PARAAT VOOR PRIVACY

Een onderzoek naar de wijze waarop Canon zich kan voorbereiden op de toekomstige privacywetgeving

Canon Nederland N.V.

L.M.C. (Lizette) Gevers
Juridische Hogeschool Avans- Fontys

’s-Hertogenbosch, 1 juni 2015

PARAAT VOOR PRIVACY

Een onderzoek naar de wijze waarop Canon zich kan voorbereiden op de toekomstige privacywetgeving

Auteur: L.M.C. (Lizette) Gevers
Studentnummer: 2051515

Onderwijsinstelling: Juridische Hogeschool Avans- Fontys te ‘s-Hertogenbosch
Opleiding: HBO-Rechten
1e docent: Mevr. Mr. M. (Marieke) Boer
2e docent: Dhr. Mr. B.C.M. (Bart) Hooijdonk

Afstudeerorganisatie: Canon Nederland N.V.
Afstudeermentor: Mevr. Mr. G.M. (Gaby) Keijsper

Afstudeerperiode: februari 2015 – juni 2015

’s-Hertogenbosch, 1 juni 2015

Voorwoord

Voor u ligt een scriptie welke het resultaat is van een onderzoek naar de gevolgen van de nieuwe privacywetgeving voor Canon Nederland N.V. Een uitdaging, omdat het privacyrecht tijdens mijn opleiding kort is behandeld. Deze scriptie is geschreven in de afstudeerperiode van mijn studie HBO rechten aan de Juridische Hogeschool Avans-Fontys te ’s-Hertogenbosch.

Ik wil hierbij van de gelegenheid gebruik maken om alle mensen te bedanken die een bijdrage hebben geleverd aan de totstandkoming van deze afstudeerscriptie. Hierbij wil ik graag mijn directe collega’s binnen Canon bedanken voor de leuke tijd. Ze hebben me goed ontvangen en waren altijd erg behulpzaam. In het bijzonder wil ik Gaby Keijsper bedanken, die de functie als afstudeermentor heeft vervuld en me heeft voorzien van nuttige feedback. Daarnaast wil ik Daniëlle van der Zande bedanken voor al haar hulp en haar nuttige feedback.

Ook wil ik mijn afstudeerdocenten, Marieke Boer en Bart Hooijdonk bedanken voor hun begeleiding en feedback. En tot slot wil ik Rigarda van den Berg bedanken voor de hulp bij het redigeren van mijn tekst.

Lizette Gevers

’s-Hertogenbosch, juni 2015

Lijst van gebruikte afkortingen

ASP	Application Service Providing
AVG	Algemene Verordening Gegevensbescherming
AWB	Algemene wet bestuursrecht
BCR	Binding Corporate Rules
CBP	College bescherming persoonsgegevens
COS	Controle- en overige standaarden
EER	Europese Economische Ruimte
EU	Europese Unie
EVRM	Europees verdrag voor de bescherming van de rechten van de mens en de fundamentele vrijheden
FG	Functionaris voor de gegevensbescherming
N.V.	Naamloze Vennootschap
PIA	Privacy Impact Assessment
SaaS	Software as a Service
Wbp	Wet bescherming persoonsgegevens

Inhoudsopgave

Lijst van gebruikte afkortingen .....
Samenvatting .....
1 Inleiding 7
1.1 Probleembeschrijving 7
1.2 Centrale vraag 8
1.3 Deelvragen Uit de centrale vraag zijn verschillende deelvragen voortgevloeid: 8
1.4 Doelstelling 8
1.5 Methoden en technieken 9
1.6 Leeswijzer 9
2 Juridisch kader 10
2.1 Privacyregelgeving 10
2.2 Verwerken van persoonsgegevens 11
2.3 Voorwaarden voor verwerkingen 12
2.4 Beveiliging persoonsgegevens 13
2.5 Bewerker en verantwoordelijke 14
2.5.1 Verantwoordelijke 14
2.5.2. Bewerker 14
2.5.3. Subbewerkerschap 15
2.5.4 Tussenconclusie 16
2.6 Bewerkersovereenkomst 16
2.7 Rechten van betrokkene 17
2.7.1 Recht van inzage 17
2.7.2 Recht van correctie 17
2.7.3 Recht van verzet 17
2.8 Doorgifte van persoonsgegevens 18
2.9 Handhaving 19
2.9.1 CBP 19
2.9.2 Functionaris voor de gegevensbescherming 20
2.10 Privacy beleid 21
3 Algemene verordening gegevensbescherming 22
3.1 AVG 22
3.2 Toepassing verordening 22
3.3 Privacy by Design en Privacy by Default 22
3.4 Privacy Impact Assessment 24
3.5 Rol van bewerker en verantwoordelijke 25
3.5.1 Verplichtingen bewerker 25
3.7 Rechten van betrokkenen 25

