



**Voorwoord**

Als vierdejaars HBO-Rechten-studente aan de Juridische Hogeschool Avans-Fontys te Tilburg heb ik de mogelijkheid een praktijkgericht juridisch onderzoek bij een bedrijf uit te voeren. Deze afstudeerscriptie is het eindproduct van het onderzoek dat ik bij Coca-Cola Enterprises Nederland B.V. (CCE-NL) heb mogen doen. Het onderwerp van mijn scriptie ‘’ huidige en toekomstige privacywetgeving’’ heb ik samen met mijn opdrachtgevers mr. Job Wijbenga en mr. Anka Greving gekozen. Van 8 september 2015 tot en met 11 december 2015 heb ik op kantoor data verzameld, gesprekken gehad, policy’s geanalyseerd en mijn onderzoek uitgevoerd.

Het doel van mijn onderzoek is het in kaart brengen van de huidige en toekomstige privacy wet- en regelgeving en het huidige privacy-beleid van CCE-NL toetsen aan dit wettelijk kader. Op deze manier wordt het duidelijk of er gaten vallen in dit beleid. Deze scriptie is dan ook bedoeld voor de medewerkers van CCE-NL die met privacygevoelige gegevens werken en dan voornamelijk persoonsgegevens.

Ik wil hier ook graag de ruimte creëren om de medewerkers van CCE-NL te bedanken voor hun tijd en kennis. Daarnaast wil ik Nadieh Denise Illustraties bedanken voor het ontwerpen van de omslag van deze scriptie. Een speciale dankbetuiging gaat uit naar mr. Job Wijbenga, die altijd tijd maakte om mijn vragen te beantwoorden en naar mijn stagebegeleider mr. Anka Greving, die altijd geduld heeft gehad, goede adviezen heeft gegeven en mij heeft betrokken bij leuke opdrachten.

Veel leesplezier.

Fabiènne Tielemans

Breda, 12 januari 2016.

**Samenvatting**

Deze scriptie heeft de titel ‘Dorstig naar data’ en verwijst hiermee niet alleen naar de corebusiness van CCE-NL, waarvoor deze scriptie is geschreven, maar ook naar de enorme hoeveelheid data die bedrijven vandaag de dag ‘opslurpen’. Dit is tevens de reden dat de Europese Commissie in 2012 een voorstel heeft ingediend om de privacywet- en regelgeving te moderniseren, zodat persoonsgegevens nog beter beveiligd kunnen worden in alle lidstaten.

In Nederland is het recht op privacy verdeeld over verschillende wetten, maar een van de belangrijkste wetten is de Wet bescherming persoonsgegevens (Wbp). Deze is gewijzigd doordat de Wet meldplicht datalekken en uitbreiding boetebevoegdheid College bescherming persoonsgegevens (Wmd) sinds 1 januari 2016 van kracht is en volledig is geïntegreerd in de Wbp. De vernieuwde Wbp speelt momenteel in op de veranderingen die op Europees niveau worden besproken.

De sancties die opgelegd kunnen worden voor het overtreden van de Wbp, bijvoorbeeld het niet melden van een datalek zijn aanzienlijk verhoogd. De maximale boete die opgelegd kan worden is € 820.000,00. Rechtspersonen worden nog zwaarder gestraft met een boete van 10 procent van de jaarlijkse omzet van het voorgaande boekjaar. Deze scriptie is dus niet alleen interessant voor de medewerkers van CCE-NL, maar voor eenieder in het bedrijfsleven die met persoonsgegevens werkt.

Het doel van deze scriptie is het in kaart brengen van de veranderingen die huidige en toekomstige privacywet- en -regelgeving met zich meebrengen. Om vervolgens de praktijk, zoals gegevensverwerkingen en het privacy-beleid te toetsen aan het wettelijk kader. Door wet- en regelgeving te combineren met concrete praktische aspecten worden er eventuele risico’s gesignaleerd en in deze scriptie worden aanbevelingen gedaan om deze risico’s te vermijden en te verhelpen.

De aanleiding voor het schrijven van deze scriptie is te vinden in het eerste hoofdstuk. Daarna volgen de beginselen waarop het Nederlands privacy recht is gestoeld in hoofdstuk twee. Hoofdstuk drie bespreekt de relevante bepalingen uit de Wbp. Het vierde hoofdstuk gaat over de Wmd en daarna volgt in het vijfde hoofdstuk de Europese privacywet- en -regelgeving en de verschillen met de Nederlandse Wmd. Het wettelijk kader wordt samengevat in de tussenconclusie. Daarna volgt het in kaart brengen van de gegevensstromen binnen CCE-NL in hoofdstuk zes. Het privacy-beleid van CCE-NL wordt in hoofdstuk zeven geanalyseerd en de conclusies en aanbevelingen volgen in hoofdstuk acht.

Inhoud

[Afkortingenlijst 6](#_Toc440040434)

[1. Aanleiding voor het onderzoek 7](#_Toc440040435)

[2. De beginselen van het Nederlandse privacy beleid 11](#_Toc440040436)

[3. De relevantie van de Wbp voor CCE-NL 13](#_Toc440040437)

[4. De Wet meldplicht datalekken 15](#_Toc440040438)

[5. Privacy wet- en regelgeving op Europees niveau 21](#_Toc440040439)

[Tussenconclusie 24](#_Toc440040440)

[6. CCE-NL en de verwerkingen van persoonsgegevens 25](#_Toc440040441)

[RIGHT CALL Hotline 25](#_Toc440040442)

[Data-uitwisseling 27](#_Toc440040443)

[Personeelsbestand 29](#_Toc440040444)

[7. Het privacy beleid van CCE-NL 32](#_Toc440040445)

[8. Conclusies en aanbevelingen 38](#_Toc440040446)

[Literatuurlijst 40](#_Toc440040447)

# Afkortingenlijst

|  |  |
| --- | --- |
| Afkorting | Betekenis |
| Ap | Autoriteit persoonsgegevens |
| AVG | Algemene Gegevens Verordening |
| Cbp | College bescherming persoonsgegevens |
| CCE-NL | Coca-Cola Enterprises Nederland B.V. |
| EC | Europese Commissie |
| EER | Europese Economische Ruimte |
| EG | Europese Gemeenschap |
| EU | Europese Unie |
| EVRM | Europees Verdrag voor de Rechten van de Mens |
| NARTD | Nonalcoholic ready to drink |
| OECD | Organanisation for Economic Co-operation and Development |
| OR | Ondernemingsraad |
| SCC | Sales support center |
| Stb | Staatsblad |
| Tw | Telecommunicatiewet |
| V.o.f. | Vennootschap onder firma |
| Wbp | Wet bescherming persoonsgegevens |
| Wmd | Wet meldplicht datalekken |

# 1. Aanleiding voor het onderzoek

**1.1 Probleembeschrijving**

De afgelopen jaren zijn er wekelijks nieuwsberichten over datalekken, grote hacks en andere veiligheidsincidenten. Recente voorbeelden zijn de datingssite Ashley Madison en de filmstudio’s van Sony. Digitale veiligheid wordt steeds belangrijker en daarom acht de regering het noodzakelijk om de Wet bescherming persoonsgegevens (nader te noemen: Wbp) en enige andere wetten te wijzigen. Per 1 januari 2016 zal de nieuwe Wet meldplicht datalekken en uitbreiding boetebevoegdheid Cbp (voortaan: Wmd) in werking treden en geïncorporeerd worden in de Wbp. Hierdoor ontstaat er een meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens. Tevens wordt de bevoegdheid van het College Bescherming Persoonsgegevens (voortaan: Cbp) uitgebreid om bij overtreding van die wet een hoge bestuurlijke boete op te leggen. Deze wet anticipeert alvast op de Europese Algemene Gegevensverordening. Tot slot verandert de naam van het Cbp naar Autoriteit Persoonsgegevens (voortaan: Ap).

Opdrachtgever Coca-Cola Enterprises Nederland B.V. (voortaan: CCE-NL) is een dochtermaatschappij van Coca-Cola Enterprises Inc. Laatstgenoemde wordt volgend jaar de grootste bottelaar ter wereld doordat Coca-Cola Erfrischungsgetränke is overgenomen en er een fusie met Coca-Cola Iberian Partners aankomt. Deze bedrijven combineren in een nieuw bedrijf genaamd: Coca-Cola European Partners[[1]](#footnote-1). Het streeft ernaar om de beste drankenverkoper te zijn met de beste klantenservice[[2]](#footnote-2). CCE-NL produceert, distribueert en verkoopt producten van merken van The Coca-Cola Company en een aantal andere dranken onder licentie. Hierdoor is er in Nederland een ruime keuze uit vele merken met een verschillend calorieniveau, suikergehalte en in verschillende verpakkingsgroottes. CCE-NL is een lokale onderneming met een krachtige regionale aanwezigheid en al meer dan 85 jaar actief in Nederland. De faciliteit in Dongen bottelt onder andere frisdrank, water, sportdrank en ijsthee. Het hoofdkantoor is gevestigd in Rotterdam en is verantwoordelijk voor de andere taken waaronder Sales, Marketing en de supportafdelingen zoals Legal.

De afdelingen Sales, Marketing en Procurement verwerken persoonsgegevens vrijwel dagelijks, door het opstellen van klantprofielen, het versturen van promotionele acties of het uitvoeren van de contracten. Deze verwerkingen gaan volgens het privacy beleid van CCE-NL.

De aankomende nieuwe Wmd en de Europese Verordening brengen heel wat veranderingen met zich mee (o.a. meldplicht en hogere boetes). CCE-NL wil weten welke gevolgen dit oplevert voor het huidige privacy beleid van CCE-NL. Er rijzen verschillende vragen, zoals:  
- Wat houdt de meldplicht precies in?;

- Wanneer is CCE-NL meldingsplichtig?;  
- Zijn er sancties als er niet of te laat wordt gemeld?;

- Moet het privacy beleid aangepast worden?

Concluderend is er behoefte aan een risico-inventarisatie van gegevensverwerkingen binnen CCE-NL en een analyse van het privacy beleid. Om de risico-inventarisatie te kunnen doen, moet de huidige en toekomstige privacywet- en regelgeving duidelijk in kaart worden gebracht, alsmede achtergrondstukken en opinies, zodat het wettelijk kader helder is.

De uitkomsten van de risico-inventarisatie komen in deze scriptie. Hier worden tevens aanbevelingen voor CCE-NL in gedaan.

**1.2 Centrale vraag**

Welke acties moet CCE-NL ondernemen om ervoor te zorgen dat haar privacy beleid voldoet aan huidige en toekomstige privacywet- en regelgeving?

**1.3 Doelstelling**

Binnen 14 weken wil ik in kaart hebben gebracht welke risico’s CCE-NL loopt als gevolg van de nieuwe wet- en regelgeving omtrent het beschermen van privacy en persoonsgegevens. Dit onderzoek zal voor CCE-NL een onderzoeksrapport met conclusies en aanbevelingen opleveren waarin duidelijk de voor CCE-NL relevante wettelijke bepalingen worden uitgelegd aan de hand van de huidige en toekomstige situatie.

**1.4 Deelvragen**

Wettelijk kader:

2.Wat zijn de beginselen van het Nederlands privacy beleid?

3.Welke bepalingen in de Wbp zijn voor CCE-NL relevant?

4.Wat houdt de Wmd in?  
5.Wat gaat toekomstige Europese regelgeving hier nog aan toevoegen?

Coca-Cola Enterprises Nederland BV:

6.Wat is de huidige situatie met betrekking tot verwerking van persoonsgegevens?

7.Hoe heeft CCE-NL haar privacy beleid ingericht?

8.Conclusies en aanbevelingen

**1.5 Onderzoeksstrategieën**

In dit onderzoek worden verschillende onderzoeksstrategieën gebruikt voor de verschillende aspecten van de centrale vraag. Hieronder wordt nader toegelicht welke strategie waarvoor wordt gebruikt. Een voor de hand liggende strategie ter voorbereiding van een nieuwe wet is het rechtsbronnen- en literatuuronderzoek. Schriftelijke bronnen worden geraadpleegd, vergeleken en geanalyseerd. Vervolgens worden deze bronnen geïnterpreteerd in de praktijk zodat er conclusies en aanbevelingen uit kunnen voortvloeien.

Voor het praktische gedeelte van de centrale vraag wordt er gebruik gemaakt van casestudy’s. In dit onderzoek wordt er een fenomeen als een geheel in en relatie tot zijn omgeving bestudeerd[[3]](#footnote-3). Om de case, in dit geval de aankomende nieuwe wet en Europese Verordening en hun impact goed te kunnen doorgronden, worden meerdere methoden gebruikt om informatie te verzamelen. Analyse van het privacy beleid, interviews met de Legal Counsels, Sales Agents, Marketingmedewerkers en Procurementmedewerkers van CCE-NL en onderzoekende observatie van de praktijk zullen gezamenlijk leiden tot een volledig beeld van de case.

**1.6 Bronnen en methoden**

Wat zijn de beginselen van het Nederlands privacy beleid?

Het bestuderen en inhoudelijk analyseren van rechtsbronnen, literatuur en documenten zal een antwoord op deze deelvraag opleveren.

Welke bepalingen in de Wbp zijn voor CCE-NL relevant?

Door middel van inhoudsanalyse van rechtsbronnen, literatuur en documenten zal deze deelvraag beantwoord worden.

Wat houdt de Wmd in?  
Deze deelvraag zal door middel van inhoudsanalyse van rechtsbronnen, literatuur en documenten beantwoord worden.

Wat gaat toekomstige Europese regelgeving hier nog aan toevoegen?

De inhoudsanalyse van literatuur en van verschillende documenten zal deze deelvraag helpen te beantwoorden.

Wat is de huidige situatie met betrekking tot verwerking van persoonsgegevens?  
Door middel van inhoudsanalyse van documenten wordt in kaart gebracht wat momenteel het beleid omtrent privacy is; tevens zullen interviews met Legal Counsels, Sales Agents, Marketingmedewerkers en Procurementmedewerkers worden afgenomen en tot slot zal onderzoekende observatie van fysieke objecten een triangulatie tot gevolg hebben, zodat de huidige situatie duidelijk is en kan worden beschreven.

Hoe heeft CCE-NL haar privacy beleid ingericht?

Het antwoord op deze deelvraag volgt uit inhoudsanalyse van rechtsbronnen en van documenten.

Is het privacy beleid van CCE-NL conform huidige en toekomstige wet- en regelgeving?

Deze deelvraag wordt beantwoord aan de hand van de conclusies van de andere deelvragen en bevat dus alle gebruikte bronnen en daarbij horende methodes.

Welke acties moet CCE-NL nemen om te voldoen aan de huidige en toekomstige wet- en regelgeving?

Door middel van analytisch denken in combinatie van de conclusie van de vorige vraag, zullen aanbevelingen tot stand komen die deze deelvraag beantwoorden.

**1.7 Verantwoording**

Gezien de juridische aard van dit onderzoek is inhoudsanalyse een gebruikelijk methode om verschillende bronnen te raadplegen. Interviews met verschillende medewerkers van de afdelingen Legal, Sales, Marketing en Procurement leiden tot een inzichtelijker beeld van de praktijk, zodat het praktisch aspect van de centrale vraag ook goed kan worden behandeld en dat verhoogt het relevantieniveau voor CCE-NL van dit onderzoeksrapport.

