitpersoonsgegevens.nl/nl/nieuws/edpb-voorstel-eprivacy-verordening-moet-beter (consultatie 29 maart 2021).
[16] Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens betreffende het vrij verkeer van die gegevens, 25 januari 2012, COM(2012)11 def – 2012/0011 (COD).
[17] A. FOCQUET, en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 3.
[18] Verord.Raad nr. 2016/679, 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, *Pb.L.* 4 mei 2016, afl. 119, 1 (hierna AVG).
[19] Overweging 3 AVG.
[20] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 5.
[21] Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.
[22] Overweging 6 en 7 AVG.
[23] Unizo, "GDPR: de nieuwe Europese privacyregels", geraadpleegd op 5 maart 2021, https://www.unizo.be/system/files/downloads/andere/uzo-6118-snelwijzer-gdpr.pdf

gebeuren binnen specifieke diensten en niveaus. Het GDPR-compliant worden, bestaat voornamelijk uit het informeren, opleiden en implementeren. Tegelijk bestaat het ook uit controleren op permanente basis, aanpassen en bestraffen. [24] De GDPR verbiedt de verwerking en verzameling van persoonsgegevens niet. De verordening omschrijft de regels over hoe ze verzamelt, bijgehouden, gebruikt en verwijderd worden.[25]

In dit hoofdstuk wordt kort teruggeblikt naar verschillen met de oude regelgeving, waarna de basisbegrippen van de GDPR zullen worden toegelicht.

Om als onderneming of overheid GDPR-compliant te zijn, moeten de nodige maatregelen en waarborgen genomen worden in het begin van het hele verwerkingsproces en tijdens de levenscyclus van de verwerking. Dit wordt ook wel privacy by design en default genoemd. Hier wordt in het volgend hoofdstuk verder op ingegaan.[26]

2.1.4.1 Wat is er nu precies veranderd?

De belangrijkste nieuwigheden die door de AVG werden ingevoerd zijn de volgende[27]:

- de informatieplicht aan betrokkenen is uitgebreid

- er zijn strengere vereisten voor de 'toestemming' van de betrokkene als rechtsgrond

- verplichtingen voor zowel verantwoordelijken als verwerkers werden ingevoerd

- een interne documentatieverplichting

- de principes van 'Privacy by Design' (door ontwerp) en 'Privacy by Default' (door standaardinstellingen) werden geïntroduceerd

- de verplichte aanstelling van een 'Functionaris voor Gegevensbescherming' ofwel de 'Data Protection Officer' in bepaalde gevallen

- de verplichting van een Privacy Impact Assessment (PIA) in bepaalde gevallen

- de introductie van enkele nieuwe rechten van betrokkenen (zoals het recht om vergeten te worden)

- de verplichting om gegevenslekken te melden in bepaalde gevallen

- de mogelijkheid om 'GDPR-compliance' aan te tonen door middel van certificering of een erkende gedragscode.

[24] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 4.
[25] Art. 4 AVG.
[26] Artikel 25 AVG.
[27] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 13.

2.1.4.2 Zijn er afwijkende bepalingen voor lidstaten?

Alhoewel de GDPR streeft naar harmonisatie tussen de EU-lidstaten, laat het de lidstaten vrij om op enkele vlakken al dan niet strengere nationale bepalingen vast te stellen. Lidstaten kunnen afwijkende bepalingen treffen voor volgende gevallen[28]:

- de verwerking van gegevens van overledenen

- de leeftijd waarop een minderjarige geldige toestemming kan geven in het kader van diensten die door een informatiemaatschappij worden aangeboden. De leeftijd kan van 16 jaar naar 13 jaar verlaagd worden.

- de verwerking van persoonsgegevens in het kader van het arbeidsrecht

- de verwerking van genetische gegevens, biometrische gegevens of gezondheidsgegevens en van het nationaal identificatienummer

- de voorwaarden waarin een DPO verplicht moet worden aangesteld

- de soorten bevoegdheden van de toezichthoudende autoriteit

2.2 De GDPR

2.2.1 Toepassingsgebied

2.2.1.2 Territoriaal toepassingsgebied

Het territoriaal toepassingsgebied is ten opzichte van de vroegere richtlijn sterk uitgebreid. De GDPR is namelijk van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke in of buiten de Unie. Om te bepalen of de verordening toepasselijk is voor een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, moet de verwerking verband houden met enkele factoren. Enerzijds kan het verband hebben met het aanbieden van goederen of diensten aan betrokkenen in de Europese unie, zonder rekening te houden met het feit of het goed betaald is. Anderzijds kan het ook verband hebben met het monitoren van het gedrag van een EU-onderdaan, zolang dit binnen de Unie gebeurt. Bovendien is de GDPR ook van toepassing als de verwerkingsverantwoordelijke niet binnen de Unie is gevestigd, maar in een gebied waar het nationaal recht toepasselijk is krachtens het internationaal publiekrecht.[29]

2.2.1.3 Materieel toepassingsgebied

Om te bepalen of een overheid of onderneming onder de GDPR valt, moet er gekeken worden naar het toepassingsgebied van de verordening. Het materieel toepassingsgebied van de verordening bevat de geheel of gedeeltelijk geautomatiseerde verwerking, waaronder ook de verwerking van

[28] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 6.
[29] Art. 3 AVG.

persoonsgegevens valt die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De verschillende criteria worden in later verder uitgelegd.[30]

2.2.1.4 Personeel toepassingsgebied

De GDPR bevat geen specifieke bepaling over het personeel toepassingsgebied. Dit sluit echter niet uit dat dit niet afgeleid kan worden uit de overwegingen.[31] De 'verwerkingsverantwoordelijke' en 'verwerker' zijn terugkerende termen in de overwegingen en bepalingen. Ze zijn van cruciaal belang, aangezien de verordening op hun toepasselijk is. De verwerkingsverantwoordelijke stelt het doel en de middelen voor de verwerking vast, terwijl de verwerker de persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke. De bescherming geschiedt ten opzichte van de 'betrokkene'. Dit is alle informatie over een geïdentificeerde of identificeerbaar persoon. Dit kan zowel op een directe als indirecte manier aam de hand van een identificator of meerdere elementen.[32] De beginselen inzake de verwerking van persoonsgegevens worden hieronder verder uitgeklaard.

2.2.2 Beginselen inzake verwerking van persoonsgegevens

a) persoonsgegeven

Om de beginselen inzake verwerking te benaderen, moeten eerst de definities worden uitgelegd en toegepast. De Europese wetgever heeft een bijzonder ruime definitie geschonken aan 'persoonsgegeven'. De AVG omschrijft het als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon[33]

Dit begrip omvat vier belangrijke elementen; alle informatie, over, geïdentificeerde of identificeerbare, natuurlijke persoon.[34]
Het eerste element omvat 'alle informatie'. Dit slaat op alle informatie ongeacht de inhoud, vorm of de aard. Ongeacht of de informatie objectief of subjectief is en of het nu betrekking heeft op het persoonlijk of het professioneel leven, het allemaal valt onder informatie. Om terug te komen op de vorm van de informatie, moet er rekening gehouden worden met het feit dat de relevante informatie kan verschijnen in tekst, beeld, geluid, papier, elektronisch of in code. Dit is van belang voor dit onderzoek, aangezien we in het tweede hoofdstuk specifieke maatregelen en waarborgen hieromtrent onderzoeken.[35]

Het tweede element heeft betrekking op het begrip 'over'. Dit slaat of het feit dat de relevante informatie betrekking moet hebben op de natuurlijke persoon, dat zowel direct of indirect kan gebeuren. Wanneer de informatie verwijst naar de identiteit, kenmerken of gedrag van de betrokkene, zal dit een directe wijze zijn. Wanneer het gaat over het doel (betrokkene beoordelen,

[30] Art. 2; art. 4 AVG.
[31] Overweging 23 AVG.
[32] Art. 4 1ste lid AVG.
[33] Art. 4 1ste lid AVG.
[34] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 5.
[35] *Ibid*., 7.

anders behandelen of willen beïnvloeden) of over de impact (groot of klein) zal dit een indirecte wijze uitmaken.[36]

Het derde element omvat de termen 'geïdentificeerd of identificeerbaar'. Wanneer een persoon onderscheiden wordt van andere personen binnen die groep, spreekt men van 'geïdentificeerd'. De verordening omschrijft dat de onderscheiding gebeurt aan de hand van een identificator. De GDPR verwijst expliciet naar naam, identificatienummer, locatiegegevens of een online identificator. Verder, is het mogelijk dat een of meerdere elementen die kenmerkend zijn voor de persoon en waardoor de persoon kan worden herkend (fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit) hieronder vallen. 'Identificeerbaar' is de persoon die onderscheiden kan worden van de groep, maar dat nog niet is gebeurd.[37]

Het vierde element heeft betrekking op de 'natuurlijke persoon'. Dit wil zeggen dat de informatie moet gaan om het individu, ongeacht de nationaliteit of de vestiging en in deze situatie dus elke EU-onderdaan.[38]

b) verwerking

Artikel 4 omschrijft de verwerking van persoonsgegevens als '*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*'. Wanneer de verwerking dus geheel of gedeeltelijk al dan niet geautomatiseerd verloopt, valt dit onder het toepassingsgebied van de verordening.[39]

c) de beginselen

Artikel 5 van de GDPR omvat de concrete beginselen inzake de verwerking van persoonsgegevens. Deze beginselen zijn van cruciaal belang, aangezien de verwerkingsverantwoordelijke deze regels strikt moet naleven om de bescherming van persoonsgegevens te eerbiedigen en dit moet kunnen verantwoorden o.b.v. de verantwoordingsplicht.[40] Persoonsgegevens moeten[41]:

a) Verwerkt worden op een rechtmatige, behoorlijke en transparante wijze.

b) Verwerkt worden voor welbepaalde, uitdrukkelijke en gerechtvaardigde doeleinden (doelbinding)

c) Toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij verwerkt worden ('minimale gegevensverwerking').

[36] *Ibid*., 8-9.
[37] *Ibid*., 10-11.
[38] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 13.
[39] Art. 4 2de lid AVG.
[40] Art. 5 2de lid AVG.
[41] Art. 5 1ste lid AVG.

d) Juist en actueel zijn, waarbij alle redelijke maatregelen moeten worden genomen om persoonsgegevens te wissen of te verbeteren die niet juist zijn (juistheid).

e) Worden bewaard op een wijze dat de betrokken persoon niet langer identificeerbaar is dan voor de doelen waarvoor de gegevens verwerkt worden. De gegevens kunnen langer worden bewaard in naam van het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden mits de voorwaarden van opslagbeperking worden gerespecteerd (opslagbeperking).

f) Verwerkt worden aan de hand van passende technische en organisatorische maatregelen zodat een passende beveiliging gewaarborgd kan worden (integriteit en vertrouwelijkheid).

Leidende principes voor de eerbiediging van deze beginselen zijn de 'data protection by design' en de 'data protection by default' die in artikel 25 van de verordening zijn opgenomen. Door middel van technische en organisatorische maatregelen en waarborgen, moeten de beginselen worden geïmplementeerd in het verwerkingsproces. Hier wordt in het volgend hoofdstuk dieper op ingegaan.

2.2.3 Rechtmatigheid van de verwerking

Zoals hierboven besproken, moet elke verwerking van persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze gebeuren. Bovendien moet het voldoende duidelijk zijn voor welke doeleinden de verwerking gebeurt. De gegevensverzameling blijft beperkt tot wat noodzakelijk is voor de daartoe geselecteerde doeleinden, tenzij de verwerkingsverantwoordelijke dit kan verantwoorden door een van de volgende factoren:[42]

a) De betrokkene heeft expliciet toestemming verleend

b) De verwerking is noodzakelijk voor de uitvoering van de overeenkomst

c) De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust

d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen.

e) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang

f) De verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde

2.2.3.1 Toestemming

De verordening omschrijft de toestemming van de betrokkene als; 'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van

[42] Art. 6 AVG.

persoonsgegevens aanvaardt'[43][44]

- de betrokkene moet geïnformeerd zijn: hiermee wil de wetgever ervoor zorgen dat de betrokkene zeer duidelijk weet waarvoor hij toestemming geeft en dat hij behoorlijk geïnformeerd is op het ogenblik dat hij akkoord gaat.

- de toestemming moet vrij zijn: de wetgever heeft dit geïmplementeerd om te vermijden dat de toestemming van de betrokkene wordt afgedwongen. Bovendien mag de betrokkene op ieder ogenblik zijn of haar toestemming intrekken zonder een sanctie op te lopen.

- de toestemming moet specifiek zijn: hiermee wil de wetgever voorkomen dat het geven van de toestemming verwerkt zou worden in vorm van een algemene aanvaarding, zoals de aanvaarding van algemene voorwaarden.

- de toestemming moet ondubbelzinnig zijn: de betrokkene moet zijn of haar toestemming geven door middel van een verklaring of een duidelijke actieve handeling. De wetgever heeft dit ingevoerd om te voorkomen dat de toestemming door middel van een passieve houding wou kunnen worden gegeven.

In de verordening worden ook andere aandachtspunten vermeld die belangrijk zijn voor de toestemming voor gegevensverwerking. Zo moet de verantwoordelijke op ieder ogenblik kunnen aantonen dat de betrokkene effectief een geldige toestemming gegeven heeft voor de verwerking van zijn/haar gegevens. De verantwoordelijke zal hier het bewijs van moeten leveren en bijhouden zoals bijvoorbeeld een kopie van een ondertekend formulier. Een tweede belangrijk aandachtspunt is dat de er in het kader van een schriftelijke verklaring dat ook andere onderwerpen bevat, het verzoek in begrijpelijk en gemakkelijk toegankelijke vorm en in een eenvoudige taal gepresenteerd wordt zodat waarbij er een duidelijk onderscheid is tussen de verschillende onderwerpen. Een derde aandachtspunt is dat de toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel hebben. Wanneer de verwerking meerdere doeleinden heeft, moet voor elk doeleinde afzonderlijke toestemming gegeven worden. Stel dat een betrokkene een fitness-app wil gebruiken. De applicatie zal zo toestemming vragen voor het verwerken van de gezondheidsgegevens maar ook voor het gebruik van het e-mail-adres voor het versturen van reclame of andere dingen. Een vierde aandachtspunt is in het kader van een rechtstreeks aanbod van onlinediensten aan een kind. De gegevensverwerking zal rechtmatig zijn wanneer het kind ten minste 13 jaar is. Wanneer het kind jonger is, dan zal de toestemming gegeven moeten worden door het ouderlijk gezag. Een vijfde aandachtspunt is in het kader van de ondubbelzinnige toestemming. Wanneer de ondubbelzinnige toestemming niet voldoende is, zal de uitdrukkelijke toestemming worden gevraagd. Dit vindt meestal plaats wanneer het betrekking heeft op gevoelige gegevens (artikel 9 AVG), strafrechtelijke gegevens (artikel 10 Kaderwet Privacy), de geautomatiseerde besluitvorming (artikel 22 AVG), en een internationale doorgifte van persoonsgegevens naar een 'niet-adequaat' land (artikel 49 AVG).[45]

[43] Art. 4 11e lid AVG.
[44] Art. 7 AVG.
[45] Overweging 32 AVG.

De schriftelijke en ondertekende verklaring is niet de enige manier om uitdrukkelijke toestemming te geven voor het verwerken van gegevens (tenzij het betrekking heeft op strafrechtelijke gegevens). Een betrokkene kan bijvoorbeeld door middel van een elektronisch formulier, e-mail, scan van een document, een elektronische handtekening ook uitdrukkelijk toestemming voor de verwerking van zijn of haar gegevens. Mondeling zou ook kunnen, maar het bewijs ervan blijft moeilijk.[46]

2.2.3.2 De verwerking is noodzakelijk voor de uitvoering van de overeenkomst

Gegevensverwerking van klanten of werknemers moet gebeuren op een wijze dat strikt noodzakelijk is voor de uitvoering van de overeenkomst. De verwerking mag niet verder gaan dan dat.[47] Een onderneming mag zo de gegevens gebruiken van klanten om leveringen te kunnen uitvoeren, maar mag deze gegevens bijvoorbeeld niet voor andere zaken gebruiken, zoals het versturen van leesbrieven. Dit is tenslotte niet strikt noodzakelijk voor de uitvoering van de overeenkomst. Op alle andere acties is de rechtsgrond dus niet van toepassing, tenzij het doel is om de uitvoering van de overeenkomst te verzekeren. Officiële herinneringen sturen voor de betaling van een factuur, kan dus wel gezien worden als argument voor de uitvoering van de overeenkomst.[48]

2.2.3.3 De verwerking is noodzakelijk voor de naleving van een wettelijke bepaling

De wettelijke verplichting is een vaak voorkomende rechtsgrond voor de verwerking van persoonsgegevens.[49] Werkgevers moeten bijvoorbeeld salarisgegevens van hun werknemers doorgeven aan instanties zoals de sociale zekerheid of de belastingdienst. Ook zijn financiële instellingen bijvoorbeeld verplicht om verdachte transacties te melden aan de bevoegde autoriteiten. Dit in het kader van de antiwitwaswetgeving. De wettelijke verplichting die als rechtsgrond gebruikt wordt om de gegevens door te geven, moet natuurlijk zijn vastgelegd in de EU- of nationale wetgeving.[50]

2.2.3.4 De afweging van gerechtvaardigde belangen

WP29, nu de EDPB, heeft in haar advies een belangrijke methodologie ingevoerd voor de belangenafweging. Vooreerst zal er een beoordeling van het gerechtvaardigd belang van de verantwoordelijke gemaakt moeten worden. De uitoefening van een fundamenteel recht, zoals het recht op informatie, het algemeen belang en bedrijfsbelangen zullen overwogen worden. Ten tweede zal er gekeken moeten worden naar de gevolgen voor de betrokkene. De ernst van de gevolgen voor de betrokkene is een van de vele elementen waarmee rekening gehouden wordt wanneer de afweging gemaakt wordt. Ten derde zal er een voorlopig balans worden opgemaakt, waarbij men ongewenste gevolgen wil verminderen. Tot slot kunnen er aanvullende waarborgen gegeven worden om ongewenste gevolgen voor de betrokkene te verminderen. Gebruikers kunnen zich bijvoorbeeld aan de verwerking onttrekken door een opt-out of er kan gebruikt gemaakt worden van

[46] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 45.
[47] Art. 6 1ste lid AVG.
[48] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 40.
[49] Art. 6 1ste lid AVG.
[50] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 45.

pseudonimisering en encryptie.[51]

2.2.5 Verplichtingen voor de verwerker en/of verwerkingsverantwoordelijke

2.2.5.1 Functionaris voor gegevensbescherming

De GDPR verplicht in bepaalde gevallen ondernemingen om een DPO aan te stellen.[52] De DPO is de centrale figuur voor de implementatie van de GDPR en draagt de verantwoordelijkheidsplicht. De DPO oftewel de data protection officier zorgt voor de communicatie tussen de autoriteiten en de betrokkenen. Alhoewel sommige ondernemingen vrijgesteld zijn van het aanstellen van een DPO, is het daarom niet minder nuttig om een verantwoordelijke voor gegevensbescherming aan te stellen.[53]

a) DPO-plicht

De GDPR verplicht zowel overheidsinstanties en organen als ondernemingen in bepaalde omstandigheden om een DPO aan te stellen. Dit wanneer deze als hoofdactiviteit en op grote schaal strafrechtelijke en/of gevoelige informatie verwerken of betrokkenen observeren op regelmatige/stelselmatige basis.[54] Wat betreft de strafrechtelijke en gevoelige gegevens, is er weinig uitlegging vereist. Het is duidelijk dat bijvoorbeeld ziekenhuizen (die nu eenmaal gevoelige informatie bezitten) een DPO aanstellen om de gegevensbescherming te garanderen. Wat betreft de verwerking op regelmatige of stelselmatige basis bedoelt de Europese wetgever dat het op een periodieke en georganiseerde/gestructureerde basis moet gaan. Dit is bijvoorbeeld zo wanneer er gebruik gemaakt wordt van een bewakingsfirma, maar ook wanneer ondernemingen zich bezighouden met traceren en profileren, locatietracering, risicobeoordeling op basis van profilering, telecommunicatiediensten en slimme apparaten, ... Het is bovendien niet noodzakelijk dat het om gevoelige of strafrechtelijke informatie moet gaan, het regelmatig en stelselmatig karakter is voldoende.[55]

De gegevensverwerking op 'grote schaal' moet worden geïnterpreteerd op basis van overweging 91 van de verordening. Er moet worden gekeken naar een aantal factoren zoals het aantal betrokkenen, de duur van de gegevensverwerking, de hoeveelheid persoonsgegevens en de geografische omvang. Wat betreft de hoofdactiviteit van de onderneming, moet er worden gekeken of de verwerking op zich de commerciële activiteit vormt of dat de gegevensverwerking een onlosmakelijk onderdeel van die activiteit vormt.[56] Een voorbeeld hiervan is dat een ziekenhuis als hoofdactiviteit medische zorg biedt, maar als onderdeel hiervan medische gegevens van de betrokkene moet verwerken. Dit valt dus ook onder dit criterium.[57]

b) Vrijwillige DPO-aanstelling

[51] Art. 6 1ste lid AVG; S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 45.
[52] Art. 37 AVG.
[53] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 111.
[54] Art. 37 1ste lid AVG.
[55] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 112.
[56] Overweging 91 AVG.
[57] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 113.