Onderzoekende observatie van onder andere huidige contracten, het privacy beleid en de actuele media is tevens nodig, zodat het juridische aspect met het praktische aspect verbonden kan worden.

**1.8 Planning**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data** | **Taak** | | Doorlopend: | |
| 8 september tot 17 september 2015 | Voorbereiden onderzoeksplan | | Uitwerken hoofdstukken onderzoeksplan | |
| 18 september 2015 | Onderzoeksplan laten checken, mailen | |
| 21 september 2015 | Deadline inleveren concept onderzoeksplan | |
| 5 oktober 2015 | Kennismakingsgesprek met docent | |
| 6 oktober 2015 | 1e Terugkomdag | |
| 7 oktober tot 23 oktober 2015 | Uitwerken hoofdstukken onderzoeksplan | |
| 26 oktober tot 30 oktober 2015 | Interne check representatief hoofdstuk | |
| 2 november 2015 | Deadline representatief hoofdstuk inleveren | |
| 10 november 2015 | 2e Terugkomdag | |
| 11 november tot 4 december 2015 | Laatste verbeteringen doorvoeren | |
| 7 december tot 10 december 2015 | Intern check conclusies en aanbevelingen | |
| 11 december 2015 | Beoordelingsformulier naar mentor | |
| 11 december 2015 | Deadline conclusies en aanbevelingen | |
| 14 december tot 26 december 2015 | Verbeteringen doorvoeren | |
| 30 december 2015 | Presentatie voor CCE-NL | |
| 8 januari 2016 | Taal check | |
| 11 januari 2016 | Scriptie inleveren via Urkund | |
| 12 januari 2016 | Scriptie inleveren fysiek |  | |

# 2. De beginselen van het Nederlandse privacy-beleid

Er is in Nederland geen algemene ‘’Wet op de Privacy’’, maar het recht op privacy is in verschillende vormen terug te vinden.

De ‘’Artikel 29 werkgroep’’ is een onafhankelijk advies- en overlegorgaan van Europese privacy-toezichthouders. De werkgroep speelt een belangrijke rol in de totstandkoming van een Europees uniform beleid voor de bescherming van persoonsgegevens. De naam van de werkgroep is ontleend aan artikel 29 van de Europese Privacyrichtlijn. Regelmatig worden werkdocumenten en opinies met uitleg over de toepassing van de Europese Privacyrichtlijn, nieuwe wetten en andere privacy onderwerpen gepubliceerd. Zo ook de interpretatie op de Richtlijn 95/46/EU.

Het Dataprotectie Verdrag van de Raad uit 1981 ligt aan de basis van privacybescherming op Europees niveau. Het is een concrete uitwerking van het recht op eerbiediging van het privéleven (artikel 8 EVRM).

De Europese Privacyrichtlijn 95/46/EG heeft het doel van privacybescherming voor alle lidstaten vastgelegd in 1995. Het doel is om de rechten en vrijheden van personen te beschermen bij de verwerking van persoonsgegevens en zorg te dragen voor vrij verkeer van persoonsgegevens tussen de Lidstaten. De implementatie van de richtlijn verschilt per lidstaat. De Nederlandse implementatie van deze richtlijn is vastgelegd in de Wet Bescherming Persoonsgegevens[[4]](#footnote-4).

De Nederlandse Grondwet. Dit is het belangrijkste staatsdocument en de hoogste nationale wet van Nederland. In het eerste hoofdstuk van de Grondwet zijn de rechten van iedere ingezetene vastgelegd. Het gaat daarbij met name om mensenrechten en democratische rechten[[5]](#footnote-5), zoals het recht op eerbiediging van persoonlijke levenssfeer, gecodificeerd in artikel 10. Dit wordt ook wel het recht op privacy genoemd. De persoonlijke levenssfeer bevat onder andere het recht op zorgvuldige behandeling van persoonsgegevens[[6]](#footnote-6).

Handvest van de grondrechten van de Europese Unie (hierna te noemen: Handvest) is een document waarin fundamentele rechten, vrijheden en beginselen in zijn opgenomen. Het Handvest heeft dezelfde juridische waarde als een EU-verdrag, ondanks dat het is opgenomen in een verklaring van het Europees Parlement, de Raad en de Europese Commissie[[7]](#footnote-7). De eerbiediging van het privéleven en de bescherming van persoonsgegevens zijn vastgelegd in respectievelijk artikel 7 en 8 van het Handvest.

The Organanisation for Economic Co-operation and Development (OECD) is een organisatie die streeft naar verbetering van economische en sociale welzijn van mensen over de hele wereld. Om dit te bereiken is er een forum gecreëerd waar verschillende overheden samen kunnen werken om dat te bereiken. Hieruit volgen vaak internationale standaarden, zoals het OECD Pivacy Framework[[8]](#footnote-8). De eerste internationale geaccepteerde set regels over privacy-principes. In 2013 is deze voor het laatst herzien om de snelle technologische ontwikkelingen bij te blijven.

Het Ontwerp Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (werknaam: Algemene Verordening Gegevensbescherming: AVG). De AVG wordt later verder uitgewerkt in hoofdstuk 5.

Het Europees Verdrag voor de Rechten van de Mens. In artikel 8 van het EVRM wordt de eerbiediging van het privéleven beschreven.

Richtlijn 2002/58/EC gewijzigd door 2009/136/EC. Deze Richtlijn, beter bekend als de e-Privacy Richtlijn reguleert de telecomsector en de persoonsgegevens die daar in omloop zijn. Hoe telefoonproviders de persoonsgegevens van hun abonnees moeten behandelen bijvoorbeeld, maar andersom geeft deze richtlijn ook rechten aan de abonnees[[9]](#footnote-9).

Telecommunicatiewet (voortaan: Tw) is van toepassing op het beschermen van de rechten van de burger betreffende elke vorm van digitale communicatie. Hoofdstuk 11 van de Tw geeft het recht op privacy weer.

Wet Bescherming Persoonsgegevens (Wbp), wordt in het volgende hoofdstuk besproken en verder uitgewerkt.

Wet Meldplicht Datalekken (Wmd), wordt later uitgewerkt in hoofdstuk 4.

Al deze wetten, regels en interpretaties vormen de basis voor het Nederlandse recht op privacy. De Wbp is de meest bekende wet met betrekking tot privacy-recht en zal in het komende hoofdstuk worden uitgewerkt. De Wmd wordt vanaf 1 januari 2016 compleet geïntegreerd in de Wbp en brengt een aantal veranderingen met zich mee die in hoofdstuk 4 worden besproken. Vervolgens wordt in hoofdstuk 5 de AVG besproken en de gevolgen die implementatie van die Verordening met zich mee brengt. Tot slot wordt het wettelijk kader samengevat om een duidelijk overzicht te schetsen.

# 3. De relevantie van de Wbp voor CCE-NL

In 1995 is de Europese Richtlijn 1995/46/EG[[10]](#footnote-10) vastgesteld op het gebied van privacy. Het doel van die Richtlijn is het waarborgen van een effectieve bescherming van persoonsgegevens, alsmede het garanderen van een functionerende interne markt[[11]](#footnote-11). De lidstaten hebben de richtlijn geïmplementeerd in een nationale wet. In Nederland is dat de Wet bescherming persoonsgegevens (Wbp). De Wbp is van toepassing op geautomatiseerde verwerking van persoonsgegevens.

Er zijn veel relevante bepalingen uit de Wbp van toepassing. Zo is het van belang om te weten wat er wordt bedoeld met de volgende begrippen:

**Persoonsgegeven.** De definitie daarvan is terug te vinden in artikel 1 sub a Wbp en luidt als volgt: *elk gegeven, betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.* Concreet gezegd zijn persoonsgegevens, alle gegevens die te herleiden zijn tot een bepaald persoon.

**Verwerking (van persoonsgegevens).** Dit omvat eigenlijk alles wat er vervolgens met die persoonsgegevens gebeurt. De definitie hiervan staat in het eerste artikel van de Wbp sub b en stelt: *elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.*

Er zijn twee typen verwerkers van persoonsgegevens volgens de Wbp, te weten:   
De Verantwoordelijke en de Bewerker. Degene die het doel van en de middelen voor de verwerking vaststelt, is de Verantwoordelijke. De Bewerker verwerkt persoonsgegevens ten behoeve van de Verantwoordelijke, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

CCE-NL komt met vele partijen in aanraking, zoals klanten, leveranciers en medewerkers. Hierbij worden gegevens verzameld om bijvoorbeeld contact te onderhouden of de overeenkomst uit te voeren[[12]](#footnote-12). Sommige klanten zijn eenmanszaken of een vennootschap onder firma (nader te noemen: V.O.F.). De verzamelde gegevens kunnen te herleiden zijn tot een bepaald persoon en dan is er sprake van persoonsgegevens. CCE-NL bepaalt onder andere welke gegevens er worden verzameld en met welk doel de gegevens worden verwerkt. Formeel-juridisch is CCE-NL dus de Verantwoordelijke, omdat deze het doel van en de middelen voor verwerking vaststelt. Dit is belangrijk, want de Wbp legt veel verplichtingen op aan de Verantwoordelijke.

Aan het verwerken van persoonsgegevens zijn eisen verbonden en die liggen besloten in ‘de zeven beginselen[[13]](#footnote-13)’ van de Wbp. Deze beginselen zijn nagenoeg allemaal vastgelegd in de Wbp. Dit zijn tevens de meest relevante bepalingen voor CCE-NL:

* Artikel 6 Wbp: het rechtmatigheidsbeginsel, dit verzekert een behoorlijke en zorgvuldige verwerking van persoonsgegevens conform de wet;
* Artikel 7 Wbp: het doelbindingsbeginsel, dit zorgt ervoor dat er een welbepaald en uitdrukkelijk doel moet zijn omschreven vóór de verwerking plaatsvindt;
* Artikel 8 Wbp: een limitatieve opsomming van grondslagen voor verwerking;
* Artikel 9 Wbp: het verenigbaarheidsbeginsel, kijkt of het nieuwe verwerkingsdoel in lijn is met het oorspronkelijke doel;
* Artikel 11, 12 en 13 Wbp: het beveiligingsbeginsel, verzekert dat de getroffen maatregelen adequaat en actueel zijn;
* Artikel 33 en 34 Wbp: het transparantiebeginsel, dit zorgt voor een actieve informatieplicht naar de betrokkene toe.
* Het beginsel der waarborg is gebaseerd op de in het maatschappelijke verkeer geldende normen.

Er moet voor gegevensverwerking altijd een doel worden bepaald. Het doel moet vervolgens in overeenstemming zijn met de grondslagen van gerechtvaardigde verwerking. Om te toetsen of de voorgenomen verwerking gerechtvaardigd is, kan Bijlage 1a worden geraadpleegd. Dan moeten er maatregelen worden getroffen waardoor de gegevensverwerking zorgvuldig gebeurt, zodat alleen de benodigde gegevens worden verwerkt. Die maatregelen moeten passen in de huidige digitale tijd, maar ook binnen de organisatie, zodat er een optimaal beveiligingsniveau wordt gerealiseerd. De bewaartermijn van artikel 10 Wbp speelt ook een grote rol bij een optimaal beveiligingsniveau. De persoonsgegevens worden niet langer bewaard in een vorm die makkelijk te herleiden is naar een bepaald persoon dan nodig voor de realisering van de eerder gestelde doelen. De betrokkene wordt actief ingelicht over bijvoorbeeld het recht van correctie of verzet.

Wanneer een organisatie persoonsgegevens gaat verwerken dan moet dit vrijwel altijd gemeld worden op grond van artikel 27 Wbp. Er staan een aantal uitzonderingen in het Vrijstellingsbesluit Wbp[[14]](#footnote-14). Om te bepalen of er gemeld moet worden, kan het stappenplan in Bijlage 1b worden geraadpleegd.

Een effectieve bescherming van het fundamentele recht op privacy en het stroomlijnen van de interne markt waren destijds de belangrijkste doelen van de Europese richtlijn en de daaruit voortvloeiende Wbp. Inmiddels is de wijze waarop een effectieve bescherming wordt gewaarborgd, veranderd en is de wet achterhaald. Er is een nieuwe Nederlandse wet die inspeelt op de snelle technologische veranderingen van deze digitale tijd.

# 4. De Wet meldplicht datalekken

**4.1 Wat betekenen de begrippen?**

In het voorgaande hoofdstuk werd al gesproken over een nieuwe wetgeving met betrekking tot privacy. Op 26 mei 2015 heeft de Eerste Kamer het wetsvoorstel voor de ‘Wet meldplicht datalekken en uitbreiding boetebevoegdheid College bescherming persoonsgegevens’ (Wmd). Deze wet is op 1 januari 2016 in werking getreden[[15]](#footnote-15) en is volledig in de al bestaande Wbp geïncorporeerd.

De titel van de Wmd geeft meteen de kern van nieuwe wet weer, namelijk de ‘meldplicht’ bij een ‘datalek’. Een **datalek** is ‘toegang tot persoonsgegevens, of vernietiging, wijziging, vrijkomen daarvan bij een organisatie, zonder dat dit de bedoeling is van deze organisatie’. Onder een datalek valt dus niet alleen het lekken van gegevens, maar ook het onrechtmatig verwerken daarvan[[16]](#footnote-16). De **meldplicht** brengt de verplichting met zich mee om een ontstane situatie of situatie die zal ontstaan bij het bevoegd gezag te melden[[17]](#footnote-17). Het bevoegd gezag is hier de Ap[[18]](#footnote-18).De ruime aanduiding van een ´datalek´ kan doen vermoeden dat de meldplicht voor alle datalekken geldt. De meldplicht zoals deze is beschreven in de Wmd is echter nadrukkelijk bedoeld voor situaties waarin sprake is van een doorbreking van technische en organisatorische maatregelen die voor de beveiliging van persoonsgegevens zijn getroffen[[19]](#footnote-19).

**4.2 Bepalingen in de Wbp (nieuw)**

De Wmd is een aanvulling op en een verandering van de Wbp, daarom zullen artikelen uit de Wmd worden aangeduid als artikel x Wbp (nieuw). In artikel 34a Wbp (nieuw) is de meldplicht opgenomen: *de verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens*[[20]](#footnote-20)*.*

In lijn van de terminologie van het voorgaande artikel, zullen in het navolgende de onderstreepte bestandsdelen worden besproken.

**4.3 In welke situaties bestaat er een meldplicht?**

Inbreuk op de beveiliging

Indien er een inbreuk op de beveiliging is geconstateerd (datalek) dan moet dit gemeld worden. Dit kan het geval zijn als de technische beveiligingsmaatregelen worden omzeild door hackers. Dat kan dan leiden tot een schending van de beveiliging persoonsgegevens. Ook wanneer er een laptop wordt gestolen uit een afgesloten locker en er wordt ingebroken in de laptop kan dat leiden tot een inbreuk op de beveiligingsmaatregelen. Er zijn echter ook andere situaties denkbaar. Wanneer gevoelige stukken als oud papier worden aangeboden of iemand raakt een USB-stick kwijt bijvoorbeeld, kan dit leiden tot organisatorische inbreuken op de beveiliging. Ongeautoriseerd, onomkeerbaar verlies van gegevens zal evenzeer gelden als een aanval op de beveiliging. In voornoemde gevallen is er een aanmerkelijk risico van ongeoorloofde toegang of onrechtmatige verwerking van persoonsgegevens en daarom moet er een melding worden gemaakt. Alleen wanneer het gaat om het falen van maatregelen die niet in het bijzonder gericht zijn op de beveiliging van persoonsgegevens valt de inbreuk niet onder de wet[[21]](#footnote-21).

Als er is vastgesteld dat er een schending van de beveiliging is geweest, dan wordt er vervolgens gekeken of er sprake is van een uitzondering op de meldplicht (artikel 34a lid 6 Wbp nieuw). De verplichting tot melding is namelijk niet van toepassing indien de Verantwoordelijke dusdanige technische beschermingsmaatregelen heeft genomen. Hiervan is bijvoorbeeld sprake als de persoonsgegevens versleuteld zijn. In dit geval wordt aangenomen dat de Verantwoordelijke er redelijkerwijs van uit mag gaan dat geen persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Om een beroep te doen op de uitzondering moet de Verantwoordelijke er van overtuigd zijn dat alle gegevens zijn versleuteld, dat de encryptie effectief en up-to-date is en tot slot moet er per geval worden afgewogen of het restrisico[[22]](#footnote-22) acceptabel is. Bij twijfel over de kwaliteit van de technische beschermingsmaatregelen, moet melding aan de Ap worden overwogen. De volgende stap in dit beslismodel is doorslaggevend in het besluitproces of er al dan niet gemeld moet worden.

**4.4 Aanzienlijke kans op ernstige nadelige gevolgen?**

Brengt de inbreuk een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens met zich mee? Om deze vraag te beantwoorden zal de Verantwoordelijke de aard van de persoonsgegevens evenals de aard en omvang van de inbreuk moeten beoordelen[[23]](#footnote-23). De regering gaat ervan uit dat de beoordeling voor de Verantwoordelijke relatief simpel is, aangezien het verwerken van persoonsgegevens onder diens verantwoordelijkheid valt[[24]](#footnote-24). CCE-NL moet zich als Verantwoordelijke de vraag stellen of er gevoelige persoonsgegevens zijn gelekt. Hierbij kan gedacht worden aan gegevens over de financiële of economische situaties van de betrokkene. Als er gevoelige gegevens zijn gelekt, moet er standaard een melding worden gedaan. Wanneer de gegevens niet gevoelig van aard zijn, worden de aard en omvang van de inbreuk beoordeeld.

Door het bestandsdeel ‘’ernstig’’ op te nemen in het artikel, tracht de regering de meldplicht af te bakenen. Zonder een goede afbakening zou de handhaving van de meldplicht door de Ap onbeheersbaar zijn en de effectiviteit zou teniet worden gedaan[[25]](#footnote-25). Op deze manier is de meldplicht alleen voorbehouden voor de ernstige gevallen. Een lek in de ledenadministratie van een sportvereniging zal niet zo snel aanleiding geven tot een melding[[26]](#footnote-26), tenzij het lek een gevolg is van een hack, waarmee de waarschijnlijkheid van misbruik[[27]](#footnote-27) toeneemt. De Verantwoordelijke moet rekening houden met de ernstige gevolgen en zowel materiële als immateriële schade vallen hieronder. Gelekte creditcardgegevens zijn een goed voorbeeld van materiële schade en gelekte medische gegevens worden geschaard onder immateriële schade.

Wanneer de uitzondering niet van toepassing is en de inbreuk op de beveiliging ernstig nadelige gevolgen heeft, moet er melding worden gedaan bij de Ap. De vraag is dan of de betrokkene ook ingelicht moet worden.

Conform lid 2 van artikel 34a Wbp (nieuw) wordt de betrokkene alleen ingelicht als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer.   
De terminologie is niet erg concreet, maar is ontleend aan artikel 11.3a Tw dat de omzetting vormt van artikel 4 e-privacy richtlijn[[28]](#footnote-28). Indien er persoonsgegevens van gevoelige aard zijn gelekt, kan ervan uit worden gegaan dat er ook altijd melding moet worden gedaan aan de betrokkene. In overige gevallen moet er altijd een afweging worden gemaakt op basis van de omstandigheden. De aard en omvang van het lek zijn mede bepalend voor het beoordelingsproces. Voorbeelden van immateriële, ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene zijn bijvoorbeeld stigmatisering of uitsluiting van de betrokkene of een onrechtmatige publicatie. Bij schade van materiële aard kan worden gedacht aan identiteitsfraude en de financiële schade die dit met zich mee kan brengen. De melding aan Betrokkene zorgt ervoor dat deze alert is op de mogelijke gevolgen en biedt de mogelijkheid dat de Betrokkene voorzorgsmaatregelen kan treffen.

**4.5 Wat is de inhoud van de melding?**

Als duidelijk is dat er gemeld moet worden, dan is de volgende vraag wat er in de melding moet staan. De wet is hierin redelijk abstract, maar de beleidsregels voor toepassing van artikel 34a Wbp (nieuw), opgesteld door de Ap, bieden hier meer duidelijkheid[[29]](#footnote-29). Deze beleidsregels hebben in de bijlage een vragenlijst opgenomen, betreffende de inhoud van de melding.

Conform 34a lid 3 Wbp (nieuw) moeten de Ap en de betrokkene een melding ontvangen met daarin in ieder geval:

1. De aard van de inbreuk;
2. Bij wie informatie over de inbreuk en het verloop van het onderzoek kan worden  
   verkregen;
3. De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. Bij vermelding van de aard van de inbreuk zal doorgaans met een algemene omschrijving kunnen worden volstaan[[30]](#footnote-30). Hierbij kan gedacht worden aan het verlies van een USB-stick tot aan een hack.
5. De Ap moet weten waar zij verdere informatie over het verloop van het onderzoek kan inwinnen en de Betrokkene wil graag weten waar hij persoonlijke hinder van ondervindt[[31]](#footnote-31).
6. De Verantwoordelijke moet de maatregelen bekend maken die de Betrokkene zelf kan ondernemen ter beperking van de schade.

De kennisgeving aan de Ap is complexer dan die aan de betrokkene en daarom heeft lid 4 van voornoemd artikel nog twee vereisten vastgesteld:

1. Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk;
2. De maatregelen die de Verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

AA) De geconstateerde gevolgen kunnen kort opgesomd worden. De vermoedelijke gevolgen zijn bij het eerste datalek moeilijk te voorspellen.

1. De getroffen maatregelen kunnen kort opgesomd worden. De voorgestelde maatregelen laten de Ap zien dat de Verantwoordelijke overzicht op de situatie heeft en die kan oplossen.

**4.6 Hoe moet er gemeld worden?**

De Ap stelt een digitaal formulier beschikbaar op de website www.autoriteitpersoonsgegevens.nl waarmee datalekken kunnen worden gemeld[[32]](#footnote-32). Er wordt een ontvangstbevestiging teruggestuurd en bij meldingen die aanleiding geven tot nadere actie door de Ap, zal er contact worden opgenomen met de Verantwoordelijke.

**4.7 Wat zijn de toetsingscriteria van de Ap?**

De beleidsregels Meldplicht Datalekken zijn door het Cbp op 9 december 2015 gepubliceerd. Deze beleidsregels zijn uitgangspunt bij het onderzoek en de beoordeling van de beveiliging van persoonsgegevens en bij het toepassen van handhavende maatregelen[[33]](#footnote-33). In de bijlage van deze beleidsregels is een vragenlijst opgenomen die de Verantwoordelijke kan doorlopen om te kijken of een situatie onder de meldingsplicht valt en wat er dan inhoudelijk in de melding moet staan.

**4.8 Binnen welke termijn moet er gemeld worden?**

Onverwijld in kennis stellen

Conform artikel 34a lid 1 Wbp moet het datalekken onverwijld gemeld worden aan de Ap. Binnen uiterlijk 72 uur na de ontdekking van het mogelijke datalek moet er door middel van het webformulier van de Ap gemeld worden. Dit houdt tevens in dat er enige tijd genomen mag worden om het mogelijke datalek te onderzoeken. Op het moment dat CCE-NL op de hoogte raakt van een beveiligingsincident begint de termijn om te melden te lopen. Mogelijk is er binnen de gestelde 72 uur nog geen volledig zicht op de precieze gebeurtenissen of welke persoonsgegevens er zijn gelekt. In dat geval meldt CCE-NL op basis van de gegevens die op dat moment bekend zijn[[34]](#footnote-34).

**4.9 Welke sancties kunnen worden opgelegd?**

Op het moment heeft het Cbp een zeer beperkte boetebevoegdheid. Er kan gebruik worden gemaakt van de last onder bestuursdwang of een kleine bestuurlijke boete van € 4.500,00.

Als het Cbp een bedrijf hard wil aanpakken, wordt er vaak gebruik gemaakt van ‘naming and shaming’. De negatieve publiciteit kan grote gevolgen hebben voor de positie van een bedrijf. Deze tactiek is echter slechts tijdelijk doeltreffend, want negatieve publiciteit waait weer over.

Door de invoering van de Wmd wordt de boetebevoegdheid van de Ap uitgebreid. Er is aangehaakt bij de hoogste boetecategorieën van het strafrecht. Volgens artikel 66 Wbp (nieuw) kan er een boete uit de vierde categorie van € 20.500,00 worden opgelegd bij een overtreding van onder andere het exportverbod[[35]](#footnote-35). De overtreding van de meeste algemene bepalingen uit de Wbp brengt echter een hogere boete met zich mee.

Als een Verantwoordelijke persoonsgegevens verwerkt zonder een gerechtvaardigd doeleinde[[36]](#footnote-36) of de verwerkte gegevens langer bewaart dan nodig is, kan er een boete worden opgelegd van maximaal € 820.000,00. Een hoge boete; daarom krijgt de overtreder eerst een bindende aanwijzing van de Ap**,** te vergelijken met een gele kaart bij het voetballen.

Als een onderneming deze aanwijzing negeert of als er is vastgesteld dat de overtreding opzettelijk is gepleegd, dan kan de Ap er voor kiezen om een boete op te leggen ter hoogte van 10% van de jaaromzet[[37]](#footnote-37) van de rechtspersoon[[38]](#footnote-38).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Oude situatie (voor 01-01-2016) | Opmerkingen | Nieuwe situatie  (na 01-01-2016) | Opmerkingen |
| Maximale boete bij het niet melden van verwerken. | Bestuurlijke boete van € 4.500,00 | Een lage boete, dus een kleine prikkel om privacybescherming als prioriteit te maken binnen een organisatie. | Bestuurlijke boete van € 20.250,00 | Een hoge boete is afschrikkend en een grote prikkel om privacybescherming als prioriteit te maken binnen de organisatie. |
| Maximale boete bij overtreding van artikel 4 lid 3 Wbp | Boete van € 8.100,00 | Derde categorie van het wetboek van Strafrecht | Boete van € 820.000,00 | Zesde categorie van het wetboek van Strafrecht |
| Maximale boete bij het opzettelijk overtreden van de algemene bepalingen Wbp | Boete van € 20.250,00 | Vierde categorie van het wetboek van Strafrecht of een gevangenisstraf van zes maanden | Bestuurlijke boete van 10% van de omzet van de rechtspersoon (van het vorige boekjaar) | Opzettelijke overtredingen kunnen worden beboet zonder voorafgaande bindende aanwijzing dus let op! |

**4.10 Wat is de vervolgstap na een melding?**

Er is een verplichting[[39]](#footnote-39) opgenomen in het nieuwe artikel 34a Wbp om de gegevens over een datalek te bewaren. Dit moet in een overzichtelijk document worden geplaatst waar de aard van de inbreuk, de gevolgen hiervan en corrigerende maatregelen zijn opgenomen[[40]](#footnote-40).

Als er ook een melding is gedaan aan de betrokkene(n) dan moet de tekst van de kennisgeving ook in het overzicht worden opgenomen[[41]](#footnote-41).

Dit document bevat natuurlijk persoonsgegevens die volgens de Wbp alleen met een bepaald doel verwerkt mogen worden. De Ap heeft de volgende doeleinden vastgesteld:

* Lering trekken uit het datalek en uit de wijze waarop dit is afgehandeld;
* Alsnog melden van een datalek aan de betrokkene(n);
* Antwoorden kunnen geven op vragen van betrokkene(n);
* Bewijsmateriaal verzamelen, indien er juridische stappen worden ondernomen naar aanleiding van het datalek.

De bewaartermijn van dit overzicht is door de Ap vastgesteld op minimaal een jaar. Als de gelekte persoonsgegevens dusdanig versleuteld zijn dat er geen melding naar de betrokkene hoeft te gaan[[42]](#footnote-42), dan moet het overzicht minimaal drie jaar bewaard worden. Er moet dan tijdens die jaren periodiek geëvalueerd worden of het datalek alsnog gemeld moet worden aan de betrokkene. Dit kan zich voordoen wanneer de stand van de techniek zover gevorderd is dat het niet zeker is of de versleutelde gegevens nog beschermd zijn door de encryptie.

Door alle nieuwsberichten omtrent privacy heeft de Europese Commissie in 2012 voorstellen gepresenteerd om de huidige privacyrichtlijn aan te passen. De Wmd is de Nederlandse anticipatie op de Europese wet- en regelgeving die nog gepubliceerd moet worden in het Publicatieblad van de Europese Unie.

# 5. Privacy wet- en regelgeving op Europees niveau

Op Europees niveau wordt wet- en regelgeving omtrent privacy ook herzien. De huidige Richtlijn[[43]](#footnote-43) is vastgesteld in 1995. De reden voor herziening ligt voor de hand[[44]](#footnote-44): het internet stond destijds nog in de kinderschoenen, maar inmiddels zijn online aankopen eerder regel dan uitzondering en wordt er constant informatie uitgewisseld met de rest van de wereld via social media platforms.

In januari 2012 heeft de Europese Commissie voorstellen gepresenteerd voor een herziening van de bestaande Privacyrichtlijn uit een Algemene Verordening Gegevensbescherming (nader te noemen: AVG) en een richtlijn ‘’gegevensbescherming opsporing en vervolging’’. Er is ditmaal bewust gekozen voor een Verordening, omdat dit zorgt voor harmonisatie tussen de lidstaten op het gebied van privacy. Dit bevordert de digitale marktdynamiek in Europa[[45]](#footnote-45). Vervolgens is de gewone wetgevingsprocedure gestart. De Europese Commissie dient een wetsvoorstel in bij het Europees Parlement (nader te noemen: Parlement) en de Raad van de Europese Unie (nader te noemen: de Raad). Het Parlement heeft met 4000 amendementen[[46]](#footnote-46) het voorstel flink gewijzigd. Op 12 maart 2014 heeft het Parlement met 621 stemmen voor het wetsvoorstel gestemd[[47]](#footnote-47). De Raad heeft ook gediscussieerd over het voorstel en op 15 juni 2015 is er overeenstemming bereikt[[48]](#footnote-48). Daarna hebben de drie organen samen over de wettekst vergaderd. Op 15 december 2015 is een sterke overeenstemming over de tekst van de Verordening uit de vergaderingen voortgekomen. Twee dagen daarna hebben de MEP’s van de ‘Civil Liberties Committee’ deze overeenstemming gesteund[[49]](#footnote-49). Er wordt verwacht dat de Verordening in het begin van 2016 wordt gepubliceerd in het Publicatieblad van de Europese Unie en vanaf dat moment hebben de lidstaten twee jaar de tijd om aan de Verordening te voldoen.