Ondernemingen die niet verplicht zijn om een Data Protection Officer aan te stellen, kunnen dit op vrijwillige basis toch best doen. De GDPR moet tenslotte nageleefd worden en toezicht op de naleving kan latere complicaties voorkomen. Het is dus aangeraden op proactief en niet reactief te zijn.[58] Wanneer ondernemingen niet zo ver willen gaan, kunnen ze een andere status geven aan de verantwoordelijke voor de gegevensverwerking, zoals 'Privacy Manager' of 'Informatieveiligheidsconsulent'.[59]

2.2.5.2 Gegevensbeschermingseffectbeoordeling

Een gegevensbeschermingseffectbeoordeling is een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Deze beoordeling gebeurt door de verwerkingsverantwoordelijke wanneer de verwerking, in het bijzonder waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden, potentieel een hoog risico bevat voor de rechten en de vrijheden van de betrokkenen.[60] Een GEB of een DPIA is dus een proces waarbij risico's worden ingeschat en maatregelen worden bepaald om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en risico's te helpen beheren voor de rechten en vrijheden van natuurlijke personen.[61]

De verordening omschrijft in bepaalde gevallen de verplichting om een gegevenbeschermingseffectbeoordeling uit te voeren.[62] De AVG bepaalt dat ondernemingen in een van de drie gevallen een GEB uitvoeren[63];

a) "een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen";

b) "grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10"; of

c) "stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten"

2.2.6 Sancties

Opmerkelijk is dat er in de verordening verregaande controle- en sanctioneringsbevoegdheden zijn toegevoegd, terwijl voorheen autoriteiten geen sanctionerende bevoegdheden hadden. Ook krijgen toezichthoudende autoriteiten een aantal onderzoeksbevoegdheden, waaronder de bevoegdheden om corrigerende maatregelen te nemen en administratieve boetes op te leggen. Administratieve boetes kunnen worden opgelegd rekening houdend met de voorwaarden in artikel 83 GDPR. De

[58] CAVOUKIAN, A., "Privacy by Design : The 7 Foundational Principles Information and Privacy Commissioner of Ontario", 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[59] A. FOCQUET en E. DECLERCK, *Gegevensbescherming in de praktijk*, Antwerpen, Intersentia, 2019, 114.
[60] Art. 35 1ste lid AVG.
[61] X, "Gegevensbeschermingseffectbeoordeling: Aanbeveling van de Privacycommissie", 2018, https://www.gdprbelgium.be/nl/nieuws/gegevensbeschermingseffectbeoordeling-aanbeveling-van-de-privacycommissie.
[62] Art. 35 3de lid AVG.
[63] Art. 35 AVG.

boetes kunnen zeer hoog lopen, dit met de bedoeling om instanties die niet GDPR-conform zijn, af te schrikken.[64]

2.3. Nationaal regelgevend kader: België

2.3.1 Inleiding

Na de inwerkingtreding van de GDPR, heeft België zijn nationaal recht in overeenstemming gebracht met de verordening. De overeenstemming gebeurde in 2 stappen. Allereerst werd de Privacycommissie omgevormd tot de GBA oftewel de Gegevensbeschermingsautoriteit. Vervolgens werd de vroegere Privacywet van 8 december 1992 opgeheven en werd de wet van 30 juli 2018 betreffende de bescherming van natuurlijk personen met betrekking tot de verwerking van persoonsgegevens geïntroduceerd (supra).[65]

2.3.2 AVG-uitvoeringswetten

Twee 'AVG-uitvoeringswetten' werden door het Belgisch parlement aangenomen. Enerzijds is er de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en anderzijds de Wet van 5 september 2018 tot oprichting van het Informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679.8. De eerste wet (wet van 30 juli 2018) wordt ook wel de "Kaderwet Privacy" genoemd. Materiele afwijkingen van en aanvullingen op de AVG worden in deze kaderwet behandelt. Allereerst verlaagt de Belgische wetgever de leeftijd van 16 tot 13 jaar waarop een minderjarige toestemming kan geven in het kader van diensten van informatiemaatschappijen. Ten tweede bevat de kaderwet ook specifieke bepalingen betreffende de verwerking van strafrechtelijke, genetische, biometrische of gezondheidsgegevens en de verwerking van persoonsgegevens door overheden en verschillende overheidsorganen. Ten derde zorgde de kaderwet voor de oprichting van een 'informatieveiligheidscomite' die de rol van sectorale comites overneemt. Deze maakten voorheen deel uit van de Privacycommissie. Het informatieveiligheidscomite is in het bijzonder bevoegd voor de toegang tot overheidsdatabanken en de uitwisseling van persoonsgegevens tussen overheden onderling en tussen overheden en de privésector. Verder wijzigt de wet ook nog andere bepalingen, maar die zijn minder relevant voor dit onderzoek.

Implementatie

Wat betreft de implementatie van de GDPR-verordening, keurde het Parlement een kaderwet goed dat betrekking had op twee Europese teksten. In deze kaderwet werd geregeld in welke mate de verordening een beoordelingsmarge toekent aan de lidstaten. Vervolgens geeft deze kaderwet uitvoering aan de bepalingen van de EU-richtlijn 2016/6809 dat de bescherming voorziet van persoonsgegevens door wetshandhavingsinstanties. Grotendeels hebben de Belgische kaderwet en de Europese regelgeving dezelfde inhoud. Enkel daar waar er enige appreciatiemarge is toegelaten,

[64] Art. 83 AVG.
[65] X, "Privacycommissie wordt Gegevensbeschermingsautoriteit", 2018, https://www.eubelius.com/nl/nieuws/privacycommissie-wordt-gegevensbeschermingsautoriteit-0.

zijn er kleine verschillen (supra).[66]

2.3.3 GBA

Het Belgisch parlement keurde op 3 december 2017 de GBA-wet tot instelling van de GBA als de opvolger/vervanger van de Privacycommissie goed. Met deze wet werd de Privacycommissie hervormd tot de GBA en kon het zo zijn taken uitvoeren overeenkomstig de GDPR-verordening. In vergelijking met de vroegere functie, vervulde de Commissie vooral een adviserende rol, terwijl de GBA een actieve functie zal hebben. Het is juist het doel om de GBA een echte toezichthoudende autoriteit te laten worden dat bevoegdheden zal hebben op het gebied van onderzoek en vervolging. De GBA heeft zo het recht om inbreuken op de verwerking van persoonsgegevens te melden aan de gerechtelijke autoriteiten.[67] Het kan ook zelf rechtsvorderingen instellen op basis van artikel 7 van de GBA-wet. De GBA heeft hiernaast ook nog ander bijzondere taken die in de wet zijn opgenomen.[68]

3. Privacy by design and default

3.1. Ontstaansgeschiedenis

In het verleden werden privacy en gegevensbescherming beschouwd als een wettelijke naleving dat beperkt was tot het formeel proces van een lang privacy-beleid. In zo'n beleid werden mogelijke incidenten gedekt en toekomstige schade aan eigen belangen beperkt of geminimaliseerd. Voor veel ondernemingen en organisaties was de gegevensbescherming dus schone schijn, waarbij er zeer weinig impact was op de organisatorische doelstellingen en praktijken, als voor de bescherming van de persoonsgegevens.[69]

De moeilijkheid inzake de uitvoerbaarheid van juridische principes en de noodzaak voor een echt multidisciplinair aanpak om privacyproblemen te vermijden, zorgde voor een kloof tussen enerzijds een juridische compliance-discipline beheert door advocaten en anderzijds een dynamisch innovatieproces aangestuurd door business managers en ingenieurs. Deze laatste zijn tenslotte eindverantwoordelijken voor het ontwerp en de implementatie van de processen en systemen, die de functionering van de organisatie sturen.[70]

Technologieontwikkeling was niet enkel de oorzaak voor bezorgdheden rondom privacy, maar het werd ook een deel van de oplossing. Verbeteringen en bijdragen in communicatietechnologie, IT-beveiliging, anonieme communicatie en cryptografie ontwikkelden stilaan meer, nu beter bekend als Privacy Enhancing Technologies (PET's).[71] PET's, zoals toegangsbeveiliging en versleuteling, zijn

---

[66] X, "Privacycommissie wordt Gegevensbeschermingsautoriteit", 2018, https://www.eubelius.com/nl/nieuws/privacycommissie-wordt-gegevensbeschermingsautoriteit-0.
[67] Art. 6 GBA-wet.
[68] X, "Privacycommissie wordt Gegevensbeschermingsautoriteit", 2018, https://www.eubelius.com/nl/nieuws/privacycommissie-wordt-gegevensbeschermingsautoriteit-0.
[69] EDPS, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 3, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
[70] EDPS, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 3-4, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf
[71] Ministerie van binnenlandse zaken en Koninkrijksrelaties, "Privacy Enhancing Technologies - Witboek voor beslissers", december 2004, 13, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/technologie/witboek_pet.pdf.

hulpmiddelen en oplossingen die in informatiesystemen worden opgenomen om privacyrisico's van betrokkenen te minimaliseren.[72]

Oorspronkelijk werd de term "privacy by design" gebruikt door Ann Cavoukian, die werkzaam was als informatie- en privacycommissaris in Ontario, Canada. In haar bijdrage schreef ze over 7 fundamentele principes m.b.t PbD.[73] Ten eerste legde ze de nadruk op de noodzaak om proactief en preventief te zijn in plaats van reactief. Zo moet er rekening gehouden worden met de privacyvereisten vanaf de ontwerpfase en dat gedurende de volledige gegevenslevenscyclus van de verwerking, waardoor privacy-invasieve gebeurtenissen voorkomen worden. Ten tweede zou er maximale bescherming moeten zijn door gegevens automatisch te beschermen in een bepaald IT-systeem of bedrijfspraktijk. Wanneer de betrokkene niets doet, moet de privacy dus te allen tijde beschermd blijven, beter bekend als 'data protection by default'. Ten derde moet PbD ingebed zijn in het ontwerp en de architectuur van IT-systemen en bedrijfspraktijken. De bescherming moet een integraal onderdeel zijn van het systeem, zonder dat er afbreuk gedaan wordt aan de functionaliteit ervan. Ten vierde probeert PbD alle legitieme belangen en doelstellingen te behartigen op een positieve win-win manier, waarbij er een evenwicht is tussen privacy en veiligheid. Ten vijfde moeten sterke beveiligingsmaatregelen essentieel zijn voor de privacy van begin tot eind. De privacy moet dus gewaarborgd worden gedurende de hele levenscyclus van de verwerking. Ten zesde streeft PbD naar zichtbaarheid en transparantie. De PhD moet alle belanghebbenden verzekeren dat de verwerking volgens de beloften en doelstellingen gebeurt, onderworpen aan de onafhankelijke verificatie. Als laatste principe wordt het respect voor de privacy van de betrokkene benadrukt. Ontwerpers en operators moeten de belangen van het individu hoog in het vaandel houden door bepaalde maatregelen te nemen. Strikte standaardinstellingen, passende kennisgeving en gebruiksvriendelijke opties zijn hier voorbeelden van.[74]

Om terug te komen op het tweede fundamentele principe, wordt duidelijk vermeld dat persoonlijke gegevens automatisch moeten worden beschermd in een IT-systeem of bedrijf. Wanneer de betrokkene niets doet, moet de privacy dus te allen tijde beschermd blijven. Het is een automatisch, ingebouwd systeem dat als standaard dient. Dit principe is de operationele definitie van 'Privacy by Default'. Het individu draagt niet de last voor de gegevensbescherming wanneer deze gebruik maakt van een dienst of product. Er is geen behoefte aan een actieve handeling, waardoor dus automatisch het grondrecht op privacy en bescherming van persoonsgegevens wordt gegarandeerd.[75]

[72] Justitia, "Privacy by design", https://www.justitia.nl/privacy/privacy-by-design (consultatie 25 maart 2021).
[73] Information and Privacy Commissioner of Ontario, "Privacy by Design: "seven foundational principles", januari 2018, https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.
[74] A. CAVOUKIAN, "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D", 2010, https://link.springer.com/article/10.1007/s12394-010-0062-y ; A. CAVOUKIAN, "Privacy by Design : The 7 Foundational Principles Information and Privacy Commissioner of Ontario", 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[75] A. CAVOUKIAN, "Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", 2010, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

Beginnende elementen van PbD kunnen terug gevonden worden in de vorige privacyregelgeving.[76] De Europese wetgever benadrukte dat de bescherming van de rechten en vrijheden van betrokkenen zowel bij het ontwerpen als bij de uitvoering van de verwerking van persoonsgegevens passende technische maatregelen vergt. De lidstaten hadden de taak om toe te zien op de naleving van de maatregelen door verwerkingsverantwoordelijken, zodoende er een passend niveau van veiligheid bereikt wordt. De stand van de techniek, de kosten van de uitvoering, de risico's van de verwerking en de aard van de te beschermen gegevens zijn elementen waarmee er rekening gehouden werd. Deze elementen komen ook terug in de AVG.[77]

De Artikel 29 Werkgroep, nu de EDPB, vereiste de Europese Commissie in 2009 dat bij de hervorming van de privacyrichtlijn het principe van PbDD moest worden opgenomen.[78] De WP29 benadrukte dat ondernemingen, publieke sectoren en betrokkenen niet in staat zijn om zelf relevante maatregelen te treffen om gegevens te beschermen en dat hierdoor applicaties en systemen ingebed moeten zijn met bescherming door standaardinstellingen. De verplichting zou dus zowel voor verwerkingsverantwoordelijken moeten gelden, alsook voor systeemontwikkelaars en producenten.[79]

Op gebied van juridische, technologische en conceptuele ontwikkeling heeft de PbD een aanzienlijke vooruitgang geboekt. Het is echter nog ver verwijderd van zijn volledige potentieel betreffende de bescherming van de fundamentele grondrechten van het individu. Het is hierdoor dat de EDPS[80] relevante ontwikkelingen en inspanningen aanraadt en dat de EDPB uitgebreide richtlijnen voorziet.[81]

3.2. De EDPS

De EDPS of de Europese Toezichthouder voor gegevensbescherming is een onafhankelijke instelling van de Europese Unie dat in 2004 werd opgericht.[82] De toezichthouder ziet erop toe dat communautaire instellingen en organen bij de verwerking van persoonsgegevens de fundamentele rechten en vrijheden van natuurlijke personen, met name het recht op de persoonlijke levenssfeer respecteren.[83] De EDPS is naast het toezien op de naleving van de verordening ook belast met het

[76] Overweging 46 Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.
[77] Art. 25 AVG.
[78] Artikel 29 Werkgroep, "The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 december 2009, nr. 168, 13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.
[79] EDPS, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 5, https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf
[80] European Data Protection Supervisor, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 1, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
[81] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[82] Europese Unie, "Europese Toezichthouder voor gegevensbescherming (EDPS)", https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_nl (consultatie 1 april 2021).
[83] Art. 41 2de lid Verord.EP en Raad nr. 45/2001, 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *PB.L.* 12 januari 2001, afl. 8, 1.

verstrekken van advies aan de communautaire instellingen en organen en aan alle betrokkenen inzake de verwerking van persoonsgegevens. Het behandelen van klachten, het adviseren van nationale overheden en het opvolgen van nieuwe technologieën zijn enkele taken en bevoegdheden die in de verordening worden opgesomd.[84]

In bepaalde gevallen voorziet de verordening een raadplegingsplicht voor. Zo moeten communautaire instellingen en organen de Europese Toezichthouder voor gegevensbescherming inlichten wanneer zij inzake de verwerking van persoonsgegevens administratieve maatregelen opstellen, waarbij een communautaire instelling of orgaan is betrokken.[85] Vervolgens moet ook de Europese Commissie de EDPS raadplegen wanneer ze een wetgevingsvoorstel aanneemt inzake de bescherming van de fundamentele rechten en vrijheden van personen.[86]

De EDPS werd in december 2014 samen met de Assistant Supervisor benoemd en belast met de specifieke taak om constructief en proactief te zijn. Een jaar later publiceerde de EDPS een strategie voor een termijn van vijf jaar. In deze strategie werd onder andere uiteengezet hoe ze hun specifieke taken zullen uitvoeren. Het EDPS schreef in 2018 een voorlopig advies m.b.t 'data protection by design en default'[87], dat door de EDPB verder werd toegelicht in specifieke richtlijnen.[88] Het advies van de EDPS werd opgesteld om bewustmaking te bevorderen, een relevant debat te promoten en om nodige acties te laten ondernemen. Het onderzoekt de historische ontwikkeling van 'data protection by design and default' en hun vertaling in 'privacy-engineering' methodologieën en technologieën die de privacy verbeteren.[89]

3.3. De EDPB

De EDPB of het Europees Comité voor gegevensbescherming is een onafhankelijk Europees orgaan dat in 2018 werd opgericht. Het Comité heeft de taak om toezicht te houden op de naleving van Algemene Verordening Gegevensbescherming. Het verleent geen individueel, maar wel algemeen advies omtrent de AVG door middel van richtlijnen, aanbevelingen en goede werkwijzen te voorzien. Ze neemt overeenstemmingsrichtlijnen aan en adviseert de Europese Commissie over alle kwesties inzake de gegevensbescherming. Bovendien stimuleert De EDPB de nationale

---

[84] Art. 46-47 Verord.EP en Raad nr. 45/2001, 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *PB.L.* 12 januari 2001, afl. 8, 1.

[85] Artikel 28 1ste lid Verord.EP en Raad nr. 45/2001, 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *PB.L.* 12 januari 2001, afl. 8, 1.

[86] Artikel 28 2de lid Verord.EP en Raad nr. 45/2001, 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *PB.L.* 12 januari 2001, afl. 8, 1.

[87] EDPS, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 1, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[88] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 1https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[89] EDPS, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 4, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf

gegevensbeschermingsautoriteiten om samen te werken zodat informatie en goede werkwijzen gedeeld kunnen worden.[90]

De EDPB bestaat uit vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten en de EVA-EER landen als de Europese Toezichthouder voor gegevensbescherming (EDPS). Het Comité heeft haar zetel in Brussel, waar alle activiteiten en vergaderingen plaatsvinden. Enkele leidende beginselen van de EDPB zijn onder andere onafhankelijkheid, onpartijdigheid, samenwerking en transparantie.[91]

3.3.1. Inleiding

Snelle technologische ontwikkelingen en globalisering hebben geleid tot nieuwe uitdagingen voor de bescherming van persoonsgegevens. Ondernemingen en overheden maken meer dan ooit gebruik van persoonsgegevens door deze te verzamelen en te delen.[92] Bewust van deze ontwikkelingen, richtte de Europese wetgever een krachtig en coherenter kader op, gesteund door een strenge handhaving.[93]

Zo schrijft de Europese wetgever passende technische en organisatorische maatregelen voor zodat voorschriften door verwerkingsverantwoordelijken worden nageleefd en de rechten en vrijheden van betrokkenen worden beschermd. De verwerkingsverantwoordelijke moet de naleving kunnen aantonen door interne beleidsmaatregelen te nemen en die toe te passen. Deze maatregelen moeten voldoen aan de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen.[94]

Ongeacht de grootte of de complexiteit van de verwerking, de PbDD is een verplichting voor alle verwerkingsverantwoordelijken. De gegevensbescherming van artikel 25 kan echter enkel gewaarborgd worden wanneer de verwerkingsverantwoordelijke de beginselen en de rechten en vrijheden begrijpt.[95]

3.3.2. Analyse van artikel 25

De principes van 'data protection by design and protection by default' of 'gegevensbescherming door ontwerp en door standaardinstellingen' zijn termen die expliciet genoemd worden in de verordening.[96] Om de vereisten te kunnen begrijpen, zullen de twee concepten worden geanalyseerd. Deze zijn complementair en versterken elkaar. Desondanks de vereiste hetzelfde is voor elke

[90] Europese Unie, "Europees Comité voor gegevensbescherming (EDPB)", https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_nl (consultatie 1 april 2021).
[91] EDPB, "European Data Protection Board: wie zijn wij", https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_nl (consultatie 2 april 2021).
[92] Overweging 6 AVG.
[93] Overweging 7 AVG.
[94] Overweging 78 AVG; art. 25 AVG.
[95] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[96] Overweging 78 AVG.

organisatie of onderneming, kan de complexiteit van de implementatie van DPbDD verschillen afhankelijk van het individueel verwerkingsproces.[97]

Artikel 25 luidt als volgt;

> *1. "Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen."*
>
> *2. "De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt."*
>
> *3. "Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan."*

3.3.3. Toepassingsgebied

De vereisten van artikel 25 richten zich op de implementatie van de principes door verwerkingsverantwoordelijken.[98] Andere spelers, zoals verwerkers en producenten die niet rechtstreeks worden genoemd in het artikel, kunnen deze richtsnoeren ook nuttig vinden om hun onderneming GDPR compliant te maken.[99] De verplichtingen zijn bovendien ook van toepassing voor verwerkingssystemen die al bestonden voordat de AVG in werking trad. De kern van de bepaling is

[97] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 5-6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[98] Dezelfde interpretatie geldt voor Art. 20 Richtl.EP en Raad nr. 2016/680, van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad; art. 27 Verord.EP en Raad 2018/1725 van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG.

[99] Overweging 78 AVG 'de stand van de techniek'.

om ervoor te zorgen dat de gegevensbescherming passend en effectief gebeurt, waarbij verwerkingsverantwoordelijken moeten kunnen aantonen dat passende maatregelen en waarborgen effectief en doeltreffend zijn.[100]

3.3.4. Art. 25 lid 1 AVG: PRIVACY BY DESIGN

Data protection by design of gegevensbescherming door ontwerp, is het idee om al in een zeer vroeg stadium gegevens te beschermen door middel van een technisch en organisatorische omgang af te dwingen.[101] Vanaf de ontwikkeling van producten of diensten zal er aandacht besteed worden aan de bescherming van gegevens. De verwerkingsverantwoordelijke zal zo moeten afwegen of de verwerking wel degelijk noodzakelijk is. Wanneer er wel degelijk gegevens verwerkt moeten worden, kan de verwerkingsverantwoordelijke deze beveiligen door middel van pseudonimisering, encryptie of access control. Dataminimalisatie verplicht de verantwoordelijke bovendien om enkel datgeen wat noodzakelijk is te verwerken. Faciliteren van de rechten van de persoon en geregelde bewaartermijnen zijn ook van groot belang om privacy-proof te zijn. Indien de verwerking van de gegevens niet noodzakelijk is, kan er eventueel wel gewerkt worden met geanonimiseerde gegevens.[102]

Pseudonimiseren is het verwerken van persoonsgegevens op een bepaalde wijze zodat de gegevens niet meer gekoppeld kunnen worden aan de betrokkene, zonder dat er aanvullende gegevens worden gebruikt en op voorwaarde dat deze aanvullende gegevens apart bewaard worden en technische en organisatorische maatregelen om te vermijden dat persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.[103] De AVG maakt een duidelijk onderscheid tussen pseudonimisering en anonimisering. Dat laatste is wanneer er anonieme gegevens worden gebruikt of wanneer persoonsgegevens zodanig anoniem worden gemaakt dat de betrokkene niet geïdentificeerd of identificeerbaar is. Anonimisering heeft tot gevolg dat de gegevensbeschermingsbeginselen en de hele Algemene verordening gegevensbescherming dus niet meer van toepassing is.[104]

Encryptie of versleuteling is een van de maatregelen die genomen kan worden om de veiligheid te waarborgen en risico's op inbreuken van gegevensverwerking te beperken.[105] Versleuteling is een systeem waarmee gegevens zodanig worden gecodeerd dat ze niet leesbaar zijn voor anderen.[106] Zowel pseudonimisering als versleuteling kunnen deel uitmaken van passende technische en organisatorische maatregelen. De genomen maatregelen moeten een passend niveau van beveiliging

---

[100] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[101] X, "Privacy by Design", januari 2018 http://www.ejure.nl/2018/01/privacy-by-design/.
[102] X, "De Avg uitgelegd deel 3: privacy by design en privacy by default", 5 april 2017, https://www.nldigital.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/#:~:text=De%20letterlijke%20vertaling%20van%20privacy,aandacht%20moet%20zijn%20voor%20privacy.
[103] Art. 4 5de lid AVG; art. 32 1ste lid AVG.
[104] Overweging 26 AVG.
[105] Overweging 83 AVG.
[106] I. BELCIC, "Wat is gegevensversleuteling en hoe werkt het?", 10 juni 2020, https://www.avg.com/nl/signal/data-encryption.

en vertrouwelijkheid waarborgen, waarbij rekening gehouden moet worden met de stand van de techniek en de uitvoeringskosten. Deze moeten afgewogen worden tegen de risico's en de aard van de persoonsgegevens. De AVG benadrukt dat bij de beoordeling van het passende beveiligingsniveau rekening gehouden wordt met de verwerkingsrisico's, zoals vernietiging en ongeoorloofde verstrekking.[107]

'Passende technische en organisatorische maatregelen voor de nodige waarborgen bij de verwerking'

De verwerkingsverantwoordelijke is verplicht passende technische en organisatorische maatregelen te treffen om de beginselen van gegevensbescherming te implementeren en om de noodzakelijke waarborgen in de verwerking te integreren. Zowel de passende maatregelen als de noodzakelijke waarborgen dienen voor hetzelfde doel. Ze beschermen beiden de rechten van betrokkenen en zorgen ervoor dat de bescherming van de persoonlijke gegevens zijn ingebouwd in de verwerking.[108]

De term 'passend' verwijst naar de geschiktheid van maatregelen en waarborgen om het beoogde doel te bereiken, m.a.w. de maatregelen moeten de beginselen van gegevensbescherming effectief en doeltreffend implementeren. De doeltreffendheid wordt later verder uitgelegd. De vereiste van geschiktheid is dus in correlatie met de doeltreffendheid.[109]

Technische of organisatorische maatregelen en waarborgen zijn zeer omvangrijk. Beginnend met een basisopleiding van personeel tot het gebruiken van geavanceerd technische oplossingen. Afhankelijk van de context en risico's verbonden aan de verwerking, kunnen bedrijven en organisaties gebruikmaken van privacy-en informatiebeveiligingsbeheersystemen, persoonlijke gegevens pseudonimiseren,[110] werknemers bijscholen en opleiden over basis cyberhygiëne etc.[111]

Normen, goede werkwijzen en gedragscodes, erkend door verenigingen en andere instanties die verschillende categorieën van verwerkers vertegenwoordigen, kunnen nuttig zijn bij het bepalen van passende maatregelen. De verwerkingsverantwoordelijke moet echter wel de geschiktheid of de doeltreffendheid van de maatregelen voor de specifieke verwerking controleren of verifiëren.[112]

---

[107] Artikel 32 AVG; Overweging 83 AVG.
[108] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[109] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[110] Art. 4 5de lid AVG.
[111] C. BROOK, "What is Cyberhygiene? A definition of Cyber Hygiene, Benefits, Best practices and More", 6 oktober 2020, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.
[112] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 6, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

'Opgesteld met als doel de beginselen inzake verwerking van persoonsgegevens op een doeltreffende manier uitvoeren en de rechten van de betrokkenen beschermen'

De verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen, specifiek het recht op bescherming van de persoonsgegevens.[113] De verwerking van persoonsgegevens moet bijgevolg ten dienste staan van de mens en niet omgekeerd. Het recht op bescherming van persoonsgegevens is niet absoluut, maar het evenredigheidsbeginsel dient ten alle tijde worden getoetst. Bij het implementeren van passende technische en organisatorische maatregelen mogen de bovenstaande principes en de daaruit voortvloeiende bescherming niet geschonden worden. De maatregelen en waarborgen moeten in respect met deze beginselen worden opgesteld.[114]

De doeltreffendheid vormt de kern van gegevensbescherming door ontwerp. De vereiste om op een doeltreffende manier te werk te gaan, betekent dat verwerkingsverantwoordelijken de nodige maatregelen en waarborgen moeten treffen om de beginselen te beschermen en rechten van de betrokkenen te waarborgen. Elke maatregel die genomen wordt, moet de beoogde resultaten opleveren die door de verwerker werd voorzien.[115]

Allereerst schrijft artikel 25 geen specifieke technische en organisatorische maatregelen voor, maar vereist het dat de gekozen maatregelen en waarborgen specifiek ten dienste moeten staan voor de implementatie van de beginselen inzake gegevensverwerking. De genomen maatregelen en waarborgen moeten dus zodanig worden opgesteld dat de kans op een eventueel risico wordt gereduceerd. Om te kunnen bepalen of maatregelen al dan een doeltreffend middel zijn, zal er gekeken worden naar de context van de verwerking en naar de beoordeling van bepaalde elementen, dat later nog aan bod komt.[116]

Vervolgens moeten verwerkingsverantwoordelijken kunnen aantonen dat de beginselen inzake gegevensverwerking gehandhaafd zijn. De geïmplementeerde maatregelen en waarborgen moeten het gewenste effect bereiken en de verantwoordelijke zou documentatie moeten hebben over de geïmplementeerde technische en organisatorische maatregelen om dit aan te tonen.[117] De verwerkingsverantwoordelijke zou zo KPI's kunnen gebruiken om de doeltreffendheid aan te tonen.[118] Een KPI is een meetbare waarde dat aantoont hoe effectief het doel wordt bereikt. KPI's kunnen zowel kwantitatief als kwalitatief zijn. Het aantal gereduceerde klachten en verkorting van

[113] Art. 1 2de lid AVG.
[114] Overweging 4 AVG
[115] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 7, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[116] Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", 30 mei 2014, nr. 218, 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.
[117] Overweging 74 AVG; Overweging 78 AVG.
[118] BSI, U General Data Protection Regulation (GDPR) 20 steps to GDPR compliance – A methodical, systematic and logical approach A whitepaper, p 9, https://www.bsigroup.com/LocalFiles/en-GB/CSIR/Resources/Whitepaper/UK-ENGB-CSIR-WP-20-steps-to-GDPR-PDF.pdf; P. DE RIDDER, "5 datasecurity-KPI's die uw onderneming zeker moet meten", Wolters Kluwer; X, "Uitleg over KPI's!", 2021, https://leansixsigmatools.nl/wat-zijn-key-performance-indactors;

de responstijd wanneer betrokkenen hun rechten uitoefenen zijn voorbeelden van kwantitatieve KPI's. Kwalitatieve KPI's hebben betrekking op het gebruik van evaluaties van prestaties en het gebruik van indelingsschalen of beoordelingen door experts. Naast het gebruik van KPI's kan de effectieve implementatie ook worden aangetoond door de ratio achter de beoordeling van de doeltreffendheid van de gekozen maatregelen.[119]

3.3.5. Andere elementen

Het eerst lid van artikel 25 kwalificeert enkele elementen waar de verwerkingsverantwoordelijke mee rekening moet houden bij het kiezen van de maatregelen. Aan de hand van deze elementen wordt bepaald of een maatregel geschikt is om de beginselen doeltreffend te implementeren. De elementen zijn dus geen doel op zich, maar zijn factoren die samen horen om het doel te bereiken.[120]

'de stand van techniek'

"De stand van de techniek" is element waar de verwerkingsverantwoordelijke rekening mee moet houden bij het bepalen van passende technische en organisatorische maatregelen.[121] Concreet verwijst het naar de huidige vooruitgang in technologie dat beschikbaar is op de markt. De verwerkingsverantwoordelijke moet voldoende kennis hebben en op de hoogte blijven van de technologische vooruitgang en hoe dit tot mogelijke risico's en kansen voor verwerkingsprocessen kan leiden. Bovendien moet de verantwoordelijke ook weten hoe de maatregelen en waarborgen geïmplementeerd en geüpdatet moeten worden om een effectieve implementatie van de beginselen en rechten te waarborgen, rekening houdend met de technologische ontwikkeling.[122]

Aangezien de stand van de techniek een dynamisch concept is dat niet statisch kan worden gedefinieerd, moet de maatregel worden beoordeeld in de context van de technologische vooruitgang. Zo kan een maatregel die ooit voldoende bescherming gaf, later geen adequate oplossing meer zijn om het beschermingsniveau te behouden. Indien de verwerkingsverantwoordelijke niet meer op de hoogte blijft van de stand van de techniek, kan dit leiden tot de niet-naleving van artikel 25.[123]

'De stand van de techniek' heeft niet enkel betrekking op technische maatregelen, maar ook op organisatorische. Bijgevolg kan het ontbreken van passende organisatorische maatregelen de

---

[119] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 7, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[120] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 8, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[121] Art. 25 1ste lid AVG; Art. 32 1ste lid AVG.

[122] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 8, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[123] IT Security Association Germany in co operation with ENISA, "IT Security Act and EU General Data Protection Regulation: Guideline 'State of the Art' technological and organisationial measures", 2021, 11, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf

effectiviteit verlagen of volledig ondermijnen. Om dit te voorkomen kunnen interne maatregelen genomen worden zoals het bieden van bijscholing om op de hoogte te blijven over technologie, veiligheid en gegevensbescherming en het hebben van een IT-beveiligingsbeheer.[124]

Factoren zoals standaardnormen, certificeringen en gedragscodes in verschillende gebieden, kunnen ook een rol spelen bij het bepalen van 'de stand van de techniek'. Wanneer zulke normen een hoog beschermingsniveau bieden, zouden verwerkingsverantwoordelijken hier ook rekening mee moeten in de ontwerpfase van het verwerkingssysteem en bij de implementatie van gegevensbeschermingsmaatregelen.[125]

'uitvoeringskosten'

Bij het bepalen van passende technische en organisatorische maatregelen mag de verwerkingsverantwoordelijke rekening houden met de uitvoeringskosten, zoals onder andere de tijd en het personeel. De verwerkingsverantwoordelijke is niet verplicht om een onevenredig bedrag aan middelen te besteden, wanneer er alternatieven zijn. Indien er middelen ingezet kunnen worden die minder bronnen vereisten en toch effectief zijn, heeft de verantwoordelijke het recht deze in te zetten.[126]

Vanzelfsprekend mag de verwerkingsverantwoordelijke geen maatregelen nemen die strijdig zijn met de beginselen en de fundamentele grondrechten. De algemene uitvoeringskosten moeten dus goed worden beheerd om de principes effectief te implementeren en de veiligheid te waarborgen.[127]

'de aard, de omvang, de context en het doel van de verwerking'

De verwerkingsverantwoordelijke moet bij het nemen van de nodige maatregelen rekening houden met de aard, de omvang, de context en het doel van de verwerking. Deze elementen moeten bovendien ook in samenhang geïnterpreteerd worden met hun rol in andere bepalingen van de verordening.[128]

Onder 'aard' wordt verstaan dat er inherente kenmerken zijn aan de verwerking, zoals de bijzondere categorieën van persoonsgegevens. De 'omvang' van de verwerking verwijst naar de breedte en het bereik ervan. De 'context' heeft betrekking op omstandigheden van de verwerking die de mogelijke verwachtingen van de betrokkene kunnen beïnvloeden, terwijl het 'doel' wel degelijk betrekking heeft op de verwerkingsdoeleinden.[129]

---

[124] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 8, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[125] *Ibid.*
[126] Art. 25 AVG; art. 32 AVG.
[127] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 9, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[128] Art. 24 AVG; art. 32 AVG; art. 35 AVG.
[129] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 9,

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

De op risico gebaseerde aanpak van de verordening is in veel bepalingen terug te vinden. Dezelfde bescherming, in de zin van de bescherming van persoonsgegevens, wordt afgewogen tegen dezelfde risico's met betrekking tot de rechten van het individu, waarbij steeds rekening gehouden wordt met dezelfde voorwaarden.[130]

Bij het uitvoeren van de risicoanalyse moet de verwerkingsverantwoordelijke de risico's voor de rechten van betrokkenen identificeren, waarbij de waarschijnlijkheid en de ernst voor uiteenlopende risico's moeten worden geïdentificeerd. Deze analyse heeft tot gevolg dat de verantwoordelijke de juiste maatregelen neemt en zo risico's vermijdt en beperkt. Een systematische en grondige evaluatie van de verwerking is bijgevolg cruciaal.[131]

Het advies van Artikel 29 Werkgroep betreffende de DPIA voorziet richtlijnen om de risico's van de verwerking in te schatten.[132] Het biedt ook richtlijnen voor het beoordelen van gegevensbeschermingsrisico's en het uitvoeren van een gegevensbeschermingsrisicobeoordeling. Afhankelijk van de mogelijke risico's zal een DPIA of gegevensbeschermingseffectbeoordeling in bepaalde gevallen verplicht zijn.[133]

'Bij de bepaling van de verwerkingsmiddelen'

Gegevensbescherming door ontwerp zal 'bij de bepaling van de verwerkingsmiddelen' geïmplementeerd worden. Verwerkingsmiddelen kunnen betrekking hebben op algemeen tot zeer gedetailleerde ontwerpelementen van de verwerking en kunnen onder andere betrekking hebben op protocollen, lay-out en het uiterlijk.[134]

Het ogenblik waarop de verwerkingsmiddelen worden bepaald, verwijst naar de periode waarin de verwerkingsverantwoordelijke beslist hoe de verwerking plaatsvindt en wordt uitgevoerd en welke mechanismen gebruikt zullen worden om de verwerking uit te voeren. In deze fase moet de verwerkingsverantwoordelijke passende maatregelen en waarborgen nemen om de beginselen en

---

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[130] Art. 24 AVG; art. 25 AVG; art. 32 AVG; art. 34 AVG.

[131] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 9, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[132] Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", nr. 248 rev.01, 4 oktober 2017, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171013_wp248_rev01_enpdf.pdf

[133] Art. 35 AVG.

[134] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 10, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

rechten van betrokkenen doeltreffend te implementeren, rekening houdend met de stand van de techniek, uitvoeringskosten, de aard etc.[135]

Voor een succesvolle implementatie van de DPbDD en de bescherming van betrokkenen is een vroegtijdige overweging van passende maatregelen en waarborgen van cruciaal belang. Het is bovendien voordeliger om zo vroeg mogelijk rekening te houden met DPbDD, aangezien latere wijzigingen aan plannen en het ontwerp zeer uitdagend en kostelijk kunnen zijn.[136]

'Bij de verwerking zelf'

Zodra de gegevensverwerking begint, is de verwerkingsverantwoordelijke voortdurend verplicht om DPbDD te onderhouden en te respecteren. De verwerker moet de principes en de rechten van de betrokkeren blijven beschermen door op de hoogte te blijven over de stand van de techniek, het risiconiveau te blijven beoordelen etc. Aangezien de aard, de omvang, de context en de risico's gedurende de verwerking kunnen veranderen, moet de verantwoordelijke de doeltreffendheid op regelmatige basis beoordelen. Enkel zo kunnen de genomen maatregelen garantie bieden.[137]

De verplichting om het verwerkingsproces te onderhouden, te herzien en bij te werken is ook van toepassing op systemen die voor de AVG bestonden. Bovendien strekt de verplichting zich ook uit tot alle verwerkingen die worden uitgevoerd door een verwerker. De activiteiten van de verwerker moeten op regelmatige basis herzien en beoordeeld worden door de verantwoordelijke om ervoor te zorgen dat de beginselen worden gerespecteerd en de verplichtingen onophoudelijk worden nageleefd.[138]

3.3.5. Art. 25 lid 2 AVG: Privacy by default

Data protection by default of gegevensbescherming door standaardinstellingen wordt beschouwd als een onderdeel van data protection by design. Het heeft betrekking op het feit dat standaardinstellingen altijd zo privacy-vriendelijk mogelijk moeten zijn. De verwerkingsverantwoordelijke moet te allen tijde passende technische en organisatorische maatregelen nemen om enkel persoonsgegevens te verwerken die noodzakelijk zijn voor het specifiek doel. Dit geldt zowel voor de hoeveelheid van de gegevens, de mate van verwerking, de termijn waarvoor de gegevens worden opgeslagen en de toegankelijkheid ervan. De maatregelen moeten vermijden dat zonder menselijke tussenkomst persoonsgegevens toegankelijk zijn voor een onbeperkt aantal natuurlijke personen.[139] Een profiel van een sociaal media platform mag dus niet standaard openbaar zijn, tenzij de betrokkene dit zelf zo heeft ingesteld. Het platform moet er dus voor opteren de meest privacy-vriendelijke instelling te standaardiseren. Dit heeft overigens niet

[135] *Ibid*.
[136] *Ibid.*
[137] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 10, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[138] *Ibid.,* 11.
[139] S. DE SMEDT en M. CAPRONI, *Praktische gids privacy in de onderneming*, Mechelen, Wolters Kluwer, 2019, 5.

enkel betrekking op sociaal media, maar ook op browser-instellingen, bedrijfs-apps, nieuwsbrieven etc.[140]

'In beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking'

Volgens computerinformatica verwijst de term 'standaard' in een softwareapplicatie, computerprogramma of apparaat naar de reeds bestaande of vooraf geselecteerde waarde van een configureerbare instelling. Deze instellingen worden ook wel voorinstellingen of fabrieksinstellingen genoemd. 'Door standaardinstellingen' heeft dus betrekking op configuratiewaarden of verwerkingsopties die vooraf bepaald zijn door instellingen. Deze opties kunnen betrekking hebben op de hoeveelheid verzamelde persoonsgegevens, de omvang van de gegevensverwerking, de opslagperiode en de toegankelijkheid.[141]

De verwerkingsverantwoordelijke moet opteren voor verwerkingsinstellingen-en opties waarbij de verwerking van gegevens enkel gebeurt indien dit strikt noodzakelijk is om het rechtmatig doel te bereiken. De verwerkingsverantwoordelijke mag standaard niet meer gegevens verzamelen, verwerken en bewaren dan noodzakelijk is. Om de noodzakelijkheid van de verwerking te beoordelen, zal de verantwoordelijke rekening moeten houden met de voorwaarden die in artikel 6 van de AVG zijn voorgeschreven. Doordat de minimumvereiste inhoudt dat de bescherming wordt ingebouwd door standaardinstellingen, moet de verwerkingsverantwoordelijke vooraf bepalen voor welke specifieke, expliciete en legitieme doeleinden de gegevens zullen worden verzameld en verwerkt.[142]

Een risicobeoordeling moet gebeuren wanneer de verwerkingsverantwoordelijke software gebruikt van een derde of beroep doet op kant-en-klare software. Functies die geen wettelijke basis hebben of onverenigbaar zijn met de beoogde verwerkingsdoeleinden moeten worden uitgeschakeld om een inbreuk te voorkomen. Dit geldt ook voor de organisatorische maatregelen die het verwerkingsproces ondersteunen. Enkel de persoonsgegevens die noodzakelijk zijn voor de specifieke verwerkingsopdracht mogen worden verwerkt.[143]

Passende 'technische en organisatorische maatregelen' in de zin van gegevensbescherming door standaardinstellingen, moeten dus worden geïnterpreteerd in dezelfde context als de gegevensbescherming door ontwerp. De verplichting om enkel minimale gegevens te verwerken die noodzakelijk zijn voor het specifiek doel, gelden voor de hoeveelheid verzamelde persoonsgegevens,

---

[140] X, "De Avg uitgelegd deel 3: privacy by design en privacy by default", 5 april 2017, https://www.nldigital.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/#:~:text=De%20letterlijke%20vertaling%20van%20privacy,aandacht%20moet%20zijn%20voor%20privacy.