Naast het creëren van meer eenheid binnen de EU en moderniseren van de huidige privacywet- en regelgeving zorgt dit wetsvoorstel er ook voor dat persoonsgegevens nog beter beveiligd worden in alle lidstaten[[50]](#footnote-50). Er komt één set regels die ook zullen gaan gelden voorbedrijven die niet in Europa gevestigd zijn, maar hier wel diensten of goederen aanbieden[[51]](#footnote-51). Hierdoor wordt een bepaald beveiligingsniveau gerealiseerd dat een voorbeeld moet worden voor de rest van de wereld.

Een aantal bedingen wordt overkoepelend op Europees niveau geregeld en hierdoor niet in de Wmd behandeld. De belangrijkste bedingen worden hieronder uitgelicht met een korte toelichting. Vervolgens worden de belangrijkste verschillen tussen de AVG en de Wmd geaccentueerd en tot slot worden hier conclusies uit getrokken.

Het ‘one-stop-shop-systeem’ of ‘éénloketregister’ wordt in de AVG geïntroduceerd. Bedrijven met vestigingen in meerdere EU-lidstaten of die diensten en goederen aanbieden in verscheidene lidstaten hebben nu te maken met verschillende toezichthouders.

Met de introductie van dit nieuwe systeem wordt de toezichthoudende autoriteit van de voornaamste vestiging van de Verantwoordelijke, de leidende toezichthouder[[52]](#footnote-52). Hierop voortbordurend moeten bedrijven buiten de EU zich ook aan de AVG houden als zij goederen en/of diensten in de EU aanbieden of als zij het onlinegedrag van EU-inwoners volgen.

Een ander beding heeft betrekking op doorgifte van persoonsgegevens naar derde landen. Dit is al wel geregeld in de Wbp, namelijk in artikel 76. Doorgifte mag alleen plaatsvinden naar een land binnen de EER of wanneer het een passend beveiligingsniveau waarborgt. Als de Europese Commissie voor Persoonsgegevens heeft besloten dat het betrokken derde land een passend beschermingsniveau heeft, dan hoeft er geen specifieke toestemming te worden gegeven om persoonsgegevens uit te wisselen met dat land[[53]](#footnote-53). De Verenigde Staten hebben geen toereikend beschermingsniveau, maar in samenwerking met het Amerikaanse ministerie voor Handel is het Safe Harbor Framework opgericht. Amerikaanse organisaties die zich hier bij aansloten, worden geacht een passend beveiligingsniveau te hebben en daarom is datadoorgifte naar deze bedrijven toegestaan[[54]](#footnote-54). Het Europees Hof van Justitie heeft echter 6 oktober jongstleden dit Framework ongeldig verklaard[[55]](#footnote-55). Persoonsgegevens mogen dus niet meer op grond van het Safe Harbor-verdrag worden doorgegeven aan de Verenigde Staten.

Doorgifte van persoonsgegevens naar het land zonder passend beveiligingsniveau is desondanks mogelijk, wanneer de verantwoordelijke passende garanties biedt of wanneer de minister van Justitie een vergunning verleent op grond van artikel 77 lid 2 Wbp. Instrumenten die passende garanties kunnen bieden, zijn bijvoorbeeld Modelcontracten[[56]](#footnote-56) of Binding Corporate Rules, beide benoemd in artikel 42 AVG. Wanneer deze middelen worden ingezet om een passend beveiligingsniveau te bieden, hoeft er vooraf geen specifieke toestemming verleend te worden door het toezichthoudende orgaan.

Tot slot is het recht om vergeten te worden een belangrijk beding. Een Betrokkene mag een onderneming al verzoeken zijn gegevens te verwijderen, maar alleen wanneer deze feitelijk onjuist zijn, niet relevant zijn voor het verwerkingsdoel of in strijd met een wettelijk voorschrift. Het recht om vergeten te worden, speelt in op het veiligheidsgevoel waar de Betrokkene om vraagt. Een jaar geleden heeft het Europees Hof van Justitie hier een uitspraak over gedaan. Een Spanjaard verzocht Google om bepaalde zoekresultaten te verwijderen[[57]](#footnote-57) en dat is toegewezen. Een individu mag dus een bedrijf verzoeken dat zijn gegevens worden verwijderd. Wanneer het bedrijf geen gerechtvaardigde reden heeft om deze gegevens nog langer te verwerken dan moet er gehoor worden gegeven aan dit verzoek. Men kan hierdoor beter zijn risico’s inschatten wat betreft online gegevensverwerking. Wanneer mensen dit zelf in de hand hebben, wordt er een stijging in het vertrouwen in online dataverwerking bemerkt. De positie van het individu wordt door dit recht dus versterkt.

De Wmd verschilt in een aantal opzichten van het wetsvoorstel van de AVG. De belangrijkste verschillen worden hieronder besproken. Het verplicht aanstellen van een Privacy Officer volgens artikel 35 AVG is één van die verschillen. Volgens het eerste lid, sub b van voornoemd artikel moet een onderneming die meer dan 250 werknemers heeft een Privacy Officer in dienst nemen.

CCE-NL heeft ongeveer 800 medewerkers en valt dus onder deze bepaling. Dit artikel verschilt van de Wmd, maar bouwt wel voort op artikel 18, tweede lid van de Richtlijn 95/46/EG[[58]](#footnote-58) en is in die zin niet nieuw. De Privacy Officer moet een natuurlijk persoon zijn.

Artikel 35 lid 5 AVG stelt dat de Privacy Officer wordt aangewezen op grond van zijn professionele kwaliteiten, deskundigheid op het gebied van privacywet- en -regelgeving en zijn vermogen om de in artikel 37 AVG genoemde taken te vervullen.

Bedoelde taken zijn bijvoorbeeld adviseren en documenteren van de adviezen en de responsen daarop, het monitoren van het privacy beleid, verzorgen van bedrijfsopleidingen en verlenen medewerking aan de toezichthouder. Tot slot wordt een Privacy Officer op grond van het zevende lid van artikel 35 AVG voor 2 jaar benoemd en kan tijdens zijn ambtstermijn niet worden ontslagen, tenzij hij niet meer voldoet aan de voorwaarden voor het uitvoeren van zijn taken.

Het verplicht bijhouden van documentatie volgens artikel 22 AVG is ook een verschil ten opzichte van de Wmd. CCE-NL moet passende maatregelen treffen om te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de Verordening wordt uitgevoerd. De vereiste inhoud van deze documentatie wordt in artikel 28 AVG opgesomd. De contactgegevens van de Privacy Officer, eventuele internationale doorgiften en een algemene aanwijzing over de bewaartermijnen zijn voorbeelden van gegevens die opgenomen moeten worden.

In de AVG wordt er een extra eis gesteld aan de inhoud van een melding van een datalek. Er moet aan zowel de toezichthouder als de betrokkene worden gemeld welke betrokken categorieën in verband met persoonsgegevens zijn gelekt. Hierbij kan gedacht worden aan bijzondere persoonsgegevens zoals politieke voorkeur. Het aantal betrokkenen moet ook in de melding staan[[59]](#footnote-59).

Een opvallend verschil is de maximale sanctie die kan worden opgelegd. De lidstaten worden in artikel 78 van de AVG verplicht voorschriften vast te stellen inzake sancties[[60]](#footnote-60), wat de lidstaten dus ruimte geeft om hier zelf inrichting aan te geven. De maximale boetes zijn wel vastgesteld. In de AVG wordt er gesproken over een maximale boete van vier procent van de wereldwijde omzet, terwijl in de Wmd wordt gesproken van tien procent van de netto-omzet van het vorige boekjaar van de rechtspersoon. Het is onduidelijk of er in de Nederlandse wetgeving ook wordt gedoeld op de wereldwijde omzet. Het grote verschil van zes procent kan echter doen vermoeden dat de boete alleen geldt voor de Nederlandse rechtspersoon.

# Tussenconclusie

Het wettelijk kader kan als volgt worden samengevat:

Er is geen Nederlandse wet op de privacy, maar het recht op privacy is in verschillende vormen verwerkt in de Nederlandse wetgeving. Er zijn internationale beginselen waar rekening mee is gehouden, zoals de interpretatie van de Richtlijn 95/46/EU van de ‘artikel 29 werkgroep’ en het OECD Privacy framework. De Nederlandse wet die het meest gericht is op het recht op privacy is de Wbp.

De Wbp is de Nederlandse invulling van de Richtlijn 95/46/EU en ziet toe op het beschermen van persoonsgegevens bij digitaal verwerken. CCE-NL is formeel-juridisch de Verantwoordelijke verwerker volgens de Wbp en moet voordat er persoonsgegevens verwerkt gaan worden een welbepaald doel vaststellen en dit melden bij de toezichthouder. Dit is een van de eisen uit de Wbp om bescherming van persoonsgegevens te waarborgen. De Richtlijn is echter al 20 jaar oud en niet meegegaan in de snelle technologische veranderingen van deze tijd; hetzelfde geldt voor de Wbp.

Daarom geldt vanaf 1 januari 2016 de vernieuwde versie van de Wbp, waarin de Wet meldplicht datalekken en uitbreiding boetebevoegdheid Cbp is geïncorporeerd. Hiermee speelt Nederland al in op de Europese Algemene gegevensverordening die nog gepubliceerd moet worden in het Publicatieblad van de Europese Unie. De nieuwe Wbp (en specifiek de Wmd) verplicht bedrijven een datalek te melden wanneer dat ernstige en nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De melding moet binnen 72 uur bij de toezichthouder binnen zijn en voldoen aan een aantal eisen. De beleidsregels Meldplicht datalekken geven de toetsingscriteria van de toezichthouder weer. Alle inbreuken op de beveiliging moeten gedocumenteerd worden volgens de toezichthouder. Laatstgenoemde kan overigens hoge bestuurlijke boetes opleggen, wanneer er niet gemeld wordt of niet volledig. Dit kan namelijk leiden tot een bestuurlijke boete van € 820 000,00 of tien procent van de omzet van een rechtspersoon.

Ook op Europees niveau komen er nieuwe wet- en regelgeving omtrent het recht op privacy. Er komt een Algemene gegevensverordening. Er is ditmaal gekozen voor een Verordening en niet voor een Richtlijn, zodat er meer harmonisatie is binnen de lidstaten op het gebied van privacy. Andere doelen van de AVG zijn o.a. modernisering van de wetgeving en betere rechtsbescherming voor de burgers. Zo komt er een éénloketregister, wat het makkelijker maakt voor bedrijven om handel te drijven. Meldingen van verwerkingen van persoonsgegevens hoeven alleen naar de nationale toezichthouder te gaan en hierdoor zijn er minder administratieve lasten. De maximale sanctie is een opmerkelijk verschil tussen de Wmd en de AVG. De Wmd spreekt van tien procent van de omzet van de rechtspersoon, terwijl de AVG vier procent van de globale omzet eist.

Nu het wettelijk kader in kaart is gebracht, wordt de praktijk onderzocht. Tot slot zullen deze analyses over elkaar heen worden gelegd om te kijken waar eventuele gaten vallen en zullen er aanbevelingen worden aangedragen hoe deze gaten verholpen kunnen worden.

# 6. CCE-NL en de verwerkingen van persoonsgegevens

CCE-NL is een producent, distributeur, marketeer en verkoper van dranken. Om deze verschillende rollen goed te kunnen vervullen, zijn er gegevens nodig. Er worden onder andere marktprofielen opgesteld door de afdeling Sales, terwijl de afdeling Procurement de inkoop van diensten verzorgt. Hierbij kan gedacht worden aan het inkopen van IT-diensten. De afdeling HR houdt het personeelsbestand bij. Allerlei typen gegevens komen binnen bij CCE-NL, waaronder dus persoonsgegevens. In voorgaande hoofdstukken is beschreven welke verplichtingen worden opgelegd aan de Verantwoordelijke CCE-NL, wanneer het gaat om het verwerken van persoonsgegevens. Nu wordt er gekeken naar de precieze data die binnen CCE-NL worden verwerkt, naar de rechtmatigheid daarvan en of het gemeld moet worden, dan wel gemeld is.

In onder andere deze situaties verzamelt en verwerkt CCE-NL persoonsgegevens:

* Bijhouden personeelsbestand;
* Data-uitwisseling met:

1. (dranken) groothandels
2. bewerkers
3. klanten
4. commerciële data-analisten

* (Incidenteel) opnemen van telefoongesprekken bij het Sales Contact Center;
* Klantenbestanden;
* Leveranciersbestand;
* Promotionele acties voor de consument;
* Registraties op CCE-NL websites, zoals ‘Blik op Fris’;
* RIGHT call Hotline;
* Videocamera’s voor het waarborgen van de veiligheid;
* Vrijwillige health risk assessment voor medewerkers van CCE-NL;
* WebEx meetings (incidenteel) opnemen.

Vanzelfsprekend komen deze gegevens op verschillende wijzen binnen. Data-uitwisseling of de aankoop ervan komt vaak via Excel-sheets binnen. Consumentgegevens komen bijvoorbeeld via apps binnen of de CCE-NL website. Er wordt ook gebruik gemaakt van leaflets[[61]](#footnote-61) om informatie van bedrijven tijdens promotionele acties te vergaren.

**6.1 Rechtmatigheid verwerking binnen CCE-NL?**

Wanneer er een stap terug wordt gedaan, blijkt dat deze verwerking van persoonsgegevens onder de reikwijdte van de Wbp valt[[62]](#footnote-62) en eerder is al vastgesteld dat CCE-NL de Verantwoordelijke is[[63]](#footnote-63). Van een aantal bovengenoemde situaties wordt nu gekeken of de gegevensverwerking rechtmatig is, of ze gemeld moeten worden en of CCE-NL dat gedaan heeft.

### RIGHT CALL Hotline

Het is een telefoonlijn waar CCE-NL personeel naartoe kan bellen wanneer het denkt dat er een overtreding van de Code of Business Conduct is, zoals onregelmatigheden van boekhoudkundige aard. De beller geeft zijn naam, personeelsnummer en functie door.

Vervolgens wordt er naar de vermeende overtreder zijn naam en functie gevraagd en wordt er een onderzoek gestart naar de vermeende onregelmatigheden. Tot slot worden er van de vermeende overtreder strafrechtelijke gegevens verwerkt. Is de vermeende overtreder al eerder veroordeeld of was er eerder een redelijk vermoeden van schuld?

Is de gegevensverwerking rechtmatig?

Om dit te bepalen moeten de eerder besproken artikelen uit de Wbp worden getoetst. Dit is het gemakkelijkst aan de hand van het stappenplan opgenomen in bijlage 1a. Dit stappenplan zal hieronder worden uitgewerkt als voorbeeld;

1. Doeleinden: Ja, er is sprake van twee duidelijk bepaalde doeleinden, namelijk ‘’Een rapportage van vermeende onregelmatigheden van bijvoorbeeld financiële, boekhoudkundige aard of fraude’’ en ‘’Onderzoek doen naar follow-up activiteiten als gevolg van rapportages[[64]](#footnote-64)’’. Deze zijn uitdrukkelijk omschreven in de melding aan het Cbp[[65]](#footnote-65).
2. Grondslag: Ja, de verwerking wordt gebaseerd op artikel 8, sub f Wbp. Daarin staat dat de verantwoordelijk een gerechtvaardigd belang moet hebben om de gegevens te verwerken, mits het belang van de betrokkene prevaleert. Het doel is het rapporteren van vermeende onregelmatigheden en eventueel onderzoek doen naar follow-up activiteiten. Er is sprake van waarheidsvinding en dat is aan te merken als een gerechtvaardigd belang van de Verantwoordelijke[[66]](#footnote-66).
3. Proportionaliteit: Ja, CCE-NL heeft maatregelen genomen om geen bovenmatige, maar wel toereikende en juiste gegevens te ontvangen. De Hotline Procedures[[67]](#footnote-67) beschrijven precies welke gegevens gevraagd worden. Tevens ligt er een bewerkersovereenkomst[[68]](#footnote-68) tussen CCE-NL en CCE Inc. waarin het gewenste beveiligingsniveau is neergelegd.
4. Bijzonder: Ja, er worden bijzondere persoonsgegevens verwerkt, namelijk strafrechtelijke gegevens van de vermeende veroorzaker van de vermeende onregelmatigheden.
5. Uitzondering: Ja, deze bijzondere gegevensverwerking geschiedt op grond van een specifieke uitzondering van het verbod, namelijk artikel 22 lid 2 sub b Wbp. Het verwerken van strafrechtelijke gegevens mag, wanneer de Verantwoordelijke zichzelf beschermt. De Verantwoordelijke is namelijk gemachtigd om gegevens vast te leggen, wanneer door zijn personeel strafbare feiten dreigen te worden gepleegd[[69]](#footnote-69).
6. Marketing: Nee, deze gegevens worden niet verwerkt voor direct marketing doeleinden.
7. Aanvullende regels: Deze vraag is niet van toepassing.
8. Doorgifte: Ja, de gegevens worden doorgegeven aan een land buiten de EU, te weten de Verenigde Staten. Daar is Coca-Cola Enterprises Inc. gevestigd.
9. Verbod op doorgifte: Ja, de doorgifte naar de Verenigde Staten is verboden door de Europese Commissie, gezien de laatste ontwikkelingen omtrent Safe Harbor[[70]](#footnote-70).
10. Uitzondering verbod: Ja, er is een uitzondering van toepassing, namelijk een vergunning in de zin van artikel 77, lid 2 Wbp verleend door de minister van Justitie[[71]](#footnote-71).
11. Beschermingsniveau: deze vraag is niet van toepassing.
12. Restverplichtingen: Ja, er is verder aan alle andere verplichtingen voldaan.

CCE-NL heeft maatregelen getroffen om de persoonsgegevens te beveiligen door onder andere firewalls, autorisatieprocedures en geheimhoudingsovereenkomsten[[72]](#footnote-72). De gegevens worden niet langer dan 2 maanden bewaard, tenzij er een juridische procedure volgt; in dat geval worden de gegevens bewaard tot na het einde van deze procedure. Tevens hoeft de Betrokkene in dit geval niet geïnformeerd te worden, omdat het gaat om opsporen en voorkomen van vermeende onregelmatigheden zoals fraude, ofwel een strafbaar feit.

Moet de RIGHT CALL Hotline gemeld worden bij het Cbp?

Het betreft een geheel automatische verwerking van persoonsgegevens. De gegevens worden namelijk in een digitale rapportage verwerkt. Vervolgens wordt er een nader onderzoek ingesteld naar de vermeende overtreder. Deze verwerking is niet vrijgesteld in het Vrijstellingsbesluit van de Wbp en dat betekent dat de hotline gemeld moet worden bij het Cbp op grond van artikel 27 Wbp.

Is de RIGHT CALL Hotline gemeld?

CCE-NL heeft de hotline gemeld bij het Cbp en deze melding is opgenomen in het meldingenregister onder nummer 142351.

De RIGHT CALL Hotline is een rechtmatige gegevensverwerking binnen CCE-NL. Deze moet gemeld worden bij de toezichthouder en dat is gedaan, getuige melding 142351 in het openbare meldingenregister.

### Data-uitwisseling

Een ander voorbeeld waarin gegevens worden verwerkt is de data-uitwisseling met een groothandel. Vanuit de business zijn er vragen gekomen of er gegevens uitgewisseld mogen worden met bijvoorbeeld een groothandel. CCE-NL ontvangt dan gegevens van klanten van de groothandel. Hieruit kan bijvoorbeeld opgemaakt worden welke klanten van de groothandel wel in het NARTD-segment aankopen doen maar geen CCE-NL pakket afnemen en de groothandel ontvangt prospectlijsten van CCE-NL, waaruit soortgelijke conclusies volgen.

Welke gegevens worden gedeeld?

De klantnummers van de klanten van de groothandel, alsmede de NAW-gegevens. Vanuit CCE-NL worden prospectlijsten, met daarop NAW-gegevens gedeeld. Klanten en prospects zijn niet alleen bedrijven zoals een besloten vennootschap, maar het kunnen ook eenmanszaken en V.O.F. zijn.

Is de gegevensverwerking rechtmatig?

Om dit te bepalen moeten de eerder besproken artikelen uit de Wbp worden getoetst. Dit is het gemakkelijkst aan de hand van het stappenplan opgenomen in bijlage 1a. Dit stappenplan zal hieronder worden uitgewerkt als voorbeeld:

1. Doeleinden: Ja, er is sprake van zeven duidelijk bepaalde doelen voor het hebben van een klantenbestand, die door de melding 1113772 uitdrukkelijk zijn omschreven. Er zijn drie specifieke doelen die op data-uitwisseling van toepassing zijn, te weten:

* Doen van marktonderzoek en onderzoek naar positie van klanten;
* Verzamelen van informatie over klanten en het opstellen van profielen van klanten (v.b. naar regio, markt, specifieke producten);
* Onderhouden van contacten met klanten en voeren van correspondentie.

1. Grondslag: Ja, de verwerking wordt gebaseerd op artikel 8, sub f Wbp. Daarin staat dat de verantwoordelijk een gerechtvaardigd belang moet hebben om de gegevens te verwerken, mits het belang van de betrokkene prevaleert.

Hiervan is bijvoorbeeld sprake, wanneer een bedrijf zijn klantgegevens wil benutten voor het doen van een mailing om een nieuw product onder de aandacht te brengen[[73]](#footnote-73). Dit voorbeeld ligt in lijn met de doeleinden waarvoor CCE-NL gegevens wil uitwisselen met een groothandel.

1. Proportionaliteit: Ja, aan de data-uitwisseling ligt een contract ten grondslag[[74]](#footnote-74), waardoor beide partijen precies weten welke informatie moet worden uitgewisseld.
2. Bijzonder: Nee, er worden geen bijzondere persoonsgegevens verwerkt.
3. Uitzondering: deze vraag is niet van toepassing.
4. Marketing: Ja, de gegevensverwerking is gericht op directe marketingdoeleinden. Volgens de handleiding Wbp wordt het onderhouden van een directe relatie met de betrokkene voor commerciële doelen, directe marketing genoemd. ‘’Het gaat dan niet alleen om mailing aan de betrokkene maar ook om het maken van profielen om bijvoorbeeld de betrokkene direct te benaderen voor commerciële doeleinden’’[[75]](#footnote-75).
5. Aanvullende regels: Ja, de specifieke regels die hierop toe zien, zijn de algemene regels van rechtmatige gegevensverwerking. In dit geval moet er gekeken worden of data-uitwisseling verenigbaar is met het doel waarvoor de gegevens in eerste instantie zijn verkregen.

|  |  |  |
| --- | --- | --- |
| Oorspronkelijk doel | Direct marketing doel | Verenigbaar? |
| Staan onder (1) van deze opsomming genoemd. | Opstellen van profielen om nieuwe klanten te werven door hier correspondentie mee te voeren. | Ja, CCE-NL maakte al profielen van bestaande klanten en voerde hier ook correspondentie mee. |

De gegevens zijn gericht op directe marketingdoeleinden, maar dat is wel verenigbaar met het oorspronkelijke doel.

1. Doorgifte: Nee, de gegevens worden niet doorgestuurd naar een land buiten de EU.
2. Restverplichtingen: De gegevensverwerking wordt beveiligd, doordat het toezenden via een eigen netwerkomgeving gebeurt en is beveiligd met een logische toegangscontrole, zoals een wachtwoord[[76]](#footnote-76). De gegevens worden niet langer bewaard dan noodzakelijk. De betrokkene hoeft niet geïnformeerd te worden, maar de herkomst van de gegevens moet wel vastgelegd worden, zodat de betrokkene altijd kan opvragen welke weg zijn gegevens hebben afgelegd[[77]](#footnote-77).

Moet dit gemeld worden?

Er is een geheel automatische verwerking van persoonsgegevens. De gegevens worden in een Excel-bestand opgenomen en vervolgens digitaal toegestuurd. Deze gegevens worden dan vergeleken met CCE-NL klantgegevens via een softwareprogramma. Deze verwerking is niet vrijgesteld in het Vrijstellingsbesluit Wbp en dat betekent dat de data-uitwisseling gemeld moet worden bij het Cbp op grond van artikel 27 Wbp.

Is het gemeld?

Ja, CCE-NL heeft een melding van het klantenbestand (meldingsnummer: 1113772) gedaan. In deze melding staat dat CCE-NL de volgende klantgegevens verwerkt: NAW-gegevens, contactgegevens en omschrijving bedrijfsgegevens en dat de ontvangers hiervan onder andere groothandels zijn. Tevens sluiten de welbepaalde doelen aan op deze data-uitwisseling.

De data-uitwisseling met een groothandel is een rechtmatige gegevensverwerking binnen CCE-NL. Deze moet gemeld worden bij de toezichthouder en dat is gedaan, getuige melding 1113772 in het openbare meldingenregister.

### Personeelsbestand

In het personeelsbestand staan alle verzamelde gegevens over werknemers, uitzendkrachten, sollicitanten en stagiaires van CCE-NL. Op deze manier kan er correspondentie worden gevoerd, zoals het toesturen van begeleidende stukken voor opleiding. Daarnaast wordt er een salarisadministratie aan de hand van dit personeelsbestand bijgehouden.

Welke gegevens worden verzameld?

De volgende gegevens worden onder meer verzameld en verwerkt: NAW-gegevens, telefoonnummer, geboortedatum/-plaats, bs-nummer en gegevens met betrekking tot gevolgde opleidingen/cursussen en functies en gegevens met betrekking tot ziekteverzuim, pensioen en lidmaatschap bedrijfsvereniging.

Rechtmatige verwerking?

Om dit te toetsen moet er naar de eisen uit het Vrijstellingsbesluit worden gekeken. In dit geval wordt artikel 7 Vrijstellingsbesluit behandeld.

1. De doeleinden voor verwerking staan vermeld in lid 2. Hierbij kan gedacht worden aan het bijhouden van de opleiding van Betrokkene of juist het verlenen van ontslag;
2. De gegevens voor verwerking zijn gelimiteerd opgesomd in lid 3. De NAW-gegevens van de medewerker, als ook de aanwezigheid op plaats waar arbeid wordt verricht, zijn voorbeelden van gegevens die verwerkt mogen worden in het kader van het Vrijstellingsbesluit;
3. De ontvangers van verwerking staan opgesomd in lid 4. De ontvangers van gegevens zijn onder andere degenen die belast zijn met het leidinggeven of die noodzakelijkerwijs daarbij betrokken zijn.
4. De bewaartermijn is niet langer dan twee jaar nadat het dienstverband is beëindigd, tenzij de wet anders voorschrijft.
5. Tot slot de algemene regels van gegevensverwerking, zoals beveiliging.
6. De zeven doeleinden die CCE-NL welbepaald heeft vastgesteld en in het personeelsbestand uitdrukkelijk heeft omschreven, zijn o.a. personeelsadministratie en informatieverstrekking aan personeel.
7. CCE-NL verwerkt alleen de gegevens van personeel die volgens het derde lid, artikel 7 Vrijstellingsbesluit zijn toegestaan, zoals NAW-gegevens en nationaliteit.
8. De ontvangers van deze gegevens zijn o.a. de Arbodienst en het pensioenfonds, maar ook CCE-NL werknemers zelf, die belast zijn met het leidinggeven en de groepsmaatschappij in de Verenigde Staten.
9. De bewaartermijn van de personeelsgegevens is conform het Vrijstellingsbesluit.
10. De beveiligingsmaatregelen zijn o.a. fysieke maatregelen voor toegangsbeveiliging, inclusief organisatorische controle en een kluis voor opslag van gegevensbestanden en logische toegangscontrole, zoals een wachtwoord. Tot slot wordt er gebruik gemaakt van een encryptie wanneer de gegevens via een publiek netwerk worden verzonden naar bijvoorbeeld de Bewerker.

Moet dit gemeld worden?

Nee, de verwerking van deze gegevens ten behoeve van een personeelsbestand is vrijgesteld van melding op grond van artikel 5,7 en 8 Vrijstellingsbesluit. Artikel 5 heeft betrekking op de verwerking van de gegevens van sollicitanten. Artikel 7 gaat over de verwerking van personeel en artikel 8 ziet toe op de salarisadministratie. De vrijstelling geldt alleen wanneer de verwerking zich limiteert tot de gestelde eisen in voornoemde artikelen.

Het CCE-NL Personeelsbestand is een rechtmatige gegevensverwerking, omdat er wordt voldaan aan de gelimiteerde eisen uit het Vrijstellingsbesluit Wbp. Tevens is het melden van het personeelsbestand vrijgesteld van melding op grond van het eerder genoemde besluit.

**6.2 Wat is de impact van Safe Harbor op CCE-NL?**

In het voorgaande zijn er een aantal situaties waarin persoonsgegevens worden verwerkt, getoetst op rechtmatigheid. Hieruit blijkt dat de verwerkte gegevens in sommige gevallen ook naar CCE Inc. gaan. Dit kantoor is gevestigd in de Verenigde Staten. Dit is één van de landen die volgens de Europese Commissie geen passend beveiligingsniveau heeft[[78]](#footnote-78). Hierdoor is doorgifte van persoonsgegevens naar de VS verboden en kan het alleen bij hoge uitzondering[[79]](#footnote-79).