[141] EDPS, "Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection", 19 december 2019, 1, https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[142] Art 6 1ste lid (b)-(e) AVG.

[143] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 11, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

de mate waarin ze worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze vier dimensies van dataminimalisatie worden hieronder verder uitgelegd.[144]

3.3.6 De verschillende dimensies van dataminimalisatie

3.3.6.1. Dimensie 1: 'de hoeveelheid verzamelde persoonsgegevens'

De verwerkingsverantwoordelijke moet bij de verwerking zowel rekening houden met de hoeveelheid van persoonlijke gegevens als de soorten, categorieën en het detailniveau die nodig zijn voor de doeleinden. Tijdens de ontwerpfase zal de verantwoordelijke zowel de mogelijke toename van risico's met betrekking tot de principes van integriteit en vertrouwelijkheid in acht moeten nemen, als de gegevensminimalisatie en opslagbeperking moeten respecteren. Tijdens de ontwerpfase moeten de risico's met betrekking tot het verzamelen van grote hoeveelheden gedetailleerde informatie worden afgewogen worden tegen de risico's van het verzamelen van kleinere hoeveelheden of minder gedetailleerde informatie. De standaardinstellingen zullen in ieder geval geen persoonlijke gegevens verzamelen die niet noodzakelijk zijn voor het specifieke doel van de verwerking. Dezelfde standaardinstellingen zijn ook van toepassing op diensten onafhankelijk van het soort platform of apparaat. Enkel persoonsgegevens die noodzakelijk zijn voor het doel te bereiken mogen worden verzameld.[145]

3.3.6.2 Dimensie 2: 'de mate waarin de gegevens worden verwerkt'

Het is van groot belang dat verwerkingsprocessen[146] worden gelimiteerd tot wat strikt noodzakelijk is. Desondanks bepaalde persoonsgegevens nodig zijn om een specifiek doel te bereiken, wil dit niet zeggen dat de gegevens gebruikt mogen worden door verschillende soorten en frequenties van verwerkingsprocessen. Bovendien moet de verwerkingsverantwoordelijke de grenzen van artikel 6 te allen tijde respecteren.[147]

3.3.6.3 Dimensie 3: 'de termijn waarvoor de gegevens worden opgeslagen'

Persoonlijke gegevens zullen niet worden opgeslagen wanneer dit niet noodzakelijk is voor het doel van de verwerking of enig ander doel of wanneer er geen rechtsgrond toe bestaat.[148] De verwerkingsverantwoordelijke moet de duur van opslag kunnen verantwoorden op basis van de verantwoordingsplicht.[149]

Aangezien de bewaartermijn beperkt wordt tot wat strikt noodzakelijk is voor het doel van de verwerking, moeten gegevens standaard worden verwijderd of geanonimiseerd indien ze niet langer nodig zijn voor het beoogde doel. De bewaartermijn wordt dus bepaald door het doel van de

---

[144] Art 25 2de lid AVG.
[145] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 12, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[146] Art. 4 2de lid AVG.
[147] Art. 6 4de lid AVG.
[148] *Ibid*; Art. 5 1ste lid (e) AVG.
[149] Art. 5 2de lid AVG.

verwerking. Deze verplichting kan rechtstreeks gelinkt worden aan het principe van opslagbeperking.[150]

Naast gegevensverwijdering kan de verantwoordelijke de gegevens ook anonimiseren. Bij anonimisering moet er echter rekening gehouden worden met alle relevante contextuele elementen, de waarschijnlijkheid en ernst van het risico en het risico van heridentificatie. De verantwoordelijke moet de beoordeling van alle deze elementen op regelmatige basis uitvoeren.[151]

3.3.6.4 Dimensie 4: 'de toegankelijkheid van de gegevens'

Op basis van de noodzakelijkheid moet de verwerkingsverantwoordelijke bepalen en beperken wie toegang krijgt tot de persoonsgegevens. Zo moeten persoonsgegevens toegankelijk zijn voor de verwerkers die het daadwerkelijk nodig hebben, zoals bijvoorbeeld in kritieke situaties. De toegang tot persoonsgegevens moet gecontroleerd worden gedurende de hele gegevensstroom gebeuren.[152]

Verder mogen persoonsgegevens niet toegankelijk worden gemaakt aan een onbepaald aantal personen zonder de tussenkomst van de betrokkene. Het is de verantwoordelijkheid van de verwerker om de toegankelijkheid stadaard te limiteren en om de betrokkene de mogelijkheid te geven om de openbaarmaking te weigeren. Het ter beschikking stellen van de persoonsgegevens aan een onbepaald aantal personen, kan tot gevolg hebben dat de verspreiding groter wordt dan initieel bedoeld was. Dit is in het bijzonder relevant in de context van het internet en zoekmachines. Het is bijgevolg de plicht van de verantwoordelijke om de betrokkene standaard de mogelijkheid te bieden om in te grijpen wanneer gegevens gepubliceerd worden op het internet. Vooral voor kinderen en kwetsbare groepen is dit van cruciaal belang.[153]

Zelfs wanneer de betrokkene persoonlijke gegevens openbaar maakt, heeft dit niet automatisch tot gevolg dat andere verwerkingsverantwoordelijken deze persoonsgegevens voor hun eigen doeleinden mogen gebruiken. Er moet tenslotte een wettelijke basis zijn voor de verwerking.[154]

3.3.7 De implementatie van de beginselen inzake verwerking van persoonsgegevens (gebruikmakend van gegevensbescherming door ontwerp en door standaardinstellingen)

[150] Artikel 5 1 e AVG
[151] Article 29 Working Party "Opinion 05/2014 on Anonymisation Techniques", 10 april 2014, nr. 216, 6-7, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[152] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 13, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[153] *Ibid*., 13-14.
[154] EHRM, 27 juni 2017, nr. 931/13 Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland

In elk stadium van het ontwerp is de verwerkingsverantwoordelijke verplicht om de verschillende elementen van gegevensbescherming door ontwerp en standaardinstellingen na te leven.[155] Het is van cruciaal belang om de beginselen inzake de verwerking van persoonsgegevens te implementeren. Artikel 5 van de AVG omvat de volgende beginselen; rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid en de verantwoordingsplicht. Om een correcte implementatie te garanderen, moeten deze beginselen goed begrepen worden.[156]

3.3.8 Rechtmatigheid

De verwerkingsverantwoordelijke is verplicht om de verwerking van persoonsgegevens te baseren op een wettelijke basis. De gekozen maatregelen en waarborgen moeten zodanig aan deze vereiste voldoen dat de hele levenscyclus van de verwerking overeenstemt met de relevante juridische gronden. De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het rechtmatigheidsbeginsel.[157]

De *relevantie* is een eerste belangrijk element dat wordt aangehaald. De relevantie verwijst naar het belang van de juiste wettelijke basis voor de verwerking. Een tweede element is de *differentiatie*. Elke verwerkingsactiviteit wordt als apart aanschouwd en moet daarom een eigen wettelijke basis hebben. Vervolgens wordt het bepalen van een *specifiek doel* opgesomd. Het is van groot belang dat dat de wettelijke basis in verband staat met het specifieke doel van de verwerking. De *noodzakelijkheid* is een volgend element dat in acht moet worden genomen. Het verwijst naar het feit dat de verwerking noodzakelijk en onvoorwaardelijk moet zijn om aan het beginsel van rechtmatigheid te voldoen. Een vijfde element is de *autonomie*. De betrokkene moet gerechtigd zijn om het hoogste niveau van autonomie te krijgen zodat hij/zij controle heeft over de eigen gegevens. Verder benadrukt de EDPB het belang van de *toestemming*, dat betrekking heeft op het instemmen van de verwerking mits het vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven wordt. Het vermogen van kinderen en jongeren om geïnformeerde toestemming te geven is bovendien een belangrijk element waar de verantwoordelijke rekening mee moet houden.[158]

De *intrekking van de toestemming* is minstens een even belangrijk element als het geven van de toestemming.[159] Het moet namelijk even gemakkelijk zijn om toestemming te geven als om het in te trekken. Een volgend element heeft betrekking op een *afweging van belangen*. Bij het afwegen van verschillende belangen, moet de verwerkingsverantwoordelijke bijzondere aandacht besteden aan de machtsongelijkheid, rekening houdend met kwetsbare groepen en kinderen onder 18 jaar[160].

---

[155] More examples can be found in Norwegian Data Protection Authority. "Software Development with Data Protection by Design and by Default". 28 November 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
[156] Art. 5 AVG; overweging 39 AVG.
[157] Art. 5 1ste lid (a) AVG; EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 16, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[158] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679 version 1.1", 4 mei 2020, 6-7, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[159] *Ibid.,* 14.
[160] Overweging 38 AVG.

De EDPB benadrukt ook het belang van de *voorafgaande bepaling*, waarbij de rechtsgrondslag waarop de verwerking steunt, voorafgaand bepaald wordt. Vervolgens heeft de verantwoordelijke ook verplichtingen bij de *beëindiging* van de rechtsgrond. Zo moet de verwerking worden stopgezet indien de rechtsgrond niet langer van toepassing is. Bovendien benadrukt de EDPB benadrukt het element van de *aanpassing*. Dit heeft betrekking op het feit dat wanneer de rechtsgrondslag verandert, de verwerking moeten worden aangepast aan de nieuwe wijziging.[161]

Tot slot wordt de *toewijzing van verantwoordelijkheid* omschreven als een laatste element waar de verantwoordelijke rekening mee moet houden. Wanneer een gezamenlijke verwerking van toepassing is, moeten beide verwerkers op een heldere en transparante wijze hun verantwoordelijkheden nemen en de nodige maatregelen ontwerpen. Al deze elementen moeten in acht genomen worden om aan de rechtmatigheid van de verwerking te voldoen.[162]

3.3.9 Behoorlijkheid

Het behoorlijkheidsbeginsel houdt in dat de verwerking van de persoonsgegevens niet onterecht schadelijk, onrechtmatig, discriminerend, onverwacht of misleidend mag zijn voor de betrokkene. Het beginsel is zeer breed en overkoepelend, omdat de maatregelen en waarborgen die dit beginsel implementeren ook andere rechten en vrijheden eerbiedigen. Het recht op informatie, het recht op rectificatie en het recht om de gegevensverwerking te beperken zijn hier enkele voorbeelden van. De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het behoorlijkheidsbeginsel.[163]

De *autonomie* is een eerste belangrijk element dat wordt aangehaald. Dit element verwijst naar de hoogst mogelijke mate van autonomie, waarbij de betrokkene zelf mag bepalen hoe de persoonsgegevens worden gebruikt en wat de reikwijdte en voorwaarden van dat gebruik moet zijn. De *interactie* is een tweede element dat door de EDPB wordt opgesomd en heeft betrekking op het recht van de betrokkene om te communiceren en zijn/haar rechten uit te oefenen. De verwerking moet vervolgens ook overeenkomen met de redelijke verwachtingen van de betrokkenen zodat het derde element van *verwachting* is voldaan. Ook het *non-discriminatiebeginsel* valt onder het behoorlijkheidsbeginsel. Dit heeft betrekking op het feit dat de betrokkene niet op oneerlijke wijze behandeld of gediscrimineerd mag worden. De *niet-exploitatie* is een volgend element. Dit houdt in dat er geen misbruik gemaakt mag worden van behoeften of kwetsbaarheden van de betrokkene. Ook *de keuze van de consument* is een belangrijk element. Dit betekent dat de betrokkene steeds eigenaar is van zijn/haar persoonlijke gegevens en dat de verantwoordelijke de gegevens niet mag 'insluiten'. Zo mag het recht op dataportabiliteit niet geschonden worden.[164]

---

[161] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679 version 1.1", 4 mei 2020, 20, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[162] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 16, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[163] Art. 5 1ste lid AVG; EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 18, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[164] Art. 20 AVG.

De *machtsbalans* is een ander element waar rekening mee gehouden moet worden. Wanneer evenwicht tussen de verwerkingsverantwoordelijke en de betrokkene niet kan worden gerealiseerd, moet dit erkend worden en worden passende tegenmaatregelen genomen. Vervolgens mogen verwerkers geen risico's van de onderneming overdragen naar de betrokkenen, wat het element van *risico-overdracht* inhoudt. De verwerkingsverantwoordelijken mogen vanzelfsprekend geen gebruik maken van *bedrog*, waardoor misleidende of manipulatieve taal of ontwerp moeten worden vermeden. Het *respecteren van de rechten van de betrokkene* is een duidelijk element. Zoals reeds vermeld, moet de verwerkingsverantwoordelijke de fundamentele rechten van de betrokkene respecteren door middel van het implementeren van passende maatregelen en waarborgen. Enkel wanneer het gerechtvaardigd is bij wet, mag hiervan worden afgeweken. De verwerking moet bovendien te allen tijde *ethisch* blijven, wat wil zeggen dat de verwerker zicht moet hebben op de brede impact op de rechten en waardigheid van de betrokkene. Verder, moet de verwerkingsverantwoordelijke altijd *waarheidsgetrouw* te werk gaan en mag hij de betrokkene niet misleiden. De verwerkingsverantwoordelijke moet vervolgens gekwalificeerde *menselijke tussenkomst* voorzien, om profilering te voorkomen.[165] Dit kan nl. veroorzaakt worden door geautomatiseerde individuele besluitvorming. Het laatste element dat de EDPB opsomt is het gebruik maken van eerlijke algoritmen. Er moet regelmatig beoordeeld worden of algoritmen in overeenstemming met hun doel functioneren. Indien nodig, moeten de algoritmen worden aangepast. Betrokkenen hebben bovendien het recht om geïnformeerd te worden over hoe de verwerking van hun gegevens gebeurt. Algoritmen kunnen niet enkel analyseren maar ook voorspellingen doen over verschillende situaties van de betrokkenen, zoals werkprestaties, persoonlijke voorkeuren en gedrag.[166] Al deze elementen moeten in acht genomen worden om aan de behoorlijkheid van de verwerking te voldoen.[167]

3.3.10 Transparantie

Het transparantiebeginsel houdt in dat de verwerkingsverantwoordelijke te allen tijde duidelijk en open moet zijn over hoe de persoonsgegevens verzamelt, gebruikt en gedeeld worden.[168] De betrokkene heeft het recht om inzicht te krijgen op zijn/haar rechten en indien nodig er ook gebruik van te maken.[169] Het transparantiebeginsel is in verschillende terug te vinden, wat duidelijk maakt dat dit toch wel een zeer belangrijk beginsel is.[170] De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het transparantiebeginsel.[171]

---

[165] Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 6 oktober 2018, nr 251 rev.01, 20, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[166] Overweging 71 AVG.
[167] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 18, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[168] Art. 5 1ste lid (a) AVG.
[169] Art. 15-22 AVG.
[170] Art. 12-14 AVG; art. 34 AVG.
[171] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 15, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Duidelijkheid omtrent alle informatie is een eerste belangrijk element dat wordt aangehaald. De betrokkene moet alle informatie kunnen begrijpen, waardoor het in duidelijke, beknopte en begrijpelijke taal gecommuniceerd moet worden. Vervolgens moet er *semantiek* aanwezig zijn, waarbij de communicatie duidelijk moet zijn voor het desbetreffende publiek. Bovendien moet de informatie ook gemakkelijk *toegankelijk*, *contextueel* en *relevant* zijn. De informatie moet op het relevante tijdstip en in de juiste vorm worden gegeven. Ook, moet het relevant en toepasbaar zijn voor de betrokkene.[172]

De EDPB benadrukt dat het *ontwerp* ook *universeel* moet zijn, omdat de informatie voor alle betrokkenen toegankelijk moet zijn. De verwerking moet vervolgens ook *begrijpelijk* zijn voor de betrokkene omtrent hetgeen wat ze kunnen verwachten. Hier moet extra aandacht gegeven worden aan kinderen en kwetsbare groepen. Een ander belangrijk element is dat de informatie niet enkel in tekst moeten worden gegeven, maar ook via *meerdere kanalen* en media. Zo is immers de kans groter dat de informatie de betrokkene effectief bereikt. Tot slot benadrukt de EDPB dat de informatie voldoende gestructureerd moet zijn, zodat de betrokkene de informatie voldoende begrijpt.[173] Al deze elementen moeten in acht genomen worden om aan de transparantie van de verwerking te voldoen.[174]

3.3.11 Doelbinding

Het beginsel van doelbinding houdt in dat de verwerkingsverantwoordelijke persoonsgegevens verzamelt voor de gekozen gespecificeerde, expliciete en legitieme doeleinden.[175] De verzamelde gegevens mogen in beginsel dus niet verwerkt worden voor andere doeleinden die hier onverenigbaar mee zijn.[176] De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het beginsel van doelbinding.[177]

Een *voorafgaande bepaling,* waarin de legitieme doeleinden bepaald worden voordat het ontwerp van verwerking plaatsvindt, is een eerste belangrijk element dat wordt aangehaald. Een tweede element is de *specificiteit*. De doeleinden moeten gespecificeerd en expliciet aangeven waarom de gegevens worden verwerkt. De verwerking moet ook *doelgericht* blijven, wat wil zeggen dat het doel het ontwerp moet leiden, waarbij er grenzen worden gezet aan de verwerking. Vervolgens moet er ook een *noodzaak* zijn voor de verwerking. De noodzaak houdt in dat de gekozen doeleinden bepalen welke gegevens noodzakelijk zijn voor de verwerking door de verantwoordelijke. De *compatibiliteit* is een vijfde belangrijk element voor de doelbinding. Wanneer gegevens verzameld worden voor het

---

[172] *Ibid*.
[173] Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679", 11 april 2018, nr. 260 rev.01, 7, https://ec.europa.eu/newsroom/article29/items/622227.
[174] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 15, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[175] Art. 5 1ste lid (b) AVG.
[176] Art. 4 4de lid AVG.
[177] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 20, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

oorspronkelijk doel, maar verwerkt zullen worden voor een nieuw doeleinde, moet deze laatste compatibel zijn met het huidig doel.[178] *Verdere verwerking beperken* is een zesde element en heeft betrekking op de compatibiliteit. Verwerkingsverantwoordelijken mogen geen gegevens verwerken voor nieuwe doeleinden die onverenigbaar zijn met de huidige. Bovendien moet ook het *hergebruik van gegevens beperkt worden* door de verantwoordelijke. Het gevaar om verzamelde gegevens opnieuw te gebruiken door middel van een nieuw doeleinde te geven, moet te allen tijde vermeden worden. De verwerkingsverantwoordelijke moet hiervoor technische maatregelen nemen zoals hashing[179] en versleuteling[180] en organisatorische maatregelen via het beleid en contractuele verplichtingen. Tot slot moet de verwerkingsverantwoordelijke op regelmatige basis een *beoordeling* doen. De verantwoordelijke moet zo nagaan of de verwerking van de verzamelde gegevens wel noodzakelijk is om de bepaalde doeleinden te realiseren.[181] Al deze elementen moeten in acht genomen worden om aan de doelbinding van de verwerking te voldoen.[182]

3.3.12 Minimale gegevensverwerking

De minimale gegevensverwerking of dataminimalisatie houdt in dat gegevens enkel verwerkt mogen worden wanneer ze adequaat, relevant en beperkt zijn tot wat noodzakelijk is voor het gekozen doel.[183] Functies, parameters en ondersteunende functies van verwerkingssystemen moeten dus op voorhand bepaald worden. Daarenboven moet de verantwoordelijke op regelmatige basis nagaan of de verwerking van de gegevens nog steeds toereikend, relevant en noodzakelijk is en desnoods de persoonsgegevens verwijderen of anonimiseren. De verwerkingsverantwoordelijke moet vervolgens toetsen of de verwerking van minder persoonlijke of minder gedetailleerde gegevens kan leiden tot het bekomen van dezelfde doeleinden.[184] Deze controle moet voor de effectieve verwerking plaatsvinden, maar mag ook tijdens de levenscyclus van de verwerking worden uitgevoerd. [185]

Dataminimalisatie kan ook betrekking hebben op de mate van identificatie. Wanneer er voor het verwerkingsdoel geen persoonlijke gegevens meer vereist zijn om te verwijzen naar een geïdentificeerde of identificeerbare persoon, dan zal de verwerkingsverantwoordelijke gehouden worden om de gegevens te verwijderen of om ze te anonimiseren.[186] Wanneer de identificatie wel nodig is voor andere verwerkingsactiviteiten moet de verantwoordelijke de persoonsgegevens pseudonimiseren om mogelijke risico's te reduceren.[187] De EDPB somt enkele belangrijke ontwerp-

[178] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 april 2013, nr. 203, 16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[179] AEPD, "Introduction to the hash function as a personal data pseudonimation technique", oktober 2019, 5, https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf.
[180] Overweging 83 AVG.
[181] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 april 2013, nr. 203, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[182] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 20, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[183] Art. 5 1ste lid (c) AVG; Art. 85 Verord.EP en Raad 2018/1725 van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG.
[184] Overweging 39 AVG.
[185] Overweging 26 AVG; overweging 39 AVG.
[186] Overweging 26 AVG.
[187] Overweging 28 AVG.

en standaardelementen op die in overeenstemming zijn met het beginsel van minimale gegevensverwerking.[188]