Data-doorgifte is een essentieel onderdeel van de trans-Atlantische relatie. De EU en de VS zijn elkaars belangrijkste handelspartners en datadoorgifte wordt een steeds groter onderdeel van de commerciële uitwisselingen[[80]](#footnote-80). Om datadoorgifte toch mogelijk te maken, terwijl er ook een hoog beveiligingsniveau wordt gegarandeerd, heeft de Europese Commissie het Safe Harbor framework aangenomen door het Safe Harbor besluit[[81]](#footnote-81). In dit besluit erkent de Commissie de Safe Harbor Principles en de veel gestelde vragen, uitgegeven door het Amerikaanse Ministerie van Handel. Het resultaat van dit besluit is dat persoonsgegevens doorgegeven mogen worden aan de bedrijven die zich bij het Safe Harbor framework hebben aangesloten. Door middel van zelfcertificering en eigen inzet sluiten deze bedrijven zich vrijwillig bij het Safe Harbor framework aan. Ondanks het vrijwillige karakter van aansluiten bij het framework zijn de regels bindend onder Amerikaans recht en kunnen worden afgedwongen door the U.S. Federal Trade Commission[[82]](#footnote-82).

Afgelopen 6 oktober 2015 heeft het Europese Hof van Justitie uitspraak gedaan[[83]](#footnote-83). Een van de conclusies was dat het Safe Harbor verdrag ongeldig is, mede omdat de Amerikaanse publieke overheidsorganen de persoonsgegevens konden inzien en tevens omdat een bedrijf zich kan aansluiten bij het Safe Harbor Framework door middel van zelfcertificering, dit is op zichzelf niet in strijd met de wet, maar het roept wel vraagtekens op bij de betrouwbaarheid van het naleven de Safe Harbor Principles. Nu het besluit ongeldig is verklaard, kan er geen beroep meer op worden gedaan, wanneer data worden doorgegeven aan de VS.

**Hoe kan data-doorgifte naar de VS toch?**

Er is een aantal alternatieve gronden waarop datadoorgifte naar de VS alsnog kan plaats vinden. De ‘’Artikel 29 werkgroep’’ adviseert om de standaard contractuele clausules (nader te noemen Modelcontracten) vastgesteld door de Europese Commissie en de interne gedragscodes, ofwel binding corporate rules, in de tussentijd te gebruiken[[84]](#footnote-84).

Wanneer er geen algemene privacywetgeving is of wanneer die wetgeving geen passend beveiligingsniveau waarborgt, moet het Modelcontract de gaten opvullen. De essentiële elementen van beveiliging die missen in een bepaalde situatie moeten worden opgenomen in het contract. De Europese Commissie heeft vier modelcontracten vastgesteld, conform het vierde lid van artikel 26 Europese Richtlijn.

In elke situatie waarin gegevens worden uitgewisseld met een land waar geen passend beveiligingsniveau wordt gegarandeerd, maakt CCE-NL gebruik van de Modelcontracten.

Wanneer het Modelcontract niet één op één wordt overgenomen, moet er een vergunning worden aangevraagd bij de Ap. Er kunnen twee situaties[[85]](#footnote-85) zijn wanneer het Modelcontract niet één op één wordt overgenomen, namelijk:

1. Aanvullingen op het Modelcontract
2. Wijzigingen op het Modelcontract of een eigen contract

De aanvullende bepalingen mogen niet in tegenspraak zijn met de standaardbepalingen en de aanvullingen mogen geen afbreuk doen aan de rechten van de Betrokkene(n). De Ap zal een positief advies afgeven wanneer dit het geval is. Een voorbeeld hiervan is de doorgifte van persoonsgegevens aan Capgemini India Private Limited gevestigd in Mumbay, India. CCE-NL heeft dit bedrijf ingeschakeld als Bewerker. De bewerkersovereenkomst is het Modelcontract plus aanvullingen. Beide partijen worden nader gespecifieerd en welke gegevens er precies worden doorgestuurd, worden extra toegelicht. CCE-NL heeft een vergunning verkregen van het Ministerie, zoals te lezen is in een brief van 20 oktober 2014[[86]](#footnote-86).

De tweede situatie, wijzigingen op het Modelcontract of een eigen contract gebruiken, is bij CCE-NL nog niet aan de orde geweest. Wanneer dit het geval is, moet de Ap een grondig onderzoek instellen omdat het om specifieke situaties betreffende doorgifte gaat. De duur van het onderzoek zal naar het bedrijf worden gecommuniceerd.

Tot slot heeft CCE-NL twee vergunningen aangevraagd om data van bijvoorbeeld personeel met CCE Inc. uit te wisselen. De vergunningsaanvragen hadden beide het Modelcontract als basis liggen, maar met aanvullende bedingen die nadere toelichting van bijvoorbeeld verzuimgegevens gaven. Deze vergunningen zijn beide afgegeven[[87]](#footnote-87).

In het volgende hoofdstuk wordt het privacy beleid van CCE-NL getoetst aan het eerder geschetste wettelijk kader[[88]](#footnote-88). Op deze manier wordt er in kaart gebracht of CCE-NL voldoet aan de verplichtingen die door de Wbp zijn gesteld en wordt er gekeken of CCE-NL klaar is voor de toekomstige eisen van de AVG.

# 7. Het privacy beleid van CCE-NL

Om te voldoen aan het eerder geschetste wettelijk kader heeft CCE-NL een Privacy Policy[[89]](#footnote-89) en een richtlijn Gegevens Privacy[[90]](#footnote-90) opgesteld. Recentelijk is hier de Web Governance Policy aan toegevoegd. Elke nieuwe website of app die voor normale bedrijfsvoering gebruikt gaat worden, moet door het speciale Web Governance team beoordeeld worden. De Legal Counsel uit het team zal onder andere privacyaspecten beoordelen. De toets op privacy van gegevens zal gaan volgens de zojuist genoemde policy en richtlijn en daarom wordt de Web Governance Policy niet verder behandeld. De Privacy Policy is gericht op klanten, betrokkenen en andere partijen waarvan gegevens worden verwerkt binnen CCE-NL. De richtlijn Gegevens Privacy is tezamen met de Code of Business Conduct het bedrijfsbeleid voor medewerkers. Het privacy beleid (de Privacy Policy en richtlijn Gegevens Privacy + Code of Business Conduct) moet CCE-NL in staat stellen om formele vragen van de Ap of van de pers te kunnen beantwoorden. In dit hoofdstuk worden algemene aspecten van een privacy beleid aangestipt[[91]](#footnote-91) en vervolgens wordt er gekeken wat er in de Privacy Policy en het bedrijfsbeleid staat en of dat voldoende is.

De onderstaande vragen richten zich op omliggende algemene aspecten van het privacy beleid. Op deze manier wordt er gekeken of er bewustzijn heerst in CCE-NL en of het privacy beleid al duidelijk geïmplementeerd is in de werkwijze van medewerkers.

* **Is het privacy beleid vastgesteld door de board?**

Het Europese privacy beleid is wel vastgesteld door de board. De Nederlandse versie niet, maar deze is uiteraard gebaseerd op de Europese versie.

* **Is er een Functionaris voor de Gegevensverwerking?**  
  Nee, momenteel is er nog geen Functionaris voor de Gegevensverwerking ofwel Privacy Officer. Dit wordt wel verplicht bij AVG[[92]](#footnote-92).
* **Is de Code of Business Conduct door de ondernemingsraad vastgesteld?**

Dit document bestaat in ieder geval al 10 jaar en is destijds door de OR vastgesteld.

* **Wordt het privacy beleid periodiek geëvalueerd?**  
  Ja, het privacy beleid wordt periodiek geëvalueerd, alleen niet structureel. Momenteel, met de aankomende veranderingen die nieuwe wetgeving met zich meebrengt, wordt het privacy beleid geëvalueerd.
* **Is het privacy beleid vertaald naar werkinstructies?**  
  Nee, het privacy beleid bevat de wettelijke vereisten, maar er zijn geen concrete uitvoeringsacties aan verbonden.
* **Is er een opleidings- of awareness-programma?**  
  Ja, er is een awareness-programma gericht op acceptabel IT-gebruik. Hierin zijn een aantal paragrafen gericht op bewustzijn rond beveiliging[[93]](#footnote-93). Er is tevens een  
   ‘’IT-richtlijnen en bescherming persoonsgegevens-module’’ in de CCE Academy opgenomen, maar deze is vrijwillig en daardoor niet kantoorbreed bekend.
* **Is er een compliance-programma ingericht?**  
  Er is geen speciaal compliance-programma voor persoonsgegevensverwerkingen. De afdeling Ethics and Compliance, samen met de afdeling Legal houdt echter wel bij dat de policy’s conform huidige wet- en regelgeving blijven.
* **Is het aantoonbaar gedocumenteerd dat CCE-NL een privacy beleid heeft en dat CCE-NL zich daaraan houdt?**Nee, CCE-NL heeft geen zogeheten logboek waarin alle verwerkingen worden bijgehouden.

Zo is gebleken dat het opnemen van WebEx-meetings nog niet gemeld is. De voorbereiding van die melding is toegevoegd als bijlage 8.

Nu de omliggende algemene aspecten zijn behandeld, wordt het privacy beleid gesplitst geanalyseerd. Als eerder gezegd, richt de Privacy Policy zich op de betrokkenen en de richtlijn GP op de medewerkers.

Privacy Policy

De Privacy Policy begint met een inleiding, waarin staat: ‘’Elke verwerking van uw gegevens voldoet aan de toepasselijke wet- en regelgeving’’.

De verwerkingsvereisten staan o.a. opgenoemd in hoofdstuk 3 van deze scriptie[[94]](#footnote-94) en in het vorige hoofdstuk[[95]](#footnote-95) is gebleken dat de getoetste gegevensverwerking inderdaad rechtmatig is.

De reikwijdte van de Policy wordt zo vastgesteld, dat de betrokkene weet welke verwerkingen onder de Policy vallen en tevens worden de Gebruikersvoorwaarden van CCE-NL van toepassing verklaard voor verwerkingen via de website. De Gebruikersvoorwaarden stellen dat de persoonlijke gegevens die via de website worden ontvangen conform de Privacy Policy worden verwerkt. Een betrokkene weet vaak niet bij wie hij terecht kan met vragen over de gegevensverwerking. Daarom moet de Verantwoordelijke ook in de Privacy Policy staan. Deze wordt in paragraaf 2.1 van de Privacy Policy genoemd.

Wanneer een betrokkene contact opneemt met CCE-NL of zich registreert als bezoeker van een CCE-NL website, worden er mogelijk persoonsgegevens verwerkt, zoals NAW-gegevens en een e-mailadres. De gebruikersnaam en het wachtwoord van geregistreerde bezoekers worden ook verwerkt, zo is terug te lezen in hoofdstuk 3 van de Privacy Policy. De doelen waarvoor deze gegevens worden verwerkt, staan opgesomd in hoofdstuk 4. De verwerkingsdoelen zijn vrijwel allemaal gebaseerd op de wettelijke grondslag ‘‘het gerechtvaardigd belang[[96]](#footnote-96)’’. Dit wordt geacht aanwezig te zijn in het geval dat de betreffende verwerking noodzakelijk is om de reguliere bedrijfsactiviteiten te verrichten[[97]](#footnote-97), zoals dienstverlening aan klanten en marketingdoeleinden. Het voldoen aan een wettelijke verplichting, neergelegd in paragraaf 4.4. van de Privacy Policy vindt zijn grondslag in artikel 8 sub c Wbp.

De proportionaliteit en subsidiariteit van de hoeveelheid persoonsgegevens zijn niet vastgelegd in de Privacy Policy. Er worden hier en daar, bijvoorbeeld in paragraaf 4.8 Privacy Policy wel een aantal persoonsgegevens benoemd, die mogelijkerwijs verzameld worden, maar er zijn geen regels vastgesteld welke persoonsgegevens redelijkerwijs nodig zijn om de doelen te realiseren.

Hoofdstuk 6 van de Privacy Policy stelt de bewaartermijn conform de wet vast. De bewaartermijn is gelinkt aan het doeleinde waarvoor de gegevens zijn verzameld en het verschilt daarom per gegevenscategorie hoe lang de gegevens bewaard blijven. Archivering is ook een doeleinde en vaak verenigbaar met het originele doel, dus de gegevens kunnen eventueel na afloop van de originele bewaartermijn, gearchiveerd worden.

Er zijn geen procedures over het hergebruik van gegevens opgenomen in de Privacy Policy. In sommige gevallen worden persoonlijke gegevens nogmaals verwerkt, maar voor een ander doel. ‘Blik op Fris’ is daar een voorbeeld van. Betrokkenen kunnen een prijs winnen wanneer ze deelnemen aan een enquête. De NAW-gegevens worden dan verwerkt om de betrokkene te contacteren over de gewonnen prijs.

Dezelfde NAW-gegevens worden nogmaals verwerkt om te kijken of de betrokkene in het afgelopen jaar ook al een prijs heeft gewonnen. Dit is een ander doel.

De betrokkene wordt in hoofdstuk 8, 9 en 10 van de Privacy Policy geïnformeerd over zijn rechten. Het recht van inzage wordt kort aangestipt en ook de redelijke vergoeding die CCE-NL hiervoor mag vragen op grond van artikel 39 Wbp staat hierin beschreven. Het kan voorkomen dat de gegevens van de Betrokkene niet correct zijn, een aanvulling behoeven of op een andere manier gecorrigeerd moeten worden; dan moet de vergoeding aan de Betrokkene worden teruggeven. Dit laatste is niet opgenomen in de Privacy Policy. De wijze waarop gecorrigeerd moet worden door de betrokkene staat in hoofdstuk 9 beschreven en het recht van verzet en wanneer dat recht gebruikt kan worden, staat in hoofdstuk 10 van de Privacy Policy gemeld.

Tot slot heeft de Privacy Policy een verzoek opgenomen om datalekken te melden aan CCE-NL. Een tekortkoming van de beveiliging wordt verzocht gemeld te worden, echter wordt de inrichting van de beveiliging van persoonsgegevens niet beschreven.

De richtlijn Gegevens Privacy

De richtlijn Gegevens privacy (hierna te noemen: richtlijn GP) begint met een inleiding waarin staat dat CCE-NL en haar medewerkers zich moeten houden aan de verschillende verplichtingen die volgen uit deze richtlijn, omdat deze gebaseerd is op de relevante wetgeving betreffende privacy. Tevens staat er dat deze richtlijn gelezen moet worden in combinatie met de Safe-Harbor overeenkomst[[98]](#footnote-98), de Code of Business Conduct en lokale CCE-procedures. De richtlijn is van toepassing op alle vaste en tijdelijke medewerkers van CCE-NL, inclusief uitzendkrachten en zelfstandigen.

De Code of Business Coduct (hierna te noemen: Code) is het bedrijfsbeleid binnen CCE Inc. Bij elke actie die een medewerker onderneemt, wordt verwacht dat hij op de juiste manier handelt, via de RIGHT way. Dit geldt dus ook voor het verwerken van persoonsgegevens. Persoonsgegevens die medewerkers van CCE-NL zijn toevertrouwd, moeten beschermd worden conform plaatselijke wetgeving en lokale bedrijfsrichtlijnen.

De richtlijn GP heeft een aantal verwerkingseisen opgenomen om er zeker van te zijn dat CCE voldoet aan de relevante wetgeving. Deze zijn o.a. eerlijk en wettig verwerken, niet langer bewaren dan noodzakelijk en uiteraard goed beveiligen. Dit zijn dezelfde verwerkingseisen die eerder in hoofdstuk 3 zijn behandeld, er is echter geen specifieke werkinstructie aan verbonden. Er is geen vastgestelde bewaartermijn per verwerkingsdoel en de proportionaliteit en subsidiariteit zijn niet ondervangen door specifieke invullingen.