De *gegevensvermijding* is een eerste belangrijk element dat wordt aangehaald. Indien het mogelijk is om het beoogde doel te bereiken zonder de verwerking van persoonsgegevens, moet de verwerkingsverantwoordelijke deze verwerking vermijden. Dit sluit ook aan met de *beperking* van de verzameling van de hoeveelheid gegevens. Enkel datgeen wat noodzakelijk is voor de verwerking, mag worden verzameld. De verwerkingsverantwoordelijke moet te allen tijde belang hechten aan de *toegangsbeperking*. Enkel het personeel dat toegang nodig heeft tot de persoonsgegevens in het kader van hun verwerkingstaken, mag hier toegang tot krijgen. Vervolgens moeten de gegevens die verwerkt worden *relevant en noodzakelijk* zijn voor de doeleinden. Gegevens die dat niet zijn, mogen bijgevolg niet verwerkt worden. *Data-aggregatie* en het gebruik van *geaggregeerde gegevens* is een ander element dat sterk wordt aanbevolen. Dit is een proces waarin informatie wordt verzameld voor statische doeleinden. Het resultaat van die verwerking bestaat bijgevolg niet uit persoonsgegevens, maar uit geaggregeerde gegevens. Belangrijk is dat de gegevens niet gebruikt mogen worden als ondersteunend materiaal voor maatregelen die de betrokkene betreffen.[189]

Een volgend belangrijk element is het *pseudonimiseren* van gegevens wanneer er geen directe identificeerbare persoonsgegevens meer noodzakelijk zijn. Ook benadrukt de EDPB dat identificatiesleutels apart moeten worden opgeslagen. *Verwijdering* en *anonimisering* van gegevens moeten bovendien in elke stadium van het proces worden getoetst.[190] Verder moet de *datastroom* efficiënt zijn om niet noodzakelijke kopieën te vermijden en risico's te reduceren. Tot slot wordt het element van de *stand van de techniek* benadrukt.[191] Zoals eerder besproken, moet de verwerkingsverantwoordelijke steeds up-to-date blijven over de toepassing van de meest geschikte technologieën voor gegevensvermijding en -minimalisatie. Al deze elementen moeten in acht genomen worden om aan de minimale gegevensverwerking te voldoen.[192]

3.3.13 Juistheid

Het beginsel van juistheid houdt in dat de verwerkingsverantwoordelijke de gegevens up-to-date houdt zodat ze steeds actueel en correct zijn. De verantwoordelijke zal bijgevolg redelijke maatregelen moeten treffen om onjuiste gegevens te corrigeren of te verwijderen.[193] De Europese wetgever wil met deze vereiste de risico's van het gebruik van onjuiste gegevens beperken, aangezien het gebruik ervan kan leiden tot een foute diagnose of verkeerde behandeling. De EDPB

---

[188] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[189] Overweging 162 AVG.
[190] Art. 4 5de lid AVG; overweging 26 AVG.
[191] Pg 33
[192] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 21, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[193] Art. 5 1ste lid (d) AVG; art. 18 1ste lid (a) AVG.

somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het beginsel van juistheid.[194]

Een eerste belangrijk element heeft betrekking op de betrouwbaarheid van *gegevensbronnen*. Bronnen zouden in elk geval betrouwbaar moeten zijn en enkel nauwkeurige en correcte elementen bevatten. De *meetbare nauwkeurig* is ook van groot belang. Dit houdt in dat aantal valse positieven/negatieven gereduceerd moeten worden om bijvoorbeeld vooringenomenheid in geautomatiseerde beslissingen en kunstmatige intelligentie te vermijden. Verder moet de *verificatie* worden aangeboden zodat de betrokkene in verschillende stadia de juistheid van de persoonsgegevens kan bevestigen. Bovendien moet de verantwoordelijke het recht op *wissing* of *rectificatie* te allen tijde respecteren.[195] Zo moeten onnauwkeurige gegevens onverwijld gewist of gecorrigeerd worden om mogelijke risico's te beperken. Vervolgens moet de verantwoordelijke de *foutverspreiding vermijden* door fouten te verminderen in het verwerkingsproces. Een ander belangrijk element is dat de verwerkingsverantwoordelijke de betrokkene de toegang moet verlenen tot en de nodige informatie moet geven over de persoonsgegevens.[196] Bovendien moet de verantwoordelijke zorgen voor de *voortdurende nauwkeurigheid* door middel van bepaalde testen uit te voeren. De voortdurende nauwkeurigheid heeft tot gevolg dat de persoonsgegevens *up-to-date* en correct blijven. Tot slot benadrukt De EDPB het belang van het gegevensontwerp. Zo moeten ingebedde technologische en organisatorische maatregelen gebruikt worden om de onnauwkeurigheid van gegevens te vermijden en te reduceren. Al deze elementen moeten in acht genomen worden om aan de juistheid van de verwerking te voldoen.[197]

3.3.13 Opslagbeperking

De opslagbeperking houdt in dat de verwerkingsverantwoordelijke verplicht is persoonsgegevens te bewaren in een vorm waarbij de betrokkene niet geïdentificeerd kan worden dan voor de beoogde doeleinden.[198] Het is van cruciaal belang dat de verwerkingsverantwoordelijke zich heeft op welke persoonsgegevens er verwerkt worden en voor welke redenen dit gebeurt. Het belangrijkste criterium om de termijn van opslag te bepalen is bijgevolg afhankelijk van het doel van de verwerking. De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het beginsel van opslagbeperking.[199]

---

[194] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 23-24, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[195] Overweging 59 AVG; art. 13 2de lid (b) AVG; art. 16-17 AVG.
[196] Artikel 12-15 AVG.
[197] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 23-24, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[198] Art. 5 1ste lid (e) AVG
[199] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 25, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Een eerste belangrijk element dat de EDPB aanhaalt, is de *wissing*[200] en *anonimisering*[201]. De verwerkingsverantwoordelijke is verplicht om te beschikken over duidelijke interne procedures en functies inzake de wissing en anonimisering. *De doeltreffendheid van anonimisering of wissing* is bijgevolg ook van groot belang. Geanonimiseerde gegevens mogen bijgevolg niet opnieuw identificeerbaar worden gemaakt en verwijderde gegevens mogen niet hersteld worden. Dit moet bovendien op regelmatige basis getest worden door de verwerkingsverantwoordelijke. Verder, moet de verwerkingsverantwoordelijke de verwijdering van bepaalde persoonsgegevens *automatiseren* en de nodige *opslagcriteria* bepalen.[202] De verantwoordelijke bepaalt de duur van de opslag en beslist welke gegevens noodzakelijk zijn voor het beoogde doel. Vervolgens, moet de opslagtermijn *gerechtvaardigd* worden op basis van achterliggende gedachten en juridische gronden. De *naleving* van dit termijn kan worden bewezen door onder andere testen uit te voeren. Vervolgens is de verantwoordelijke verplicht om de opslagduur en de soort gegevens te bepalen die noodzakelijk zijn voor eventuele *back-ups.* Tot slot moedigt de EDPB aan om de tijdelijke opslag van gegevens zo beperkt mogelijk te houden. Al deze elementen moeten in acht genomen worden om aan de opslagbeperking van de verwerking te voldoen.[203]

3.3.14 Integriteit en vertrouwelijkheid

Het beginsel van integriteit en vertrouwelijkheid houdt in dat de verwerkingsverantwoordelijke passende technische of organisatorische maatregelen neemt om persoonsgegevens te beschermen tegen ongeoorloofde of onwettige verwerking en tegen opzettelijk verlies, beschadiging of vernietiging van persoonsgegevens.[204] De maatregelen moeten datalekken voorkomen en de juiste naleving van gegevensverwerking en andere beginselen verzekeren. Bovendien moeten de maatregelen de effectieve uitoefening van de rechten van betrokkenen vergemakkelijken. De verantwoordelijke moet de maatregelen op regelmatige basis beoordelen voor hun effectiviteit.[205] De EDPB somt enkele belangrijke ontwerp- en standaardelementen op die in overeenstemming zijn met het beginsel van integriteit en vertrouwelijkheid.[206]

Een eerste element dat de EDPB aanhaalt, is het belang van *informatiebeveiligingsbeheersystemen*, die op een effectieve manier het beleid en de procedures omtrent de informatieveiligheid beheren. Verder, moeten *risicoanalyses* worden uitgevoerd, waarbij de beveiliging van persoonsgegevens beoordeeld wordt door de impact van individuele rechten af te wegen tegen geïdentificeerde risico's. Om een risicobeoordeling zo doeltreffend mogelijk uit te voeren, moet een systematisch en realistisch beveiligingsmodel ontwikkeld worden. Door middel van een 'attack surface analysis' moeten zwakke punten en kwetsbaarheden verbeterd worden. Door beveiligingsvereisten zo vroeg mogelijk in het

---

[200] Art. 17 AVG.
[201] Overweging 26 AVG.
[202] Overweging 39 AVG.
[203] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 25, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[204] Art. 5 1ste lid (f) AVG.
[205] Overweging 78 AVG; art. 32 1ste lid (d) AVG.
[206] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 26-27, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

systeem te ontwerpen en op regelmatige basis testen uit te voeren, wordt er voldaan aan het criterium van *veiligheid door ontwerp*. Regelmatig *onderhoud* door het beoordelen en testen van verschillende software, hardware, systemen en diensten, kan kwetsbaarheden ontdekken en verhelpen.[207] Het toegangscontrolebeheer is een ander element waar de verwerkingsverantwoordelijke rekening mee moet houden. Zo mag enkel geautoriseerd personeel toegang krijgen, in het kader van de uitoefening van de verwerkingstaken, tot de persoonsgegevens. Vervolgens heeft de verwerkingsverantwoordelijke de plicht om *veilige overdrachten* te garanderen, waarbij ongeoorloofde toegang en veranderingen streng moeten worden opgevolgd en beveiligd. Daarenboven moet een *veilige opslag* van persoonsgegevens gegarandeerd worden. Om dit te verzekeren moet stelselmatig beoordelingen worden uitgevoerd en indien nodig, aanvullende beveiligingsmaatregelen genomen worden. Een volgend element, dat al enkele keren ter sprake kwam, is de *pseudonimisering*. Dit om zowel de veiligheid te waarborgen maar ook om risico's op mogelijke datalekken te minimaliseren. Verder, mogen *back-ups enkel plaatsvinden* in de mate waarin het noodzakelijk is voor de veiligheid. Verder, moet de verwerkingsverantwoordelijke de nodige maatregelen treffen inzake *noodherstel of bedrijfscontinuïteit*.[208] Door een noodherstelsysteem en de nodige bedrijfscontinuïteitmaatregelen, voorkomt de verantwoordelijke het verlies van persoonsgegevens na grote incidenten. Ook, moet de mate van bescherming worden bepaald *naargelang het risico*. Wanneer bepaalde gegevens bijzondere risico's teweegbrengen, moeten deze gescheiden worden van de andere gegevens. Een voorlaatste element is het bezitten van een *management dat veiligheidsincidenten* snel opspoort, beheerst, afhandelt en rapporteert door middel van verschillende routines en procedures.[209] Op deze manier kan geleerd worden uit incidenten en datalekken, waardoor toekomstige risico's gereduceerd worden. Tot slot moet elke verantwoordelijke een *incidentenbeheer* hebben, waarbij de toezichthoudende autoriteit of de betrokkene wordt ingelicht bij datalekken en inbreuken. Al deze elementen moeten in acht genomen worden om aan de integriteit en vertrouwelijkheid van de verwerking te voldoen.[210]

3.3.15 Verantwoordingsplicht

Het beginsel van de verantwoordingsplicht houdt in dat de verwerkingsverantwoordelijke alle beginselen naleeft en hier het bewijs van levert.[211] De verantwoordelijke zal de nodige documentatie moeten bijhouden om deze nakoming aan te tonen. Goedgekeurde gedragscodes[212], certificeringen[213] en de aanwijzing van een functionaris voor gegevensbescherming zijn enkele elementen die als bewijs kunnen dienen.[214] Bovendien bepaalt de AVG dat de verantwoordelijke elke

[207] Art. 32 1ste lid (d) AVG.
[208] Art. 32 1 ste lid (b) AVG.
[209] Art. 32 1ste lid (c) (d) AVG.
[210] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 26-27, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[211] Art. 5 2de lid AVG; Overweging 82 AVG; Autoriteit Persoonsgegevens, "verantwoordingsplicht" https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht (consultatie op 8 maart 2021).
[212] Art. 40 AVG.
[213] Art. 42 AVG.
[214] Overweging 77 AVG.

verwerkingsactiviteit bijhoudt in een register en deze ter beschikking stelt aan de toezichthoudende autoriteit.[215]

3.4 Art. 25 (3) Certificering

Het derde lid van artikel 25 omschrijft dat een goedgekeurd certificeringsmechanisme gebruikt kan worden om de naleving van DPbDD aan te tonen.[216] De toezichthoudende autoriteit houdt bijgevolg rekening met dit certificaat tijdens hun beoordeling over de naleving van de bepalingen. De criteria, de afgifte en de verlening van een certificaat gebeurd door certificatie-organen.[217] Het bekomen van een certificering sluit echter niet uit dat op regelmatige basis de naleving van gegevensbescherming wordt gecontroleerd.[218] De EDPB heeft uitgebreide richtlijnen voorzien m.b.t het certificeringsmechanisme.[219]

3.4.1 Handhaving van DPbDD en de gevolgen

Om de handhaving van de verplichtingen van artikel 25 te garanderen, kunnen toezichthoudende autoriteiten de nodige bevoegdheden treffen. Deze kunnen onderzoeksbevoegdheden[220], corrigerende maatregelen[221] en autorisatie-en adviesbevoegdheden[222] zijn. Bovendien voorziet de verordening een specifieke bepaling voor het opleggen van administratieve geldboeten.[223] Geldboeten kunnen zowel naast of samen met de andere maatregelen opgelegd worden.[224] Bij het bepalen van de hoogte van de boete, moeten de autoriteiten rekening houden met enkele voorwaarden zoals de aard en ernst van de inbreuk.[225] Instanties die niet GDPR-comform zijn, riskeren een administratieve boete tot wel 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet. De GDPR vereist dat de boete in ieder geval dat de boete doeltreffend, evenredig en afschrikwekkend is.[226]

---

[215] Overweging 82 AVG; EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 28, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[216] Art. 25 3de lid AVG; art. 42 AVG.
[217] Art. 43 1ste lid AVG.
[218] EDPB, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 28, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[219] EDPB, "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation", 4 juni 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf
[220] Art. 58 1ste lid AVG.
[221] Art. 58 2de lid AVG.
[222] Art. 58 3de lid AVG.
[223] Art. 83 AVG.
[224] Art. 83 2de lid AVG.
[225] *Ibid*.
[226] Art. 83 1ste lid AVG.

4. De uitdagingen van privacy by design en default

4.1 Inleiding

Sinds de AVG haar intrede kent in 2018, is het aantal klachten bij de Autoriteit Persoonsgegevens op ruim 1 jaar tijd gestegen met zo'n 79 procent gestegen. De meerderheid van de klachten had betrekking op privacyschendingen, waaronder de schending van het recht op inzage en wissing.[227] Ook ontving de AP in 2019 27.000 meldingen van datalekken, wat een stijging is van meer dan 29 procent ten opzichte van 2018.[228] Uit onderzoek van de 'International Computer Security Association' bleek dat 78 procent van de bedrijven de AVG-verplichtingen een zware last vinden.[229] Desondanks de Algemene verordening Gegevensbescherming verwerkingsverantwoordelijken en verwerkers specifieke bepalingen voorschrijft, blijven uitdagingen zich voordoen. Dit hoofdstuk bespreekt drie mogelijke uitdagingen.

4.2 Een eerste uitdaging: het financieel draagvlak

Een eerste uitdaging voor verwerkingsverantwoordelijken en verwerkers is het nemen van passende technische en organisatorische maatregelen dat binnen het bedrijfsbudget blijft. Aangezien deze maatregelen in de ontwerpfase genomen moeten worden, kan dit op korte termijn financieel zwaar zijn voor kleine of nieuwe bedrijven. Met de steeds meer toenemende promoties van PET's, lijken deze technieken op het eerste zicht een kostelijke investering.[230]

De AVG geeft toezichthoudende autoriteiten het recht om bij inbreuken verschillende bevoegdheden uit te oefenen.[231] Zo kan de AVG geldelijke boetes geven die erg hoog kunnen oplopen.[232] Desondanks verplicht de verordening autoriteiten rekening te houden met verschillende elementen bij het opleggen van sancties. Een van die elementen zijn de uitvoeringskosten. Indien blijkt dat een desbetreffende maatregel financieel onmogelijk of buitensporig is, zal de toezichthoudende autoriteit hier rekening mee houden.[233]

PET's of Privacy Enhancing Technologies is de verzamelnaam voor verschillende technieken inzake informatiesystemen om persoonsgegevens te beschermen. Het gebruik van PET's heeft veel voordelen. Zo maken ze toepassingen mogelijk die anders onmogelijk zijn en automatiseren ze privacymaatregelen effectiever en efficiënter dan organisatorische procedures en handmatige activiteiten. Ze kunnen reeds bestaande technieken ook verder optimaliseren. Verder, geeft het gebruik van PET's een positieve uitstaling naar betrokkenen toe en wekt het vertrouwen op in het verwerkingsproces. Bovendien, kunnen de kosten van PET's beperkt worden mits er rekening wordt

---

[227] AP, "Forse stijging privacyklachten in 2019", 14 januari 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019.
[228] X, "De AVG na twee jaar: knelpunten en oplossingen", 2 september 2020, https://www.pwnet.nl/instroom/nieuws/2020/09/de-avg-na-twee-jaar-knelpunten-en-oplossingen-10135587?io_source=www.pwnet.nl&_ga=2.186955816.1052085973.1620812362-1750095038.1620812362.
[229] *Ibid.*
[230] C. HILLEN, "Privacy by design en privacy by default", 28 februari 2018, https://www.computable.nl/artikel/blogs/security/6310028/5260614/privacy-by-design-en-privacy-by-default.html.
[231] Art. 58 2de lid (i) AVG.
[232] Art. 83 4de – 5de lid AVG.
[233] Art. 25 1ste lid AVG; art. 32 1ste lid AVG.

gehouden met gegevensbescherming in het ontwerp. Deze technieken hebben zowel kwantitatieve als kwalitatieve baten voor organisaties, de maatschappij en de burgers.[234]

Er zijn meerdere classificaties van PET's mogelijk. De meeste classificaties hebben betrekking op de technische kenmerken ervan. Het AEDP deelt PET's in naargelang de doelen die ze nastreven. Ze worden dus ingedeeld naargelang hun doel om te beschermen of om te beheren. Privacybescherming combineert technieken en technologieën om de privacy te garanderen tijdens de gegevensverwerking, terwijl privacybeheer betrekking heeft op het behandelen van technieken en technologieën die procedures inzake privacybeheer ondersteunen.[235]

Privacybescherming
Door middel van pseudonimiseringstechnieken moeten transacties kunnen plaatsvinden zonder persoonsgegevens op te vragen. Met anonimiseringsproducten en diensten moeten betrokkenen recht hebben tot toegang van producten of diensten zonder zich te moeten identificeren. Versleutelingstechnieken moeten voorkomen dat documenten en transacties door derden geraadpleegd worden. Filters en blocker kunnen gebruikt worden om onnodige inhoud en e-mails te vermijden. Tot slot kunnen anti-trackers worden ingezet om de voetafdruk van de betrokkene weg te werken.[236]

Privacybeheer
Informatietechnieken kunnen gebruikt worden voor het opstellen en controleren van een privacybeleid. Administratieve technieken kunnen gebruikt worden om de identiteit en de toestemming van de betrokkene te beheren en te regelen.[237]

Op eerste zicht lijken goede technieken, systemen en applicaties een dure investering te zijn, maar op lange termijn zorgen ze voor een voordeligere situatie. Ondernemingen zullen namelijk minder negatieve gevolgen ervaren, doordat ze op lange termijn financieel voordeliger en tijdbesparend.

4.3 Een tweede uitdaging: Verwerkingsverantwoordelijken en verwerkers buiten de Unie

De AVG is van toepassing op verwerkingsverantwoordelijken en verwerkers die zich buiten de Unie bevinden, indien ze persoonsgegevens van EU-burgers verwerken met betrekking tot het aanbieden van goederen of diensten of het monitoren van hun gedrag.[238] Aangezien de verordening in deze gevallen van toepassing is, zijn verantwoordelijken en verwerkers verplicht om te voldoen aan DPbDD te voldoen.[239]

---

[234] Ministerie van binnenlandse zaken en Koninkrijksrelaties, "Privacy Enhancing Technologies - Witboek voor beslissers", december 2004, 13, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/technologie/witboek_pet.pdf.
[235] AEPD, "A guide to privacy by design", oktober 2019, 27, https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf
[236] *Ibid*.
[237] *Ibid*.
[238] Art. 3 2de lid AVG.
[239] Art. 25 AVG.