De meeste verwerkingssituaties van persoonsgegevens van medewerkers worden benoemd en hiermee wordt ook het verwerkingsdoel duidelijk. Deze verwerkingsdoelen richten zich voornamelijk op de gerechtvaardigde grondslag van artikel 8 sub b Wbp ‘het uitvoeren van een contract’.

De richtlijn GP heeft geen procedures opgenomen over hergebruik van gegevens. Er staat bij de verwerkingseisen dat de gegevens alleen voor het opgegeven en wettige doel mogen worden verwerkt. Wanneer er echter een nieuwe verwerkingsactiviteit wordt ontplooid, zoals een nieuwe marketingdatabase, moet er navraag worden gedaan bij de juridische afdeling.

Betrokkenen worden geïnformeerd over recht van correctie, verzet en toegang in deze richtlijn GP.

De procedure voor toegang tot eigen persoonlijke gegevens wordt in gang gezet door middel van een aanvraagformulier ‘’persoonlijke gegevens’’.

Tevens wordt er benadrukt dat elke wijziging van persoonlijke gegevens doorgegeven moet worden, zodat CCE-NL de actuele en correcte gegevens bijhoudt.

Dit is niet alleen belangrijk voor correcte administratie van bijvoorbeeld secundaire arbeidsvoorwaarden, maar ook in geval van nood om een contactpersoon te bereiken.

Tot slot wordt voor de invulling van beveiliging van persoonsgegevens verwezen naar het informatiebeveiligingsbeleid en de Code. Laatstgenoemde bevat een hoofdstuk over gepast gebruik van technologieën. Hard- en software van CCE-NL moeten beschermd worden tegen schade, diefstal, fraude en onbevoegde toegang[[99]](#footnote-99). De specifieke veiligheidsmaatregelen, zoals versleuteling, firewalls en wachtwoorden[[100]](#footnote-100) moeten in acht worden genomen. Het informatiebeveiligingsbeleid is echter niet terug te vinden op de intranetomgeving van CCE-NL.

Na een gesprek met IT-specialist Perry Wetsteijn[[101]](#footnote-101) blijkt dat er een uitgebreide policy is over het Acceptabel IT-gebruik. Deze is echter lastig te vinden op de intranetomgeving van CCE-NL. Deze Policy heeft als doel dat iedereen binnen CCE-NL op de hoogte is van het programma rond gegevensbeveiliging, zodat er een uniforme werkwijze ontstaat. Alleen als het personeel goed ingelicht en opgeleid is en zich bewust is van de regels, kan erop worden gerekend dat zij zich verantwoordelijk gedragen. Eventuele wijzigingen in de policy worden dan ook op verschillende manieren verspreid en elk jaar wordt de hele policy opnieuw bekeken en aangepast in overeenstemming met het bedrijfsbeleid en lokale wet- en regelgeving.

**7.1 Waar actie op moet worden ondernomen**

Uit voorgaande analyse van het privacy beleid is gebleken dat CCE-NL voldoet aan de randvoorwaarden van de huidige Wbp. Er zijn echter wel een aantal verbeterpunten waar actie op moeten worden ondernomen. Als deze acties worden doorgevoerd is CCE-NL volledig conform de huidige Wbp en goed voorbereid op de aankomende Wmd en AVG. De volgende opsomming is gebleken uit analyses van voorgaande hoofdstukken.

Algemene aspecten:

* De board betrekken bij het privacy beleid;
* Een Privacy Officer benoemen;
* Concrete werkinstructies verbinden aan het privacy beleid;
* Documentatie bijhouden voor eventuele verantwoording over de verwerkingen;
* Datalekbeleid opstellen.

Privacy policy:

* Koppel doeleinden voor verwerking aan de gegevens die nodig zijn dat doel te bereiken;
* Bewaartermijn per doeleinde vaststellen of dit opnemen in de Retention Policy;
* Procedures hergebruik persoonsgegevens opnemen;
* Betrokkene wijzen op mogelijke archivering;
* Concreet contactpersoon aanwijzen voor betrokkene.

Richtlijn GP:

* Verwerkingsdoelen compleet opsommen;
* Koppel doeleinden voor verwerking aan de gegevens die nodig zijn dat doel te bereiken;
* Bewaartermijn per doeleinde vaststellen of dit opnemen in de Retention Policy;
* Procedures bij hergebruik, stappenplan doorlopen en dan laten checken door legal.

**7.2 Het belang van de actiepunten**

Er is gebleken dat de Nederlandse board niet is betrokken bij het vaststellen van het privacy beleid. Dit is zeker een punt waar CCE-NL actie moet ondernemen. Het betrekken van de board bij het privacy beleid verzekert een bepaalde mate van bewustzijn vanuit de top. Vanzelfsprekend komt er dan ook meer bewustzijn op de werkvloer.

De board moet in ieder geval geïnformeerd worden over de hoge boetes die vanaf 1 januari 2016 gelden. Wanneer de Ap een onderzoek instelt, kan dat gepaard gaan met negatieve pers en reputatieschade. Wordt de board niet geïnformeerd dan kan CCE-NL hier ook aan blootgesteld worden.

Er moet een Privacy Officer komen om te voldoen aan de AVG[[102]](#footnote-102). CCE-NL kan ervoor kiezen om een eigen medewerker hiervoor te laten omscholen. Ook bestaat de mogelijkheid om een externe organisatie te benaderen. Daarnaast is het mogelijk dat de groep (CCE) een Privacy Officer in dienst neemt. Wanneer deze functie is vervuld, moeten de contactgegevens van de Privacy Officer vermeld worden in de Policy’s en de toezichthouder en Betrokkene moeten hiervan op de hoogte worden gesteld.

Er zijn geen werkinstructies die volgen uit het privacy beleid en ook dit is een actiepunt voor CCE-NL. Werkinstructies zijn een opsomming van uitvoeringsacties. Hierdoor kan elke medewerker zelfstandig de rechtmatigheid van de gegevensverwerking in de gaten houden. Dit zal leiden tot een uniforme werkwijze waardoor er minder risico’s zijn tijdens het verwerken van persoonsgegevens.

Een ander actiepunt is het bijhouden van documentatie, zodat CCE-NL zich kan verantwoorden over bijvoorbeeld datalekken. Het wettelijk kader is geschetst in hoofdstuk 5 van deze scriptie. De AVG expliciteert de eisen die in het kader van verantwoording aan de documentatie van een onderneming worden gesteld. Wanneer er geen verantwoording kan worden overlegd of de documentatie niet volledig is, zijn hier hoge sancties aan verbonden. Sancties zijn al eerder aan bod gekomen in deze scriptie, echter de specifieke administratieve boete die voor het niet of niet volledig bijhouden van documentatie geldt, is op grond van artikel 79, lid 5 sub f AVG €500.000,00 of 1% van de jaarlijkse wereldwijde omzet van de groep.

Het opstellen van een datalekbeleid garandeert dat het duidelijk is hoe er gehandeld moet worden op het moment dat er een beveiligingsincident is. Wanneer er niet goed gehandeld wordt (denk aan te laat melden of niet volledig melden), kunnen hiervoor hoge boetes worden opgelegd. Het is handig om een samengestelde werkgroep te hebben van bijvoorbeeld een IT-specialist, jurist en een medewerker van PAC (public affairs and communication). Het incident moet onderzocht worden en het moet duidelijk worden wat er precies is gebeurd met de gegevens, welke gegevens zijn getroffen en om hoeveel betrokkenen het gaat.

Wanneer de benodigde persoonsgegevens aan het doeleinde worden gekoppeld, kan er geen onduidelijkheid ontstaan over welke gegevens noodzakelijkerwijs worden verwerkt om het doeleinde te realiseren. Dit zorgt voor een uniforme werkwijze. Het behoorlijk en zorgvuldig verwerken, alsmede relevante, toereikende en niet bovenmatige gegevensverwerking vormt het wettelijk kader[[103]](#footnote-103) voor dit actiepunt.

Wanneer dit niet wordt nageleefd is er sprake van een wederrechtelijke gegevensverwerking. Dit kan leiden tot een onderzoek van de toezichthouder en uiteindelijk tot hoge boetes.

Het koppelen van een concrete bewaartermijn aan een verwerkingsdoeleinde biedt een concrete actie aan ‘’het niet langer bewaren dan noodzakelijk’’, zoals in het wettelijk kader eerder is vermeld. De Retention Policy heeft alle bewaartermijnen opgesomd voor documenten, tevens waar en hoe de documenten opgeslagen moeten worden. Het is belangrijk dat CCE-NL de bewaartermijnen van specifieke gegevensverwerking hierin ook opneemt, zodat uit documentatie kan blijken dat CCE-NL en haar medewerkers conform de wet handelen en niet in overtreding zijn. Als eerder gezegd is archivering ook een bewaardoel[[104]](#footnote-104) en moet de betrokkene hier op worden gewezen. Dit bewerkstelligt het transparante en open karakter dat gegevensverwerking vraagt.

Wanneer een Policy stelt dat de meeste verwerkingsdoelen staan opgesomd, lijkt het erop dat niet alle verwerkingsdoelen zijn benoemd. Een gegevensverwerking mag niet plaatsvinden zonder een welbepaald en uitdrukkelijk omschreven doel, dus het is van groot belang dat de verwerkingsdoelen compleet zijn.

Tot slot is het van belang dat er procedures/werkinstructies worden geïntegreerd om gegevens eventueel verder te verwerken. Dit zal leiden tot meer bewustzijn dat gegevens niet zomaar opnieuw gebruikt mogen worden. Nu wordt er naar de afdeling Legal verwezen, maar dit proces kan korter en gemakkelijker gemaakt worden door een stappenplan te volgen, voordat er naar de afdeling Legal wordt gegaan.

# 8. Conclusies en aanbevelingen

Nieuwe wet- en regelgeving brengt altijd veranderingen met zich mee. De aankomende veranderingen zijn gelegen in het recht op privacy en hoe bedrijven daarmee om moeten gaan. CCE-NL heeft hierin de kans gezien om haar privacy beleid te evalueren en te toetsen aan huidige, maar ook toekomstige wet- en regelgeving. De volgende vraag stond centraal in dit onderzoek: ‘’Welke acties moet CCE-NL ondernemen om ervoor te zorgen dat haar privacy beleid voldoet aan huidige en toekomstige privacywet- en regelgeving?’’

Deze vraag is ontleed in de volgende aspecten:  
Het Nederlands privacy ‘’recht’’ en haar beginselen (Hoofdstuk 2)  
De Wbp en de bijbehorende verwerkingsvereisten. (Hoofdstuk 3)  
De Wmd en de veranderingen. (Hoofdstuk 4)  
De eventuele toevoegingen en/of veranderingen van de Europese AVG. (Hoofdstuk 5)  
De gegevensstromen binnen CCE-NL. (Hoofdstuk 6)

Het toetsen op rechtmatigheid daarvan.  
Het privacy beleid van CCE-NL. (Hoofdstuk 7)

Het toetsen op overeenstemming met de wet.

Het privacy beleid van CCE-NL is gestoeld op de Nederlandse wetgeving. Het is daarom van belang te weten waar het Nederlandse recht op privacy vandaan komt en hoe dat in elkaar steekt. De beginselen die ten grondslag liggen aan het Nederlandse recht op privacy, zoals internationale richtlijnen, interpretaties en verdragen, zijn in deze studie meegenomen in de visie op het Nederlandse ‘’privacy-recht’’.

Het verwerken van persoonsgegevens moet zo gebeuren, dat de Betrokkene hier geen hinder van ondervindt. De Wbp heeft daarom allerlei vereisten voor het verwerken van persoonsgegevens opgesteld. Het melden van gegevensverwerking is (in de meeste gevallen) één van die vereisten. Er is echter een situatie (te weten: WebEx meetings opnemen) opgemerkt, waarin de gegevensverwerking niet is gemeld. Dit is dan ook niet conform de Wbp.

Een ander vereiste voor het verwerken is het bepalen van een doel voor de verwerking en deze uitdrukkelijk omschrijven. Het privacy beleid heeft een aantal van de verwerkingsdoelen opgenomen, maar niet allemaal. Wanneer een gegevensverwerking geen uitdrukkelijk omschreven verwerkingsdoel heeft, is dit ook niet conform de Wbp.

De uitkomst van de toets op de huidige wet- en regelgeving is dat het privacy beleid van CCE-NL hier momenteel niet op alle fronten aan voldoet.

Bij het voorbereiden van CCE-NL en haar privacy beleid moet er eerst gekeken worden naar de aanstaande veranderingen. De Wmd introduceert een tweede meldplicht betreffende persoonsgegevens, maar dit keer in verband met een datalek. Wanneer er een inbreuk op de beveiliging is geweest en dit een incident met zich meebrengt, moet de onderneming hier melding van doen bij de toezichthouder. Volgens de beleidsregels van het toenmalige Cbp moet het incident binnen 72 uur worden gemeld. Na afhandeling van het datalek moeten de gegevens hieromtrent gedocumenteerd worden. Tevens is CCE-NL ook verantwoordelijk voor het afhandelen van de melding wanneer er een datalek is bij een Bewerker. De wet verplicht de Bewerker niet om dit aan de Verantwoordelijke te melden, dus dit moet contractueel goed geregeld worden. De Wmd regelt tevens de uitgebreidere bevoegdheid van de toezichthouder om boetes op te leggen. Deze boetes zijn afschrikwekkend hoog en kunnen bij opzettelijke overtreding van de Wmd leiden tot een boete van € 820.000,00 of 10% van de jaaromzet van de rechtspersoon. CCE-NL heeft momenteel geen datalekbeleid. Het privacy beleid van CCE-NL is nog niet goed voorbereid op de veranderingen van de Wmd.

De Wmd anticipeert al op de Europese AVG, welke naar verwachting in het begin van 2016 gepubliceerd wordt in het Publicatieblad van de Europese Unie. De Wbp (en daarmee ook de Wmd) wordt vervangen door de AVG wanneer deze van kracht gaat. Er zijn echter wel een aantal verschillen ten opzichte van de Wmd, zoals het verplicht bijhouden van documentatie over alle verwerkingen. CCE-NL houdt op dit moment geen documentatie bij van alle gegevensverwerkingen.

Het doorgeven van persoonlijke data naar een land buiten de EER is in de Wbp al niet toegestaan. Wanneer het derde land een passend beveiligingsniveau heeft, wordt er een uitzondering gemaakt. De Verenigde Staten is een derde land zonder passend beveiligingsniveau, echter bestond er een Safe Harbor Framework waar Amerikaanse bedrijven zich verplichtten om wel passende beveiliging te garanderen, naar Europese maatstaven. Het Europese Hof van Justitie heeft dit besluit recentelijk ongeldig verklaard. Het doorgeven van persoonlijke data naar de Verenigde Staten zal dus op andere manieren moeten plaatsvinden, bijvoorbeeld door middel van Modelcontracten of binding corporate rules. Gezien de meeste data doorgegeven worden naar het hoofdkantoor in Atlanta, verdient het aanbeveling dat CCE Inc. binding corporate rules implementeert om tijd te besparen ten opzichte van Modelcontracten.