Het probleem is echter dat deze partijen vaak weinig kennis hebben inzake de AVG. Dit leidt tot snellere inbreuken op beginselen van gegevensbescherming en rechten en vrijheden van de betrokkene. Onlangs heeft de Nederlandse Autoriteit Persoonsgegevens zo'n verwerker een boete van ruim een half miljoen euro opgelegd. Locatefamily.com publiceerde namelijk allerlei gegevens zoals adressen en telefoonnummers zonder medeweten van EU-burgers. Doordat de zoeksite geen vertegenwoordiger heeft binnen de Unie, kan de Nederlandse Autoriteit Persoonsgegevens deze informatie niet laten schrappen.[240]

Het niet bezitten van de nodige kennis mag niet gebruikt worden als excuus. De richtlijnen van de EDPB omtrent de DPbDD zijn namelijk zeer uitgebreid en publiek toegankelijk. Iedere verwerkingsverantwoordelijke en verwerker kan deze richtlijnen gratis raadplegen en kan zich desnoods laten bijstaan door een expert om de juiste implementatie te waarborgen.[241]

4.4 Een derde uitdaging: de noodzakelijkheid van datawarehousing in het businessmodel

Zoals reeds besproken, houdt dataminimalisatie in dat zo min mogelijk gegevens worden verzameld. Enkel datgeen wat noodzakelijk is, mag volgens dit beginsel verzameld en verwerkt worden. De verplichting in de verordening gaat dus uit van een businessmodel waarbij zo weinig mogelijk wordt verzameld, terwijl persoonsgegevens net nodig zijn voor datawarehousing. Datawarehousing is het opslaan van informatie met als doel om zakelijke beslissingen te nemen, dat bijgevolg aan de basis van business intelligence ligt.[242] De AVG staat in beginsel dus haaks op het principe van datawarehousing.[243]

Dit probleem kan in beginsel eenvoudig worden opgelost door anonimisering en data fading. Door anonimisering[244] kan de data-analist de gegevens analyseren zonder dat een persoon geïdentificeerd of identificeerbaar wordt. Data fading is het verzamelen van persoonsgegevens die geleidelijk aan geaggregeerd worden. Zo heeft een onderneming de adresgegevens van de betrokkene enkel nodig om een product af te leveren. Na de levering is het adres niet meer noodzakelijk. Deze gegevens kunnen echter wel interessant zijn om te bepalen wat de beste locatie is om een toekomstige vestiging te openen. Hiervoor heeft de onderneming geen specifieke adresgegevens nodig, maar zou de locatie van een stad voldoende kunnen zijn. Datafading kan datawarehousing blijven garanderen.[245]

---

[240] X, "Privacywaakhond legt familiezoeksite boete van ruim een half miljoen euro op", 12 mei 2021, https://datanews.knack.be/ict/nieuws/privacywaakhond-legt-familiezoeksite-boete-van-ruim-een-half-miljoen-euro-op/article-news-1733353.html.
[241] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679 version 1.1", 4 mei 2020, 1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[242] X, "Datawarehousing", https://www.ictportal.nl/ict-lexicon/datawarehousing-dwh.
[243] E. DE WIT, "Dataminimalisatie en privacy by design: hoe minder data, hoe beter" 19 januari 2017, https://www.computable.nl/artikel/blogs/security/6310028/5260614/privacy-by-design-en-privacy-by-default.html.
[244] Overweging 26 AVG.
[245] E. DE WIT, "Dataminimalisatie en privacy by design: hoe minder data, hoe beter" 19 januari 2017, https://www.computable.nl/artikel/blogs/security/6310028/5260614/privacy-by-design-en-privacy-by-default.html; M. WARD, "Fading data could improve privacy", 16 juni 2010, https://www.bbc.com/news/10324209.

5. Hoe zou de wetgeving moeten zijn?

5.1 VK: het ICO

5.1.1 Inleiding

De ICO is de leidende toezichthoudende autoriteit die instaat voor de naleving van de voorschriften inzake gegevensbescherming in het Verenigd Koninkrijk.[246] Ze biedt advies en begeleiding, ze houdt toezicht op inbreukrapporten, behandelt klachten en voert audits en adviesbezoeken uit en neemt handhavingsmaatregelen indien nodig. Het ICO werkt samen met gegevensbeschermingsautoriteiten van andere landen, waaronder het Europees Comité voor gegevensbescherming (EDPB). Dat comité bevat tenslotte vertegenwoordigers van gegevensbeschermingsautoriteiten van elke EU-lidstaat.[247]

Op 25 mei 2018 trad de 'Data Protection Act 2018' in werking, dat een geüpdatet versie is van de 'Data Protection Act 1998'. Door de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie werd de privacywetgeving op 1 januari 2021 officieel gewijzigd. Het VK heeft zo een eigen Britse variant van de AVG uitgevaardigd dat grotendeels overeenkomt, maar op sommige vlakken werd aangepast om de uitvoering in het VK doeltreffender te maken. De Britse AVG wordt bovendien ook aangevuld door de DPA 2018.[248]

5.1.2 De Britse AVG en data protection by design en default

Net zoals de AVG vereist de Britse AVG een bepaling om passende technische en organisatorische maatregelen te treffen om gegevensbescherming effectief te implementeren om zo de rechten en vrijheden van de betrokkenen te beschermen.[249] Deze bescherming moet geïntegreerd zijn in het ontwerp en gedurende de hele levenscyclus van de verwerking. PbD is geen nieuw concept, aangezien het altijd al onderdeel is geweest van de vorige privacywetgeving. Een groot verschil is dat het onder de Britse AVG nu wel een verplichting is. [250]

5.1.2 Data protection by design

Om te voldoen aan PbD[251], moeten privacy en gegevensbeschermingskwesties in het ontwerp van elk systeem, dienst, product en processen worden geïntegreerd en dat gedurende de hele levenscyclus ervan. Zoals reeds besproken moeten hiervoor passende technische en organisatorische maatregelen en waarborgen genomen worden. De ICO benadrukt dat PbD een breed concept is en dat het betrekking kan hebben op verschillende elementen. Zo heeft PbD betrekking op het ontwikkelen van nieuwe IT-systemen, diensten, producten en processen die de verwerking van persoonsgegevens integreren. Het concept bevat ook de ontwikkeling van een organisatorisch beleid,

---

[246] EDPB, Informatie over bindende gegevensbeschermingsvoorschriften voor ondernemingen met de ICO als leidende toezichthoudende autoriteit Vastgesteld, 12 februari 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexit_nl.pdf.
[247] ICO, "Some basic concepts", https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/#9 (consultative op 5 april 2021).
[248] ICO, "About the DPA 2018", https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (consultative op 5 april 2021).
[249] Art. 25 lid VK AVG; art. 25 lid AVG.
[250] ICO, "The Guide to Data Protection", 11 mei 2016, 75.
[251] Art. 25 1ste lid VK AVG.

processen, bedrijfspraktijken en strategieën die het privacyreglement implementeren. Vanzelfsprekend heeft het ook betrekking op het fysiek ontwerp van de verwerking en het gebruik van persoonsgegevens voor nieuwe doeleinden. Dit zijn slecht enkele voorbeelden die de ICO aanhaalt.[252]

5.1.3 Data protection by default

Gegevensbescherming door standaardinstellingen[253] houdt in dat de gegevensbescherming standaard ervoor zorgt dat enkel gegevens worden verwerkt die noodzakelijk zijn voor het beoogde doel. De verwerkingsverantwoordelijke zal dus voor de verwerking plaatsvindt, de gegevens standaard moeten specifiëren. De maatregelen die de verwerkingsverantwoordelijke moet nemen, zijn afhankelijk van de omstandigheden en de risico's voor de betrokkene. In elk geval zal er rekening worden gehouden met een 'privacy eerst' benadering. De verantwoordelijke mag bovendien geen illusies wekken inzake de opties voor gegevensverwerking. Verder, mogen aanvullende gegevens enkel verwerkt worden met de toestemming van de betrokkene. De toestemming moet ook gegeven worden om persoonsgegevens openbaar te maken of om ze te delen met derden. Tot slot moeten betrokkenen hun rechten te allen tijde kunnen uitoefenen en moeten verantwoordelijken hier de nodige controle en opties voor voorzien.[254]

De ICO heeft in haar richtlijnen een korte checklist geïntegreerd zodat verwerkingsverantwoordelijken een snel beeld hebben over de naleving van DPbDD.[255] Zo moet de onderneming gegevensbeschermingskwesties als onderdeel zien van het ontwerp en deze implementeren in alle systemen, diensten, producten en bedrijfspraktijken. De bescherming moet vervolgens een essentieel deel uitmaken van de kernfunctionaliteit van de verwerkingssystemen. Vervolgens, moet de onderneming anticiperen op toekomstige risico's door preventieve maatregelen nemen om inbreuk en schade te voorkomen. Verder, mogen enkel persoonsgegevens verwerkt worden die noodzakelijk zijn voor de beoogde doeleinden. Bovendien, moeten persoonsgegevens automatisch beschermd zijn, zodat de betrokkene zelf geen specifieke actie moet ondernemen. De onderneming moet vervolgens transparant zijn over de identiteit en contactgegevens van de verwerkingsverantwoordelijke en dat zowel intern als naar de betrokkene toe. De onderneming moet bovendien een beleid in duidelijke taal hanteren, zodat de betrokkene gemakkelijk begrijpt wat er met de persoonsgegevens gebeurt. Zo moet de betrokkene ook kunnen bepalen hoe de persoonlijke gegevens gebruikt worden. De onderneming moet verder strenge privacy-instellingen en gebruikersvriendelijke opties integreren en alle voorkeuren van de betrokkene respecteren. Bovendien zou de onderneming enkel voor verwerkers mogen opteren die voldoende garanties bieden inzake technische en organisatorische maatregelen betreffende de PbD. Wanneer de onderneming beroep doet op ontwerpers of architecten en fabrikanten, moeten ook deze de gegevensbeschermingskwesties in acht nemen. Tot slot moet de onderneming PET's gebruiken om de naleving van DPbDD ondersteunen.[256]

[252] ICO, "Guide to the General Data Protection Regulation", 1 januari 2021, 177.
[253] Art. 25 2de lid VK AVG.
[254] ICO, "Guide to the General Data Protection Regulation", 1 januari 2021, 177.
[255] *Ibid.,* 174.
[256] *Ibid.,* 174-175.

Wat

Passende technische en organisatorische maatregelen kunnen niet door een 'one-size-fits-all methode' gepromoot worden, omdat ze afhankelijk zijn van de eigen omstandigheden. Het ICO benadrukt wel dat de gegevensbeschermingskwesties vanaf het begin van elke verwerkingsactiviteit in overwogen moeten worden, zodat er voldaan wordt aan de vereisten van gegevensbescherming door ontwerp en door standaardinstellingen. Dataminimalisering, pseudonimisering en het bieden van de nodige transparantie zijn hier enkele voorbeelden van. De opsomming is niet exhaustief, aangezien er veel meer vereist is dan deze voorbeelden. De ICO raadt verwerkingsverantwoordelijken om beroep te doen op een specialist, aangezien de richtlijnen geen complete gids zijn voor specifieke situaties.[257]

Wanneer

De ICO vermeldt dat PbD in de vroege beginfase van elk systeem, dienst, product of proces moet beginnen. Verwerkingsverantwoordelijken moeten dus bij het ontwerp rekening houden met verschillende factoren zoals de beoogde verwerkingsactiviteiten, de risico's voor betrokkenen en de bescherming van de rechten van betrokkenen. Bij het nemen van de passende technische en organisatorische maatregelen worden o.a. de stand van de techniek, de uitvoeringskosten en de aard van de verwerking in acht genomen. De Britse AVG bepaalt dat de maatregelen genomen moeten worden op het ogenblik dat de middelen van de verwerking bepaald zijn, m.a.w. de ontwerpfase of op het moment van de verwerking zelf, m.a.w. levenscyclus van de verwerkingsactiviteit.[258]

5.1.4 Toepassingsgebied DPbDD

De verwerkingsverantwoordelijke

In beginsel staat de verwerkingsverantwoordelijke in voor de naleving van de gegevensbescherming door ontwerp en door standaardinstellingen.[259] Afhankelijk van de interne organisatie, kan de 'verantwoordelijke' verschillen. Zo is het 'seniormanagement' verantwoordelijk voor een privacy-bewust cultuur te ontwikkelen en na te zien of het beleid in overeenstemming is met de gegevensbescherming. Vervolgens, zijn software-ingenieurs, systeemontwerpers en applicatieontwikkelaars ook verantwoordelijk om bij het ontwerp alle vereisten van gegevensbescherming te respecteren. Verder, benadrukt de ICO het belang van bedrijfspraktijken en het integreren van gegevensbescherming in alle processen en procedures.[260]

Wanneer de verantwoordelijke een inbreuk pleegt op de gegevensbescherming of de rechten en vrijheden van de betrokkene, kan de ICO boetes opleggen. Bij het bepalen van de boete wordt rekening gehouden met technische en organisatorische maatregelen die het bedrijf genomen heeft.[261] Bovendien, kan de ICO op grond van de DPA een handhavingsbericht uitvaardigen voor eventuele tekortkomingen.[262]

[257] ICO, "Guide to the General Data Protection Regulation", 1 januari 2021, 179.
[258] *Ibid.*, 179-189; Art. 25 VK AVG.
[259] Art. 25 VK AVG.
[260] ICO, "Guide to the General Data Protection Regulation", 1 januari 2021, 177.
[261] *Ibid.*, 177-178.
[262] Art. 149 UK Parliament, nr c.12, 23 mei 2018, Data Protection Act.

De verwerker

Wanneer een onderneming beroep doet op een andere organisatie om de gegevens te verwerken, spreekt de Britse AVG, net zoals de EU AVG, over een 'verwerker'.[263] Bij het kiezen van de verwerker moet de verwerkingsverantwoordelijke uitsluitend beroep doen op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen zodat de beginselen en de rechten van betrokkenen gewaarborgd worden.[264]

Andere partijen

Buiten verwerkingsverantwoordelijken en verwerkers kunnen ook andere partijen betrokken zijn bij de verwerkingsactiviteit, zoals fabrikanten, productontwikkelaars, applicatieontwikkelaars en serviceproviders. Dit wordt niet expliciet genoemd in artikel 25, maar kan wel teruggevonden worden in overweging 78. Desondanks deze partijen niet verplicht zijn om te voldoen aan de verplichting van DPbDD, moeten ze toch worden aangemoedigd om er rekening mee te houden tijdens de ontwikkeling en het ontwerpen van producten, diensten en systemen. Dit moet in overeenstemming zijn met 'de stand van de techniek'[265], zodat verwerkingsverantwoordelijken en verwerkers de vereisten van DPbDD kunnen naleven.[266]

Op het eerste zicht lijkt het dus dat de Britse AVG geen directe verplichtingen oplegt aan andere partijen, maar indirect doet het dat wel. Verwerkingsverantwoordelijken en verwerkers moeten namelijk de gegevensbescherming door ontwerp mee in hun overweging nemen bij het selecteren van systemen, diensten en producten. Het ICO benadrukt daarom dat ook ontwerpers en ontwikkelaars rekening moeten houden met de PbD aangezien dat een betere positie opbrengt.[267]

5.2 Frankrijk

5.2.1 Inleiding

De Franse regering kondigde in de jaren 70 een plan aan, genaamd SAFARI, om elke burger te linken aan een specifiek nummer om zo alle regeringsdocumenten met elkaar te kunnen verbinden. Dit plan leidde tot discussies en grote controverse bij de publieke opinie. Het volk vreesde dat gegevens over de hele Franse bevolking in dossiers gingen worden opgenomen. Genoodzaakt richtte de regering een commissie op dat concrete maatregelen moest aanbevelen om de privacy en de rechten en vrijheden van betrokkenen te garanderen bij nieuwe ontwikkelingen in de informatietechnologie.[268]

De CNIL of de 'Commission Nationale de l'Informatique et des Libertes' werd opgericht in 1978.[269] Het is een onafhankelijke administratieve autoriteit die haar taken uitoefent in overeenstemming met de Franse wetgeving inzake gegevensbescherming. De voorzitter stelt de agenda op, waarna de

[263] Art. 28 VK AVG; art. 28 AVG.
[264] Art. 28 1ste lid VK AVG; art. 28 1ste lid AVG.
[265] pg 33
[266] Overweging 78 VK AVG; Overweging 78 AVG.
[267] ICO, "Guide to the General Data Protection Regulation", 1 januari 2021, 177-178.
[268] CNIL, "The CNIL's mission", https://www.cnil.fr/en/cnils-missions (consultatie 4 april 2021).
[269] Art. 11 Act nr. 78-17, 6 januari 1978 on information technology, data files and civil liberties.

leden wekelijks in plenaire vergaderingen samenkomen. Tijdens deze vergaderingen worden wetsvoorstellen en ontwerpbesluiten voorgelegd door de regering voor een officieel CNIL-advies. Aanvullend kan de CNIL ook machtiging verlenen voor de verwerking van gevoelige gegevens in bepaalde gevallen. Tot slot analyseert de organisatie ook de gevolgen en mogelijke risico's van nieuwe informatietechnologieën voor het privéleven van betrokkenen.[270]

5.2.2 De CNIL

Als algemene taak informeert de CNIL de burgers over hun rechten inzake de gegevensbescherming. Advies en informatie wordt zowel aan particulieren als bedrijven gegeven. De organisatie maakt gebruik van de pers, de website, sociale netwerken en workshops om dit te doen. De CNIL neemt bovendien ook deel aan conferenties en seminars om te informeren en geïnformeerd te worden.[271]

Wanneer burgers moeilijkheden ondervinden bij het uitoefenen van de rechten inzake gegevensbescherming, kunnen zij contact opnemen met de CNIL. De CNIL kan de burger effectieve toegang verlenen tot zijn/haar gegevens in elk stadium van de verwerking. Iedere burger heeft namelijk het recht op toegang tot zijn of haar persoonsgegevens, recht om geïnformeerd te worden, recht om bezwaar te maken en om de gegevens te corrigeren. Ook het recht op toegang tot bestanden van nationale veiligheid, defensie en openbare veiligheid is een recht dat op legitieme gronden kan worden gewaarborgd. De CNIL heeft hier indirecte toegang tot.[272]

Het adviseren over gegevensbescherming gebeurt op verschillende wijzen. Dit kan onder andere door officiële adviezen te geven over wetsvoorstellen, door wettelijke kaders die de eerbiediging van eerdere formaliteiten vereenvoudigen of door aanbevelingen te geven aan verwerkingsverantwoordelijken en gegevensbeschermingsfunctionarissen.[273]

De CNIL kan door verschillende actiemiddelen de beginselen inzake gegevensbescherming garanderen. Opmerkelijk heeft ze de bevoegdheid om 'privacyzegels' af te leveren voor producten, procedures en systemen die gegevensbescherming garanderen. Deze zegels zorgen er namelijk voor dat bedrijven voor kwaliteit kiezen. De bedrijven die zulke zegels krijgen, worden op positieve wijze onderscheiden, dat bovendien als vertrouwensindicator voor gebruikers kan dienen.[274]

Verder, zet de CNIL in op innovatie en toekomstperspectieven onder andere door in een zeer vroeg stadium rekening te houden met nieuwe tendensen en technologieën. Bovendien bezit de organisatie een laboratorium waarin geavanceerde producten en applicaties worden getest om zo de mogelijke impact op het privéleven te evalueren. Met het oog op PbD wil de CNIL haar adviserende rol versterken en garanderen dat vereisten inzake gegevensbescherming in technologische

[270] CNIL, "The CNIL's mission", https://www.cnil.fr/en/cnils-missions (consultatie 4 april 2021).
[271] CNIL, "The CNIL in a nutshell - Protect personal data, Accompany innovations, Preserve civil liberties", 2019, 4, https://www.cnil.fr/sites/default/files/atoms/files/the-cnil-in-a-nutshell.pdf.
[272] CNIL, "The CNIL in a nutshell - Protect personal data, Accompany innovations, Preserve civil liberties", 2015, 3, https://linc.cnil.fr/sites/default/files/typo/document/CNIL_EN_BREF-VEN-VD.pdf
[273] CNIL, "The CNIL in a nutshell - Protect personal data, Accompany innovations, Preserve civil liberties", 2015, 3, https://linc.cnil.fr/sites/default/files/typo/document/CNIL_EN_BREF-VEN-VD.pdf.
[274] *Ibid*., 5.

ontwikkelingen worden geïmplementeerd. De organisatie wil bijdragen naar ontwikkelen van technologische oplossingen die het privéleven beschermen.[275]

De CNIL bezit verschillende bevoegdheden bij het vaststellen van inbreuken op gegevensbescherming. De organisatie kan waarschuwingen geven, die eventueel openbaar wordt gemaakt, aanvullende dwingende sancties en gelboetes uitvaardigen. Verder, kan er ook een bevel tot staken van de verwerking worden uitgeroepen en kan de reeds gegeven machtiging worden ingetrokken. Bij onmiddellijke en ernstige schendingen van fundamentele rechten en vrijheden kan de CNIL de bevoegde rechter verzoeken om de nodige veiligheidsmaatregelen te treffen.[276]

Opmerkelijk is dat CNIL promotiecampagnes inzake gegevensbescherming voert in Franstalige landen. Deze campagnes zorgden in 2007 voor de oprichting van de 'Association Francophone des Autorités de Protection des Données Personnelles' die samenwerkt met de Internationale Organisatie van La Francophonie (OIF). Dit succes leidde tot wetgeving inzake privacyrechten in Franstalige landen zoals Marokko.[277]

5.2.3 Welke privacyregels zijn er toepasselijk in Frankrijk?

De eerste Franse wetgeving inzake gegevensbescherming trad in werking op 6 januari 1978 en werd ondertussen twee keer gewijzigd.[278] De eerste wijziging vond plaats in 2004 na de privacyrichtlijn[279] en de tweede in 2016 na de 'Digital Republic Act'.[280] De huidige Franse wet inzake gegevensbescherming werd aangenomen op 20 juni 2018, in overeenstemming met AVG. De nieuwe Franse wet betreffende de gegevensbescherming is samengesteld uit 72 artikelen en bevat de wijzigingen die zijn aangebracht in de vorige Franse wet inzake de gegevensbescherming. Op sommige vlakken vervangt de GDPR de nationale wetgeving, zoals o.a. bij de rechten van betrokkenen en veiligheidsmaatregelen. Op andere gebieden laat het invulling door nationale wetgeving toe. Het kader omtrent gegevensbescherming is dus samengesteld uit de nationale Franse wetgeving en de Europese wetgeving.[281]

5.2.4 Hoe zit het met privacy by design en default?

Wanneer we de website van de CNIL bekijken, zien we dat er in elke 'Guideline' gerefereerd wordt naar ofwel de WP29 ofwel de nieuwe Guidelines van de EDPB. We kunnen bijgevolg besluiten dat deze hetzelfde zijn zoals in de EU GDPR.

---

[275] *Ibid*.
[276] *Ibid.,* 6.
[277] *Ibid.*
[278] Act nr. 78-17, 6 januari 1978 on information technology, data files and civil liberties.
[279] Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.
[280] A. DAZY, "New French Digital Republic Law boosts support for OA and TDM", 2016, https://www.openaire.eu/blogs/new-french-digital-republic-law-boosts-support-for-oa-and-tdm-1; the French Law for a Digital Republic Act nr 2016-1321, 7 oktober 2016 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/.
[281] X, "French Data Protection Law Act: What's new", 4 december 2018, https://www.dreyfus.fr/en/2018/12/04/french-data-protection-act-whats-new/

5.3 California
5.3.1 Inleiding

De toenemende rol van technologie, gegevens en het delen van persoonlijke informatie heeft ook overzees geleid tot een groter risico van ongeoorloofd gebruik van persoonlijke informatie. Steeds meer bedrijven verzamelen persoonlijke informatie, zoals de gezinssituatie, financiële informatie, en de geolocatie van consumenten. Het ongeoorloofd publiek maken en misbruiken van persoonlijke informatie kunnen zeer ernstige en negatieve gevolgen met zich meebrengen. Financiële fraude, identiteitsdiefstal en emotionele stress zijn hier enkele voorbeelden van. Het Cambridge Analytica schandaal dat in 2018 aan het licht kwam, zorgde voor veel frustratie en boosheid. Tientallen miljoenen mensen werden slachtoffer door dit dataminingbedrijf, waardoor duidelijk werd dat gegevensverwerkers meer verplichtingen en consumenten meer controle moeten krijgen.[282] Om toekomstig misbruik te vermijden, nam de staat California als eerste Amerikaanse staat een uitgebreide privacywet aan, de California Consumer Privacy Act.[283] De CCPA zal echter op 1 januari 2023 vervangen worden door een nieuwe wet, de California Privacy Rights and Enforcement Act.[284] De CPRA zal van toepassing zijn op persoonsgegevens die verzameld worden vanaf 1 januari 2022. Tot dan moeten bedrijven voldoen aan de CCPA.[285]

5.3.2 De CalOPPA

De California Online Privacy Protection Act heeft betrekking op websites en online bedrijven die persoonsgegevens van consumenten uit Californië verzamelen of gebruiken. Opmerkelijk is dat de CalOPPA bepaalde vereisten stelt voor de inhoud van het privacybeleid van commerciële websites. Zo moet er vermeld worden welke type persoonlijke informatie er wordt verzameld en wat de beweegredenen hiervoor zijn. De onderneming zal ook melding moeten maken wanneer deze gegevens met een derde worden gedeeld. Deze wetgeving is van kracht sinds 2004 en is een van de belangrijkste online privacywetgevingen in de VS. De CalOPPA zal in dit hoofdstuk niet verder besproken worden, aangezien het enkel betrekking heeft op privacybeleiden van commerciële websites.[286]

De CCPA is een privacywet die sinds 2020 van kracht is en gezien wordt als 'aanvulling' op de CalOppa, hoewel dat niet volledig zo is. De CCPA introduceert aanvullende rechten voor consumenten die websites en onlinebedrijven moeten respecteren. Vervolgens wordt de definitie van 'persoonlijke informatie' breder gemaakt in de CCPA, om een grotere bescherming te bieden. Bovendien moeten ondernemingen meer transparantie bieden betreffende de verkoop van persoonsgegevens. Tot slot

---

[282] Art. 375 sec. 2 Governor nr. SB-1121, 23 september 2018, California Consumer Privacy Act
[283] Governor nr. SB-1121, 23 september 2018, California Consumer Privacy Act; L. JEHL, A. FRIEL, "CCPA and GDPR Comparison Chart", 2018, 3, https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf.
[284] X, "The California Privacy Rights Act of 2020", 2020, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/.
[285] J. KING ALLEN, "Worldwide: California Privacy law vs GDPR", 5 maart 2021, https://www.mondaq.com/unitedstates/privacy-protection/1043204/california-privacy-law-vs-gdpr#:~:text=In%20the%20European%20Union%2C%20the,CCPA)%20provides%20protection%20for%20consumers.&text=The%20CPRA%20will%20go%20into,as%20of%20January%201%2C%202022.
[286] X, "CalOPPA vs CCPA: What You Must Know to Comply With Both", 26 januari 2021, https://www.websitepolicies.com/blog/caloppa-vs-ccpa

introduceert de CCPA een nieuwe reeks boetes voor ondernemingen die de persoonsgegevens niet voldoende beschermen. Beide wetgevingen hebben hetzelfde doel, nl. de gegevens beschermen van de inwoners van Californië beschermen.[287]

De CCPA vertoont enkele vergelijkbare elementen met de AVG. Beiden bevorderen de transparantie over het gebruik van gegevens en bieden grotendeels dezelfde rechten, zoals het recht op toegang. Desalniettemin vertonen ze ook verschillen.[288] Het doel van dit hoofdstuk is dan ook om kort de verschillen en gelijkenissen te bespreken, onderzoek te doen naar DPbDD in de CCPA en om te concluderen welke wetgeving consumentvriendelijker is.

5.3.3 Het toepassingsgebied

5.3.3.1 Personeel toepassingsgebied

Onder de AVG zijn zowel bedrijven en openbare instellingen als non-profitorganisaties onderworpen aan de wetgeving.[289] De CCPA is op dit vlak anders, aangezien enkel entiteiten met een winstoogmerk, nl. bedrijven, onder de CCPA vallen.[290] Zowel de AVG als de CCPA zijn van toepassing op ondernemingen die doeleinden en middelen bepalen voor de verwerking. Belangrijk om te benadrukken is dat de CCPA consumenten beschermt, die natuurlijke personen en bewoner zijn van Californië. De AVG is op dit vlak veel breder en beschermt alle betrokkenen[291], in de zin van 'alle natuurlijke personen' zonder vereiste voor ingezetenschap of burgerschap.[292]

Om terug te komen op bedrijven die onder de CCPA vallen, heeft de wetgeving specifieke voorwaarden vastgelegd. Zo moet het gaan om een bedrijf met een winstoogmerk die in California actief is, die de persoonlijke informatie van consumenten verzamelt en die de doeleinden en de middelen van de verwerking bepaalt. Bovendien zet de wetgeving ook enkele drempelvoorwaarden uiteen die niet cumulatief moeten worden toegepast. Zo kan het bedrijf een bruto-omzet hebben van 25 miljoen euro. Een andere voorwaarde is het jaarlijks kopen, ontvangen voor commerciële doelen, het verkopen of delen van persoonlijke informatie van meer dan 50.000 consumenten, huishoudens of apparaten voor commerciële doeleinden. Ook kan de CCPA toepasselijk zijn op bedrijven die meer dan 50% van de jaarlijkse inkomsten haalt uit de verkoop van persoonlijke informatie. Andere entiteiten die het bedrijf besturen of bestuurd worden, zijn ook verworpen aan de CCPA.[293]

---

[287] X, "CalOPPA vs CCPA: What You Must Know to Comply With Both", 26 januari 2021, https://www.websitepolicies.com/blog/caloppa-vs-ccpa.
[288] J. KING ALLEN, "Worldwide: California Privacy law vs GDPR", 5 maart 2021, https://www.mondaq.com/unitedstates/privacy-protection/1043204/california-privacy-law-vs-gdpr#:~:text=In%20the%20European%20Union%2C%20the,CCPA)%20provides%20protection%20for%20consumers.&text=The%20CPRA%20will%20go%20into,as%20of%20January%201%2C%202022.
[289] Art. 2 1ste lid AVG.
[290] Art. 1798.140 (c) CCPA.
[291] Art. 4 1ste lid AVG.
[292] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 7-8, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[293] *Ibid.;* Art. 1798.140 (c) CCPA.

5.3.3.2 Territoriaal toepassingsgebied

Zoals besproken in het eerste hoofdstuk, is de AVG van toepassing op verwerkingsverantwoordelijken en verwerkers binnen de Europese Unie. In de gevallen wanneer de verwerker buiten de EU is gevestigd en goederen of diensten aanbiedt aan EU-burgers of het gedrag van personen binnen de EU monitort, is de AVG ook van toepassing.[294] De CCPA is toepasselijk op bedrijven die commercieel actief zijn in Californië.[295] Hoewel de CCPA het niet expliciet vermeldt, is het ook van toepassing op bedrijven die buiten California gevestigd zijn en gegevens van consumenten verzamelt of verkoopt in California.[296]

5.3.3.3 Materieel toepassingsgebied

Het materieel toepassingsgebied van de AVG en de CCPA vertonen op enkele vlakken overlappingen. De AVG is van toepassing op alle soorten verwerking (zoals het verzamelen, gebruiken, verspreiden, structureren etc.) al dan niet door een geautomatiseerd procedé.[297] Uit de CCPA kan worden afgeleid dat de verwerking betrekking heeft op het verzamelen, verkopen of delen van persoonlijke informatie, ongeacht of het door een geautomatiseerd procedé plaatsvindt. Geanonimiseerde gegevens onder de CCPA leiden net zoals bij de AVG tot een uitsluiting van de bepalingen.[298] De CCPA vermeldt ook de uitsluiting voor verwerking van niet-geïdentificeerde gegevens, maar vult dit aan met verwerking van "geaggregeerde consumenteninformatie". Dit laatste is het geval wanneer de gegevens niet naar de individuele persoon verwijzen, maar naar een groep van consumenten. De AVG sluit de verwerking van gegevens door een natuurlijke persoon voor strikt persoonlijke of huishoudelijke activiteiten uit.[299] De CCPA doet dit ook, alhoewel het ook een onderneming kan betreffen in het kader van niet-commerciële activiteiten.[300]

In tegenstelling tot de AVG biedt de CCPA specifieke uitsluitingen waarbij verwerking niet onder de bepalingen valt, zoals bijvoorbeeld bij medische informatie en beschermde gezondheidsinformatie.[301] Opmerkelijk is dat beiden wetgevingen niet van toepassing zijn op vlak van rechtshandhaving en nationale veiligheid, hoewel ze dat wel kunnen zijn op bedrijven die deze diensten verlenen.[302]

5.3.4 Beginselen inzake verwerking van persoonsgegevens

5.3.4.1 Persoonsgegevens

De term 'persoonlijke gegevens' is onder de AVG ruim gedefinieerd, net zoals bij onder de CCPA. De AVG omschrijft 'persoonsgegevens' als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon op een directe of indirecte wijze aan de hand van een indicator of kenmerkende

---

[294] Art. 3 AVG.
[295] Section 1798.140 (d)-(e) CCPA.
[296] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 8-9, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[297] Art. 2 1ste lid AVG; art. 4 1ste lid AVG.
[298] Sections 1798.140 (o) (1) CCPA; Overweging 26 AVG.
[299] Art. 2 2de lid (c) AVG.
[300] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 11, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[301] *Ibid.*
[302] *Ibid.*

elementen.[303] De CCPA definieert de persoonlijke informatie als 'informatie die identificeert, betrekking heeft op, beschrijft, kan worden geassocieerd met, direct of indirect verband houdt met een consument of huishouden'.[304] Alhoewel de AVG niet expliciet 'huishoudens' vermeldt, kunnen persoonsgegevens ook huishoudens omvatten.[305]

Wanneer een verwerker informatie verzamelt dat publiek toegankelijk is, valt het nog steeds onder de AVG terwijl de CCPA dit uitsluit. Er moet echter wel een verschil gemaakt worden tussen de definities. De CCPA is niet toepasselijk op verwerking van informatie die op wettige wijze beschikbaar is gemaakt uit registers van de federale, staats- of lokale overheid, als die gegevens worden gebruikt voor een doel dat compatibel is met het doel waarvoor de gegevens worden bewaard en beschikbaar worden gemaakt in de regeringsdocumenten waarvoor ze openbaar zijn gehandhaafd.[306] Wat betreft biometrische gegevens van de consument die verzameld zijn door een onderneming, is de CCPA wel nog toepasselijk.[307] De AVG heeft bovendien een afzonderlijke bepaling met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens en verbiedt de verwerking waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging of lidmaatschap van vakbond blijken.[308] Bovendien verbiedt het ook om genetische en biometrische gegevens te verwerken om een uniek persoon te identificeren of dienst gezondheid of geaardheid. Enkel onder voorwaarden zijn uitzonderingen mogelijk.[309] Hoewel de CCPA biometrische gegevens definieert en het beschermt onder persoonlijke informatie[310], heeft het geen afzonderlijk regime voor bijzondere categorieën van persoonsgegevens. Wat betreft de verwerking van medische gegevens over gezondheid, sluit de CCPA de toepassing van de wet uit.[311]

5.3.4.2 Verwerker en verwerkingsverantwoordelijken

Zoals eerder besproken heeft de AVG enkele verplichtingen die zowel van toepassing zijn op verwerkingsverantwoordelijken als verwerkers. De verantwoordelijke bepaalt het doel en de middelen en de verwerker voert de verwerking uit.[312] De CCPA bevat ook enkele verplichtingen voor de verwerkingsverantwoordelijke en de verwerker. Hoewel er gelijkenissen zijn tussen verwerker en dienstverlener, omvat de AVG meer directe en gedetailleerde verplichtingen dan de CCPA. Zo moeten verwerker en verwerkingsverantwoordelijke in een overeenkomst of via een andere rechtshandeling vastleggen wat het onderwerp de duur, de aard en het doel zijn van de verwerking, alsook de soort persoonsgegevens en de categorieën van betrokkenen dat verwerkt worden en de

[303] Art. 4 1ste lid AVG.
[304] Sections 1798.140 (o) CCPA.
[305] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 13, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[306] *Ibid.,* 15.
[307] Sections 1798.140 (b) CCPA.
[308] Art. 9 1ste lid AVG.
[309] Art. 9 2de lid AVG.
[310] Sections 1798.140 (b) CCPA.
[311] Sections 1798.145 (c) CCPA.
[312] Art. 4 AVG; art. 7-8 AVG.

rechten en verplichtingen van de verwerkingsverantwoordelijke.[313] De CCPA vereist ook een contract tussen de onderneming en de dienstverlener, maar met minder verplichtingen.[314]

5.3.4.3 Beginselen

Beide wetgevingen hebben een definitie voorzien voor pseudonimisering die bovendien ook erg lijken op elkaar. Onder beide definities kan geconcludeerd worden dat pseudonimisering inhoudt dat persoonsgegevens op een zekere manier verwerkt worden, zodat een persoon niet meer geïdentificeerd of identificeerbaar is zonder aanvullende informatie te gebruiken. Deze aanvullende informatie moet door technische en organisatorische maatregelen apart worden bewaard zodat de persoonsgegevens deze niet gekoppeld of gelinkt kunnen worden aan geïdentificeerde of identificeerbaar persoon.[315] Zowel de AVG als de CCPA bepalen dat verwerkingsverantwoordelijken en bedrijven in bepaalde gevallen niet verplicht zijn om aanvullende gegevens bij te houden. Het grootste verschil is echter dat onder de AVG aanvullende gegevens door betrokkenen bij heridentificatie zelf kunnen worden verschaft, terwijl dat bij de CCPA ook is in het geval van recht op toegang'.[316]

5.3.4.4 Kinderen

De AVG benadrukt speciale bescherming voor de verwerking van persoonsgegevens van kinderen inzake de aanbieding van diensten of het leveren van producten in een informatiemaatschappij.[317] De CCPA heeft ook een speciale regeling betreffende het 'verkopen' van gegevens van kinderen, dat echter niet enkel beperkt is tot diensten van de informatiemaatschappij.[318]

De AVG laat lidstaten toe om de leeftijd voor een geldige toestemming te verlagen van 16 jaar tot 13 jaar, zonder de vereiste van toestemming of machtiging van ouderlijk gezag. De CCPA daarentegen verplicht ondernemingen om toestemming te krijgen volgens de 'opt-in' voor kinderen onder de 16 jaar, wanneer bedrijven de leeftijd wisten of weten. Wat betreft kinderen onder de 13 jaar, moet de verkoop van gegevens bevestigd zijn door de ouder of de voogd. Onder de CCPA wordt de onderneming geacht feitelijke kennis te hebben wanneer ze de leeftijd van het kind negeert door geen aandacht te schenken.[319]

Onder de AVG is de verwerkingsverantwoordelijke verplicht om passende maatregelen te nemen om informatie met betrekking tot de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm te verstrekken, gebruikmakend van duidelijke taal, die het kind gemakkelijk begrijpt. Een verwerkingsverantwoordelijke die niet 'op de hoogte' was van de leeftijd,

---

[313] Art. 28 AVG.
[314] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 17-19, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[315] Art. 4 5de lid AVG; art. 11 AVG; overwegingen 26 AVG; overweging 28 AVG; Sections 1798.140 (r) CCPA.
[316] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 16, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[317] Art. 8 AVG; Sections 1798.120 (c) CCPA.
[318] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 19-20, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[319] *Ibid.*

zal bijgevolg nog steeds aansprakelijkheid gehouden worden terwijl de CCPA wel nog een uitzondering wat betreft dit voorziet.[320]

5.3.4.5 Rechtmatigheid van de verwerking

De AVG heeft een specifieke bepaling toegewijd aan de gronden voor rechtmatige verwerking.[321] In tegenstellig tot de AVG, bevat de CCPA geen lijst met gronden die voorafgaand moeten worden getoetst bij het verzamelen, verkopen en vrijgeven van persoonlijke informatie. Het voorziet enkel een a posteriori mechanisme, namelijk dat consumenten zich kunnen afmelden voor de verkoop van persoonsgegevens.[322]

5.3.4.6 Rechten van betrokkenen

De rechten van individuen onder de AVG en de rechten van consumenten onder de CCPA komen grotendeels overeen, op enkele uitzonderingen na. Onder de AVG worden de rechten opgesomd vanaf artikel 12 tot en met artikel 23. Onder de CCPA vinden we ze terug in secties 1798.100 - 1798.199.100.[323]

5.3.4.7 Sancties

Ook op vlak van sancties zien we dat de AVG en de CCPA bevoegdheden verlenen om inbreuken te bestraffen. Het grootste verschil is dat geldelijke sancties onder de AVG gegeven worden door toezichthoudende overheden, terwijl de CCPA geldelijke sancties als een burgerlijke straf ziet, dat door de rechter moet worden uitgesproken.[324]

5.3.5 De CCPA inzake privacy by design en default

De CCPA bevat een bepaling dat het meest aansluit bij DPbDD dat als volgt luidt; *"A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section".*[325]

Bedrijven moeten de gebruikers dus inlichten over de categorieën van gegevens die verzameld worden en het doel waarvoor deze zullen worden gebruikt. Het is dus verboden voor bedrijven om

---

[320] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 19-20, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[321] Art. 6 AVG; Sections 1798.120 (c) CCPA.
[322] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 23, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.
[323] *Ibid.,* 26.
[324] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 37, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.; art. 83-84 AVG; sections 1798.155 CCPA.
[325] Section 1798.100(b) CCPA.

de gegevens voor niet-genoemde doeleinden te gebruiken. In tegendeel tot de CCPA gaat de impact van de AVG betreffende DPbDD[326] veel verder.[327]

Privacy geïmplementeerd in het ontwerp van een systeem of software voorkomt dat bedrijven achteraf problemen krijgen. Bedrijven zijn beter uitgerust om de bescherming van persoonsgegevens te garanderen en datalekken te voorkomen. Het implementeren in het ontwerp zou dus goedkoper zijn voor lange termijn, aangezien de kosten om het probleem op te lossen of een eventuele rechtszaak te doorlopen erg hoog kunnen oplopen. Dit gebeurde namelijk in 2018. Het Cambridge Analytica schandaal, waarbij Facebook inbreuk pleegde op de beveiliging van meer dan 50 miljoen gebruikers, zorgde voor heel veel vrees en een publiekelijk onveilig gevoel. Namen, e-mailadressen, telefoonnummers, wachtwoorden enz. werden zo openlijk blootgesteld. In Californië werd namens de 50 miljoen gebruikers een groepsvordering gestart en werd het privacybeleid van Facebook in vraag getrokken. De lakse beveiligingsmaatregelen in het beleid hebben namelijk geleid tot de inbreuk.[328] Naast Facebook zijn er tal van andere bedrijven die inbreuken plegen op de gegevensbescherming.[329]

Het probleem is dat ondernemingen het vaak financieel niet kunnen veroorloven op proactief te zijn en dus daarom liever reactief werken. Zoals reeds besproken leidt dit echter niet tot de beste en goedkoopste oplossing op lange termijn. De AVG geeft bedrijven geen keuze om al dan niet aan de maatregelen te voldoen, waardoor betrokkenen meer beschermd worden. Wanneer buitenlandse ondernemingen actief willen zijn in de EU, zullen dus ook zij de nodige maatregelen en waarborgen moeten treffen in de zin van artikel 25 GDPR.[330]