Het privacy beleid van CCE-NL is nog niet goed voorbereid op de veranderingen van de AVG. Er is bijvoorbeeld nog geen Privacy Officer aangesteld door de groep of CCE-NL. De functie voor Privacy Officer wordt bij een onderneming met meer dan 250 medewerkers verplicht.

Op de vraag of het privacy beleid van CCE-NL voldoet aan huidige en toekomstige privacywet- en regelgeving moet het antwoord luiden: nee. Om ervoor te zorgen dat het privacy beleid voldoet aan huidige en toekomstige wet- en regelgeving wordt aanbevolen dat CCE-NL de volgende acties onderneemt:

* Alle gegevensverwerkingen die nog niet gemeld zijn, melden bij de toezichthouder;
* Alle verwerkingsdoelen bepalen en uitdrukkelijk omschrijven in het privacy beleid;
* Een datalekbeleid opstellen;
* Documentatie bijhouden over datalekken;
* Documentatie bijhouden over alle gegevensverwerkingen binnen CCE-NL;
* Een Privacy Officer aanstellen.

Wanneer deze acties worden doorgevoerd dan worden de risico’s op hoge boetes verholpen en voldoet het privacy beleid van CCE-NL aan huidige en toekomstige privacywet- en regelgeving.

# Literatuurlijst

**Coca-Cola Nederland**[www.coca-colanederland.nl](http://www.coca-colanederland.nl)

**Berkvens & Hennekens 2015**J. Berkvens & M. Hennekens, *Checklists privacy compliance. Stappenplan in checklistvorm, naar een Privacy Compliance Systeem*,Den Bosch: Banning 2015.

**Goudsmit 2015**M. Goudsmit, ‘Wet meldplicht datalekken en uitbreiding boetebevoegdheid CBP’, *Bedrijfsjuridische berichten* 2015-53.

**Hooghiemstra & Nouwt 2014**

T.F.M. Hooghiemstra & S. Nouwt, *Sdu Commentaar Wet bescherming persoonsgegevens*, Den Haag: Sdu uitgevers 2014.

**OESO-Richtlijnen 2011**

*De OESO-Richtlijnen voor Multinationale Ondernemingen*, *Nederlandse vertaling*, Den Haag: Ministerie van Buitenlandse Zaken 2011.

**Sauerwein & Linnemann 2002**

L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002.

**Van der Pot/Elzinga & De Lange 2006**

D.J. Elzinga & R. de Lange, *Van der Pot. Handboek van het Nederlandse staatsrecht*, Deventer: Kluwer 2006.

**Van Schaaijk 2011**

G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom Juridische uitgevers 2011.

1. [Home.cceportal.com](http://Home.cceportal.com) zoek op: merger information [↑](#footnote-ref-1)
2. [www.coca-colanederland.nl](http://www.coca-colanederland.nl), zoek op: ons bedrijf [↑](#footnote-ref-2)
3. van Schaaijk 2011 [↑](#footnote-ref-3)
4. 1995/46/EG Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG 1995, C93/1).* [↑](#footnote-ref-4)
5. [www.denederlandsegrondwet.nl](http://www.denederlandsegrondwet.nl) (zoek op inleiding) [↑](#footnote-ref-5)
6. Van der Pot/Elzinga & De Lange 2006 387 t/m 428. [↑](#footnote-ref-6)
7. [www.minbuza.nl](http://www.minbuza.nl) (zoek op EU-essentieel). [↑](#footnote-ref-7)
8. [www.oecd.org](http://www.oecd.org) (zoek op internet economy, privacy guidelines) [↑](#footnote-ref-8)
9. Ec.europa.eu (zoek op: digital society, e-privacy directive) [↑](#footnote-ref-9)
10. *PbEG* 1995, C 93/1. [↑](#footnote-ref-10)
11. *Factsheet Why do we need an EU protection reform*, ec.europa.eu, zoek op data protection. [↑](#footnote-ref-11)
12. *Melding 1113772*, *Ap.* [www.autoriteitpersoonsgegevens.nl](http://www.cbpweb.nl) zoek op: meldingenregister. [↑](#footnote-ref-12)
13. Zie toelichting bij de regeling van 9 juli 2001, *Stcrt. 2001*, 132. [↑](#footnote-ref-13)
14. *Stb*. 2001, 250. [↑](#footnote-ref-14)
15. *Stb.* 2015, 281. [↑](#footnote-ref-15)
16. ‘Cbp publiceert Beleidsregels meldplicht datalekken’, [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-16)
17. *Lycaeus juridisch woordenboek*, [www.juridischwoordenboek.nl](http://www.juridischwoordenboek.nl), zoek op meldplicht. [↑](#footnote-ref-17)
18. Art. 51 Wbp. [↑](#footnote-ref-18)
19. *Kamerstukken I* 2014/15, 33 662, nr. C, p. 2. [↑](#footnote-ref-19)
20. Art. 34a Wbp (nieuw). [↑](#footnote-ref-20)
21. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 5-6. (MvT) [↑](#footnote-ref-21)
22. Cbp publiceert Beleidsregels meldplicht datalekken’, [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-22)
23. *Kamerstukken II* 2014/15, 33 662, nr. 6, p. 19. [↑](#footnote-ref-23)
24. *Kamerstukken II* 2014/15, 33 662, nr. 11, p. 9. [↑](#footnote-ref-24)
25. *Kamerstukken I* 2014/15, 33 662, nr. C, p. 2. [↑](#footnote-ref-25)
26. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 7. [↑](#footnote-ref-26)
27. *Kamerstukken II* 2014/15, 33 662, nr. 6, p. 19. [↑](#footnote-ref-27)
28. *Kamerstukken II* 2014/15, 33 662, nr. 6, p. 17. [↑](#footnote-ref-28)
29. ‘Cbp publiceert Beleidsregels meldplicht datalekken’, [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-29)
30. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 21. [↑](#footnote-ref-30)
31. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 22. [↑](#footnote-ref-31)
32. ‘Cbp publiceert Beleidsregels meldplicht datalekken’, www.autoriteitpersoonsgegevens.nl zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-32)
33. *Ap*, www.autoriteitpersoonsgegevens.nl, zoek op: beleidsregels, overzicht richtsnoeren [↑](#footnote-ref-33)
34. ‘Cbp publiceert Beleidsregels meldplicht datalekken’, www.autoriteitpersoonsgegevens.nl zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-34)
35. Artikel 78 lid 2 sub a Wbp [↑](#footnote-ref-35)
36. Artikel 7 Wbp [↑](#footnote-ref-36)
37. Artikel 2:377 lid 6 BW [↑](#footnote-ref-37)
38. Artikel 23 lid 7 Wetboek van Strafrecht [↑](#footnote-ref-38)
39. Artikel 34a lid 8 Wbp (nieuw) [↑](#footnote-ref-39)
40. Artikel 31 lid 4 AVG, uit document DGD 2C/15039/15 [↑](#footnote-ref-40)
41. ‘Cbp publiceert Beleidsregels meldplicht datalekken’, www.autoriteitpersoonsgegevens.nl zoek op: beleidsregels meldplicht datalekken. [↑](#footnote-ref-41)
42. Artikel 34a lid 6 Wbp (nieuw). [↑](#footnote-ref-42)
43. *PbEG* 1995, C 93/1. [↑](#footnote-ref-43)
44. ‘Europese privacyrichtlijn’*,* www.autoriteitpersoonsgegevens.nl zoeken op: Europese privacyrichtlijn. [↑](#footnote-ref-44)
45. ‘Press Release European Commission 15 juni 2015’, [www.europa.eu](http://www.europa.eu) search for press releases. [↑](#footnote-ref-45)
46. [www.europadecentraal.nl/nieuws](http://www.europadecentraal.nl/nieuws) zoeken op: vertraging in werking treden Verordening bescherming persoonsgegevens. [↑](#footnote-ref-46)
47. [www.eerstekamer.nl/eu](http://www.eerstekamer.nl/eu) zoeken op aangenomen teksten van de vergadering van 12-03-2014. [↑](#footnote-ref-47)
48. Press Release European Commission 15 juni 2015, [www.europa.eu](http://www.europa.eu) search for press releases. [↑](#footnote-ref-48)
49. ‘New data protection standards to ensure smooth police cooperation in the EU’, [www.europarl.europa.eu](http://www.europarl.europa.eu) zoeken op: newsroom data protection. verholpen enico' manier lrivacy beleid van CCE0esteld door de groep of CCE-NL. Deze functie e Unie en dan moet het [↑](#footnote-ref-49)
50. Opmerking 8 voorafgaand aan de wettekst AVG, document DGD 2C/15039/15. [↑](#footnote-ref-50)
51. Artikel 3 lid 2 AVG uit document DGD 2C/15039/15. [↑](#footnote-ref-51)
52. Artikel 51, lid 2 AVG, uit document DGD 2C/15039/15. [↑](#footnote-ref-52)
53. Artikel 41, lid 1 AVG, uit document DGD 2C/15039/15. [↑](#footnote-ref-53)
54. [www.justitia.nl](http://www.justitia.nl) zoeken op: safe harbor [↑](#footnote-ref-54)
55. HvJEU C-362/14 Maximillian Schrems v. Data Protection Commissioner. [↑](#footnote-ref-55)
56. Artikel 77 lid 1 sub g Wbp en artikel 42 lid 2 sub b AVG uit document DGD 2C/15039/15. [↑](#footnote-ref-56)
57. HvJEU C-131/12 Google Spain SL, Google Inc. versus Agencia Española de Protección de Datos, Mario Costeja González. [↑](#footnote-ref-57)
58. Toelichting van juridische elementen van het voorstel AVG, document DGD 2C/15039/15. [↑](#footnote-ref-58)
59. Article 31 lid 1 AVG, uit document DGD 2C/15039/15. [↑](#footnote-ref-59)
60. Toelichting op de Verordening, eur-lex.europa.eu legal content 52012PC0011. [↑](#footnote-ref-60)
61. Een leaflet is een enkelvoudig blad, dat voor commerciële doeleinden wordt gebruikt om een korte boodschap achter laten. Wanneer er meer informatie wordt gewenst, kan een brochure worden toegezonden, nadat de betrokkene zijn contactgegevens heeft ingevuld. [↑](#footnote-ref-61)
62. Stappenplan 1 [↑](#footnote-ref-62)
63. Hoofdstuk 3 [↑](#footnote-ref-63)
64. Melding 1423451, *Cbp,* www.autoriteitpersoonsgegevens.nl (zoek op meldingenregister). [↑](#footnote-ref-64)
65. Hooghiemstra & Nouwt 2014, p. 44. [↑](#footnote-ref-65)
66. Hof ’s Hertogenbosch 14 oktober 2003, ECLI:NL:GHSHE:2003:AM7927. [↑](#footnote-ref-66)
67. Bijlage 2. [↑](#footnote-ref-67)
68. Bijlage 3. [↑](#footnote-ref-68)
69. Hooghiemstra & Nouwt 2014, p. 93. [↑](#footnote-ref-69)
70. Zie hoofdstuk 5, wettelijk kader EU en paragraaf 6.2 [↑](#footnote-ref-70)
71. Vergunning, kenmerk WBP0900001. [↑](#footnote-ref-71)
72. Vergunningaanvraag opgesteld door externe partij. Datum 29 December 2009. [↑](#footnote-ref-72)
73. Hooghiemstra & Nouwt 2014, p. 47. [↑](#footnote-ref-73)
74. Dit contract is niet bijgesloten als bijlage, wegens vertrouwelijke afspraken. [↑](#footnote-ref-74)
75. Sauerwein & Linnemann 2002, p. 51. [↑](#footnote-ref-75)
76. Bijlage 4 voorbereiding meldingsformulier Wbp klantenbestand, vraag 8. [↑](#footnote-ref-76)
77. Sauerwein & Linnemann 2002, p. 35. [↑](#footnote-ref-77)
78. Comission decicions on the adequacy of the protection of personal data in third countries. <http://ec.europa.eu> search for international transfers and adequacy. [↑](#footnote-ref-78)
79. Wettelijk kader wordt geschetst in hoofdstuk 5. [↑](#footnote-ref-79)
80. COM 2015/566 Communication from the Commission to the Parliament and the Council. [↑](#footnote-ref-80)
81. **2000/520/EG: Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd. PbEG 2000, C2441.**  [↑](#footnote-ref-81)
82. COM/2013/847 final [↑](#footnote-ref-82)
83. [Case C-362/14](http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1444299455884&uri=CELEX:62014CJ0362) – Schrems v Data Protection Commissioner [↑](#footnote-ref-83)
84. Statement of the Article 29 Working party, [ec.europa.eu](http://ec.europa.eu) search for press releases Article 29 Working party, filter on date 16 October 2015. [↑](#footnote-ref-84)
85. ,‘Doorgifte binnen en buiten de EU’, www.autoriteitpersoonsgegevens.nl, zoek op: internationaal gegevensverkeer. [↑](#footnote-ref-85)
86. Bijlage 5: brief van het Ministerie [↑](#footnote-ref-86)
87. Bijlage 6: vergunning voor data uitwisselen met de VS [↑](#footnote-ref-87)
88. Zie hoofdstuk 2 tot en met 5. [↑](#footnote-ref-88)
89. Bijlage 11: Privacy Policy. [↑](#footnote-ref-89)
90. Bijlage 12: Richtlijn Gegevens Privacy. [↑](#footnote-ref-90)
91. Berkvens & Hennekens 2015, p. 15. [↑](#footnote-ref-91)
92. Uitleg in hoofdstuk 5 scriptie. [↑](#footnote-ref-92)
93. Bijlage 7: Policy voor Acceptabel IT-gebruik. [↑](#footnote-ref-93)
94. Pagina 9 van deze scriptie. [↑](#footnote-ref-94)
95. Pagina 20 van deze scriptie. [↑](#footnote-ref-95)
96. Artikel 8 sub f Wbp, zie hoofdstuk 3 voor de wettelijke grondslag en h6 voor praktische toepassing. [↑](#footnote-ref-96)
97. Hooghiemstra & Nouwt 2014, p. 47. [↑](#footnote-ref-97)
98. In paragraaf 6.2 kan gelezen worden hoe er nu met de Safe-Harbor overeenkomst moet worden omgegaan. [↑](#footnote-ref-98)
99. Bijlage 9: Code of Business Conduct, p. 14. [↑](#footnote-ref-99)
100. Bijlage 10: Gesprek met IT-specialist Rob Franken en Perry Wetsteijn. [↑](#footnote-ref-100)
101. Bijlage 10: Gesprek met IT-specialist Rob Franken en Perry Wetsteijn. [↑](#footnote-ref-101)
102. Het wettelijk kader wordt geschetst in hoofdstuk 5. [↑](#footnote-ref-102)
103. Artikel 6 en 11 Wbp, eerder uitgelegd in hoofdstuk 3. [↑](#footnote-ref-103)
104. Pagina 29 scriptie [↑](#footnote-ref-104)