5.3.5.1 De CPRA

De California Privacy Rights Act breidt de rechten binnen de bestaande CCPA uit. De CPRA bouwt voort op de principes van gegevensminimalisatie en biedt meer controle en transparantie aan de consument met betrekking tot het gebruik en verzamelen van persoonlijke gegevens. De CPRA kan zorgen voor nieuwe mogelijkheden voor softwareontwikkelaars en onafhankelijke softwareleveranciers die overschakelen naar de privacy by design softwareontwikkeling.[331]

De CPRA zal net zoals de AVG een specifieke bepaling voor 'gevoelige gegevens' introduceren, denk dan aan ras en etnische afkomst, seksuele geaardheid, politieke overtuiging etc. De consument zal voor deze verwerking zijn/haar expliciete toestemming moeten geven en heeft het recht het gebruik hiervan te beperken. De CPRA zal ook leiden tot nieuwe technologische mogelijkheden, aangezien

[326] art. 25 AVG.
[327] S. SARAIVA, "Data Protection through Privacy by Design", 9, https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments.pdf.
[328] M. KAMINSKY, "Facebook Faces Class Action Over Security Breach That Affected 50 Million Users", https://www.forbes.com/sites/michellefabio/2018/09/30/facebook-faces-class-action-over-security-breach-that-affected-50-million-users/?sh=6b9984777b6c.
[329] S. SARAIVA, "Data Protection through Privacy by Design", 11, https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments.pdf.
[330] Ibid., 12; art. 3 AVG.
[331] J. MCCALL, "CPRA Pushes "Privacy by Design" Shift for Software Developers", 25 september 2020, https://www.devprojournal.com/technology-trends/data-privacy/cpra-pushes-privacy-by-design-shift-for-software-developers/.

de lat behoorlijk hoger wordt gelegd dan de huidige wetgeving. Zo zullen operationele-en systeemupgrades onmiskenbaar zijn op het gebied van gegevensverzameling, opslag, beheer en beveiliging. Deze technologische behoeftes zullen betrekking hebben op technieken zoals datamapping en dataminimalisatie.[332]

In bepaalde gevallen moeten persoonlijke gegevens in het hele IT-landschap van een organisatie worden bijgehouden. Zo zullen eigenaars van de gegevens worden toegewezen om het datagebruik binnen hun domein van het IT-landschap te regelen en om eventuele gegevensoverdrachten te beheren. Vervolgens, moeten ondernemingen in het kader van gegevensminimalisatie enkel de gegevens verzamelen die noodzakelijk zijn om de interactie of transactie te voltooien. Bovendien, zullen ondernemingen de gegevens die niet meer noodzakelijk zijn voor het doel, moeten anonimiseren. Zo worden risico's op datalekken gereduceerd. Tot slot moeten ondernemingen ingaan op de verzoeken om toegang te krijgen tot gegevens. Zonder automatisering zal dit kostenprijsje snel oplopen tot $ 1.400 per verzoek. Ondernemingen zullen dus op zoek moeten gaan naar oplossingen die veiliger en efficiënter verlopen. Het gebruik van PET's wordt sterk aangeraden.[333]

5.3.5.2 Sancties

Zoals eerder besproken zal de naleving van de maatregelen in het begin kostelijk zijn, maar niet op lange termijn. Echter, zal de niet-naleving ook kosten met zich meebrengen. Onder de CCPA heeft de procureur-generaal van Californië de bevoegdheid om de verordening af te dwingen, maar onder de CPRA zal hier een nieuwe instantie voor worden opgericht, namelijk de California Privacy Protection Agency. De instelling heeft autoriteit en jurisdictie en kan zware monetaire sancties opleggen voor de niet-naleving. Bovendien worden straffen van overtredingen m.b.t kinderen onder de 16 jaar verdrievoudigd. De niet-naleving van de wetgeving kan er ook voor zorgen dat het vertrouwen van de consument wordt beschaamd wat bijgevolg even ernstig kan zijn als financiële verliezen.[334]

5.3.6 Privacy by design raakt de kern van gegevensbeveiliging

Softwareontwikkelaars in California zullen een mentaliteitsverandering moeten ondergaan. Privacy is namelijk niet enkel een toegevoegde waarde of een louter element, maar het is de kern. Het zou dus in elk systeem moeten worden ingebouwd en tijdens de hele levenscyclus moeten worden gewaarborgd. Zo zouden privacy, veiligheid en transparantie de kernwaarden van de softwareontwikkelaar moeten zijn die tevens in elk systeem worden geïncorporeerd. Op lange termijn zullen deze ontwikkelaars en ontwerpers gezien worden als belangrijke speler betreffende privacy en oplossingen, wat enkel maar voordelig kan zijn.[335]

---

[332] J. MCCALL, "CPRA Pushes "Privacy by Design" Shift for Software Developers", 25 september 2020, https://www.devprojournal.com/technology-trends/data-privacy/cpra-pushes-privacy-by-design-shift-for-software-developers/.
[333] *Ibid.*
[334] X, "California Officials Announce California Privacy Protection Agency Board Appointments", 17 maart 2021, https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/.
[335] *Ibid*.

Hoewel noch de CCPA en noch de CPRA expliciet data protection by design voorschrijven, gaat de CPRA wel die richting uit. De CPRA zal ook enkele fundamentele principes van de AVG bevatten. Dataminimalisatie, dataretentie en het herkennen van categorieën als gevoelige persoonlijke informatie hier voorbeelden van. Applicaties die de verzameling van gegevens beperken en de gegevens in de volledige levenscyclus volgen, waarbij regelmatig onnodige gegevens worden verwijderd, zullen de bepalingen van de CPRA eerbiedigen. Desondanks er niet expliciet 'privacy by design' wordt vermeld, legt de CPRA de lat hoger. Het zet ondernemingen en softwareontwikkelaars aan om gegevensbescherming in nieuwe systemen en applicaties te implementeren. Indirect bevat de CPRA dus wel het principe van privacy by design, wat baandoorbrekend is in de Amerikaanse privacyregelgeving. Zullen bedrijven deze indirecte verplichtin met open armen ontvangen of zullen zij dit zien als blokkade?[336]

[336] E. T. DAVIS, A. VAN MARTER, "Privacy by design—opportunity or roadblock?", 3 maart 2021, https://www.nixonpeabody.com/en/ideas/blog/data-privacy/2021/03/03/privacy-by-design-opportunity-or-roadblock.

Conclusie

In het eerste en tweede deel van deze masterproef werd ingegaan op de privacy en gegevensbescherming in het algemeen. Eerst en vooral werd de ontstaansgeschiedenis besproken van de huidige privacywetgeving en werd kort ingegaan op het nationaal regelgevend kader in België. Het is duidelijk dat de Europese wetgever geopteerd heeft voor een sterk en coherent kader waar harmonisatie binnen de EU centraal staat. Om deze wetgeving af te kunnen dwingen, richten lidstaten onafhankelijke toezichthoudende overheden. Deze hebben verschillende bevoegdheden om inbreuken inzake gegevensbescherming te straffen, wat al ettelijke malen gebeurd is.

In het derde deel werd ingegaan op het concept van de privacy by design en default, waarbij elk lid van artikel 25 ontleed en geanalyseerd werd. Het advies van de European Data Protection Board bood hiervoor een grote hulp. De bepaling inzake gegevensbescherming door ontwerp en standaardinstellingen lijkt op het eerste zicht zeer duidelijk en concreet, maar dat is het eigenlijk niet. De richtlijnen van de EDPB maken duidelijk dat technische en organisatorische maatregelen vaak afhankelijk zijn van de concrete omstandigheden. Zo wordt er onder andere rekening gehouden met uitvoeringskosten en de stand van de techniek voor het nemen van maatregelen.

Verder werden drie dimensies onderschept van mogelijke uitdagingen van privacy by design en default. Het financieel draagvlak, de verwerker buiten de Unie en de noodzakelijkheid van businessmapping werden echter snel onderuitgehaald. We kunnen concluderen dat de verplichtingen onder data protection by design en default geen echte struikelblokken vormen.

Tot slot werd gekeken hoe toezichthoudende autoriteiten in Frankrijk en in het Verenigd Koninkrijk te werd gaan. Over het algemeen zijn deze niet bijzonder, aangezien de bevoegdheden overal hetzelfde zijn. Door de Brexit heeft het Verenigd Koninkrijk echter haar eigen Britse AVG, die zeer gelijkend is aan de Europese AVG. Aansluitend werd de privacywetgeving in de Amerikaanse Staat, California, besproken. We concluderen dat die privaywetgeving geen directe bepaling heeft inzake privacy by design en default, maar dat het met de nieuwe wetgeving een indirecte bepaling kan vormen. De AVG biedt over het algemeen meer bescherming en is dus consumentvriendelijker dan de CCPA.

Concluderend op de centrale hoofdvraag in welke mate de GDPR en de privacy by design en default voldoende bescherming biedt, moeten bovenstaande aspecten in rekening gebracht worden. De AVG is een zeer sterk en coherent kader en de bepaling van privacy by design en default is een instrument dat haar doel zal realiseren, namelijk het beschermen van persoonsgegevens en de rechten en vrijheden van het individu.

Bibliografie

Wetgeving

Europese wetgeving

Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele vrijheden van 4 november 1950, *BS* 19 augustus 1955.

Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, *BS* 30 december 1993.

Verdrag betreffende de werking van de Europese Unie (geconsolideerde versie), *Pb.L.* 7 juni 2016.
Handvest van de grondrechten van de Europese Unie van 7 december 2000, *Pb.L.* 18 december 2000.

Verord.Raad nr. 2016/679, 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, *Pb.L.* 4 mei 2016, afl. 119, 1.

Verord.EP en Raad nr. 45/2001, 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *PB.L.* 12 januari 2001, afl. 8, 1.

Verord.EP en Raad nr. 2018/1725, 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG

Richtl.EP en Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.

Richtl.EP en Raad nr. 2002/58/EG, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *Pb.L.* 31 juli 2002, afl. 201, 37.

Richtl.EP en Raad nr. 2016/680, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens betreffende het vrij verkeer van die gegevens, 25 januari 2012, COM(2012)11 def – 2012/0011 (COD).

Belgische wetgeving

De gecoördineerde Grondwet, *BS* 17 februari 1994.

Wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *BS* 3 februari 1999.

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.

Engelse wetgeving

UK Parliament, nr c.12, 23 mei 2018, Data Protection Act.

United Kingdom GDPR.

Franse wetgeving

Act nr. 78-17, 6 januari 1978 on information technology, data files and civil liberties.

Act nr. 2016-1321 du 7 oktober 2016 on Digital Republic Act.

Amerikaanse wetgeving

Govern. nr. SB-1121, 23 september 2018, California Consumer Privacy Act.

Rechtspraak

EHRM, 27 juni 2017, nr. 931/13 Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland.

Rechtsleer

Boeken

B. VAN ALSENOY, "Data Protection Law in the EU: Roles, responsabilities, and liability, 2019, Intersentia, 694 p.

CHAUMONT, D., DE BOT, D., DOCQUIR, B., GUERGUINOV, O., JOURET, J., LAHAYE, C., LEONARD, T., PLASSCHAERT, E., RAGHENO, N., SUFFUYS, C., TAMAS, R., VAN EECKE, VAN OLMEN C., VAN OVERSTRAETEN, T., VAN REMOORTEL F., VANDE VORST., C., VANDEPUTTE, O., VANDERMEERSCH, I., VERBRUGGEN, V., "Dataprotection & privacy", 2017, Anthemis, 230 p.

DE SMEDT, S. en CAPRONI, M., "*Praktische gids privacy in de onderneming"*, Mechelen, Wolters Kluwer, 2019, 346 p.

FOCQUET, A. en DECLERCK, E., "Gegevensbescherming in de praktijk", Antwerpen, Intersentia, 2019, 218 p.

Adviezen

EDPS

European Data Protection Supervisor, Opinion 5/2018 "Preliminary Opinion on privacy by design", 31 mei 2018, 1, https://edps.europa.eu/sites/default/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

European Data Protection Supervisor, "Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection", 19 december 2019, 1, https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

EDPB

European Data Protection Board, Guidelines 4/2019 on Article 25 "Data Protection by Design and by Default" version 2.0, 20 oktober 2020, 1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679 version 1.1", 4 mei 2020, 1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Board, "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation", 4 juni 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf.

European Data Protection Board, Informatie over bindende gegevensbeschermingsvoorschriften voor ondernemingen met de ICO als leidende toezichthoudende autoriteit Vastgesteld, 12 februari 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexit_nl.pdf.

Artikel 29 Werkgroep

Article 29 Data Protection Working Party, "The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 december 2009, nr. 168, 1, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.

Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", 30 mei 2014, nr. 218, 1, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", nr. 248 rev.01, 4 oktober 2017, 1, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171013_wp248_rev01_enpdf.pdf.

Article 29 Working Party "Opinion 05/2014 on Anonymisation Techniques", 10 april 2014, nr. 216, 1, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 6 oktober 2018, nr 251 rev.01, 1, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.

Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679", 11 april 2018, nr. 260 rev.01, 1, https://ec.europa.eu/newsroom/article29/items/622227.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 april 2013, nr. 203, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Andere adviezen

AEPD and EDPS, "Introduction to the hash function as a personal data pseudonimation technique", oktober 2019, 1, https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf.

AEPD, "A guide to privacy by design", oktober 2019, 27, https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

Onlinebronnen

Autoriteit Persoonsgegevens, "EDPB: voorstel ePrivacy Verordening moet beter", https://autoriteitpersoonsgegevens.nl/nl/nieuws/edpb-voorstel-eprivacy-verordening-moet-beter, (consultatie 29 maart 2021).

Autoriteit Persoonsgegevens, "verantwoordingsplicht" https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht (consultatie op 8 maart 2021).

AP, "Forse stijging privacyklachten in 2019", 14 januari 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019.

BELCIC, I., "Wat is gegevensversleuteling en hoe werkt het?", 10 juni 2020, https://www.avg.com/nl/signal/data-encryption.

BROOK, C., "What is Cyberhygiene? A definition of Cyber Hygiene, Benefits, Best practices and More", 6 oktober 2020, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.

BSI, U General Data Protection Regulation (GDPR) 20 steps to GDPR compliance – A methodical, systematic and logical approach A whitepaper, p 9, https://www.bsigroup.com/LocalFiles/en-GB/CSIR/Resources/Whitepaper/UK-ENGB-CSIR-WP-20-steps-to-GDPR-PDF.pdf.

CAVOUKIAN, A., "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D", 2010, https://link.springer.com/article/10.1007/s12394-010-0062-y.

CAVOUKIAN, A., "Privacy by Design : The 7 Foundational Principles Information and Privacy Commissioner of Ontario", 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

CAVOUKIAN, A., "Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", 2010, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

CNIL, "The CNIL's mission", https://www.cnil.fr/en/cnils-missions (consultatie 4 april 2021).

CNIL, "The CNIL in a nutshell - Protect personal data, Accompany innovations, Preserve civil liberties", 2019, 4, https://www.cnil.fr/sites/default/files/atoms/files/the-cnil-in-a-nutshell.pdf.

CNIL, "The CNIL in a nutshell - Protect personal data, Accompany innovations, Preserve civil liberties", 2015, 3, https://linc.cnil.fr/sites/default/files/typo/document/CNIL_EN_BREF-VEN-VD.pdf

DAVIS E. T., VAN MARTER A., "Privacy by design—opportunity or roadblock?", 3 maart 2021, https://www.nixonpeabody.com/en/ideas/blog/data-privacy/2021/03/03/privacy-by-design-opportunity-or-roadblock.

DAZY, A., "New French Digital Republic Law boosts support for OA and TDM", 2016, https://www.openaire.eu/blogs/new-french-digital-republic-law-boosts-support-for-oa-and-tdm-1;

DE WIT, E., "Dataminimalisatie en privacy by design: hoe minder data, hoe beter" 19 januari 2017, https://www.computable.nl/artikel/blogs/security/6310028/5260614/privacy-by-design-en-privacy-by-default.html.

Europese Unie, "Europese Toezichthouder voor gegevensbescherming (EDPS)", https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_nl (consultatie 1 april 2021).

Europese Unie, "Europees Comité voor gegevensbescherming (EDPB)", https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_nl (consultatie 1 april 2021).

EDPB, "European Data Protection Board: wie zijn wij", https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_nl (consultatie 2 april 2021).

HILLEN, C., "Privacy by design en privacy by default", 28 februari 2018, https://www.computable.nl/artikel/blogs/security/6310028/5260614/privacy-by-design-en-privacy-by-default.html.

ICO, "About the DPA 2018", https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (consultative op 5 april 2021).

ICO, "Some basic concepts", https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/#9 (consultative op 5 april 2021).

ICO, "Guide to the General Data Protection Regulation", 1 januari 2021.

ICO, "The Guide to Data Protection", 11 mei 2016.

Information and Privacy Commissioner of Ontario, "Privacy by Design: "seven foundational principles", januari 2018, https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf

IT Security Association Germany in co operation with ENISA, "IT Security Act and EU General Data Protection Regulation: Guideline 'State of the Art' technological and organisationial measures", 2021, 11, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf.

Justitia, "Privacy by design", https://www.justitia.nl/privacy/privacy-by-design (consultatie 25 maart 2021).

JEHL, L. FRIEL A., "CCPA and GDPR Comparison Chart", 2018, 3, https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf.

KING ALLEN, J., "Worldwide: California Privacy law vs GDPR", 5 maart 2021, https://www.mondaq.com/unitedstates/privacy-protection/1043204/california-privacy-law-vs-gdpr#:~:text=In%20the%20European%20Union%2C%20the,CCPA)%20provides%20protection%20for%20consumers.&text=The%20CPRA%20will%20go%20into,as%20of%20January%201%2C%202022.

MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY, G. SEN, "Comparing privacy laws: GDPR v. CCPA", 2019, 7-8, https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf.

MCCALL, J., "CPRA Pushes "Privacy by Design" Shift for Software Developers", 25 september 2020, https://www.devprojournal.com/technology-trends/data-privacy/cpra-pushes-privacy-by-design-shift-for-software-developers/.

KAMINSKY, M., "Facebook Faces Class Action Over Security Breach That Affected 50 Million Users", https://www.forbes.com/sites/michellefabio/2018/09/30/facebook-faces-class-action-over-security-breach-that-affected-50-million-users/?sh=6b9984777b6c.

Ministerie van binnenlandse zaken en Koninkrijksrelaties, "Privacy Enhancing Technologies - Witboek voor beslissers", december 2004, 13, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/technologie/witboek_pet.pdf.

SARAIVA, S., "Data Protection through Privacy by Design", 9, https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments.pdf.

WARD, M., "Fading data could improve privacy", 16 juni 2010, https://www.bbc.com/news/10324209.

Unizo, "GDPR: de nieuwe Europese privacyregels", https://www.unizo.be/system/files/downloads/andere/uzo-6118-snelwijzer-gdpr.pdf (concultatie 5 maart 2021).

X, "Gegevensbeschermingseffectbeoordeling: Aanbeveling van de Privacycommissie", 2018, https://www.gdprbelgium.be/nl/nieuws/gegevensbeschermingseffectbeoordeling-aanbeveling-van-de-privacycommissie.

X, "Privacycommissie wordt Gegevensbeschermingsautoriteit", 2018, https://www.eubelius.com/nl/nieuws/privacycommissie-wordt-gegevensbeschermingsautoriteit-0.

X, "Privacy by Design", 2018 http://www.ejure.nl/2018/01/privacy-by-design/.

X, "De Avg uitgelegd deel 3: privacy by design en privacy by default", 5 april 2017, https://www.nldigital.nl/news/avg-uitgelegd-deel-3-privacy-by-design-privacy-by-default/#:~:text=De%20letterlijke%20vertaling%20van%20privacy,aandacht%20moet%20zijn%20voor%20privacy.

X, "Uitleg over KPI's!", 2021, https://leansixsigmatools.nl/wat-zijn-key-performance-indactors.

X, "De AVG na twee jaar: knelpunten en oplossingen", 2 september 2020, https://www.pwnet.nl/instroom/nieuws/2020/09/de-avg-na-twee-jaar-knelpunten-en-oplossingen-10135587?io_source=www.pwnet.nl&_ga=2.186955816.1052085973.1620812362-1750095038.1620812362.

X, "Privacywaakhond legt familiezoeksite boete van ruim een half miljoen euro op", 12 mei 2021, https://datanews.knack.be/ict/nieuws/privacywaakhond-legt-familiezoeksite-boete-van-ruim-een-half-miljoen-euro-op/article-news-1733353.html.

X, "Datawarehousing", https://www.ictportal.nl/ict-lexicon/datawarehousing-dwh.

X, "French Data Protection Law Act: What's new", 4 december 2018, https://www.dreyfus.fr/en/2018/12/04/french-data-protection-act-whats-new/.

X, "The California Privacy Rights Act of 2020", 2020, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/.

X, "The California Privacy Rights Act of 2020", 2020, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/.

X, "CalOPPA vs CCPA: What You Must Know to Comply With Both", 26 januari 2021, https://www.websitepolicies.com/blog/caloppa-vs-ccpa.

X, "California Officials Announce California Privacy Protection Agency Board Appointments", 17 maart 2021, https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/.