3.7.1 Recht om te wissen 25
3.8 Functionaris voor de gegevensbescherming 27
3.8.1 Taken FG 27
3.8.2 Positie FG 27
3.8.3 Intern of extern? 27
3.9 Doorgifte naar derde landen 28
3.9.1 Besluit van een passend beschermingsniveau 28
3.9.2 Passende garanties 28
3.9.3 Binding Corporate Rules 29
3.10 Sancties 29
3.11 Meldplicht datalekken 30
4 Meldplicht datalekken en uitbreiding boetebevoegdheid 31
4.1 Aanleiding 31
4.2 Meldplicht datalekken 31
4.2.1 Wanneer wordt een datalek gemeld? 32
4.2.2 Wie meldt het datalek? 32
4.2.3 Aan wie wordt de datalek gemeld? 33
4.2.4 Logboek datalekken 33
4.2.5 Nalaten van de meldplicht 33
4.3 Uitbreiding boetebevoegdheid CBP 34
4.3.1 Bindende aanwijzing 34
4.3.2 Waarom een bindende aanwijzing? 34
4.3.3 Aan wie kan een bestuurlijke boete worden opgelegd? 35
5 Conclusies en aanbevelingen 36
5.1 Conclusies 36
5.2 Aanbevelingen 38
Literatuurlijst 40
Bijlage I standaard bewerkersovereenkomst Canon
Bijlage II Dienstverlening bewakingssysteem
Bijlage III Naar welke landen kan Canon persoonsgegevens doorgeven?
Bijlage IV De 7 fundamentele principes
Bijlage V Overzicht uitbreiding boetebevoegdheid
Bijlage VI Privacychecker

Samenvatting

Canon is gespecialiseerd in dienstverlening die onder andere bestaat uit print -en documentverwerking en de daarbij behorende bedrijfsprocessen. Vaak brengt het verlenen van deze dienstverlening met zich mee dat Canon over de persoonsgegevens van medewerkers en/of het klantenbestand van de opdrachtgever dient te beschikken. De wet- en regelgeving omtrent de verwerking van persoonsgegevens spelen derhalve een grote rol. De huidige Wet bescherming persoonsgegevens (hierna: Wbp) is gebaseerd op een privacyrichtlijn die stamt uit 1995. In januari 2012 presenteerde de Europese Commissie daarom een Algemene verordening gegevensbescherming (hierna: AVG) die de huidige wetgeving gaat veranderen. Deze treedt waarschijnlijk in werking in de loop van 2016. Om daarop vooruit te lopen is de Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP (hierna: Meldplicht datalekken en uitbreiding boetebevoegdheid) in Nederland ingediend. Op 26 mei 2015 is deze wet aangenomen en zal omstreeks 1 januari 2016 in werking treden.

In dit onderzoeksrapport staat daarom de volgende vraag centraal: “Op welke wijze kan Canon voldoen aan de Meldplicht datalekken en uitbreiding boetebevoegdheid en de AVG ten aanzien van de verwerking van persoonsgegevens bij de uitvoering van overeenkomsten met haar opdrachtgevers?”. In dit onderzoeksrapport is onderzoek gedaan naar de veranderingen van de nieuwe privacywetgeving. Naar aanleiding van een analyse van de rechtsbronnen en literatuur is de huidige privacywetgeving en de toekomstige privacywetgeving geïnterpreteerd en vervolgens uiteengezet. Hierin is naar voren gekomen dat de nieuwe wetgeving ingrijpende veranderingen met zich meebrengt voor Canon. Zo wordt Canon verplicht een intern privacy beleid vast te stellen, een Functionaris voor de gegevensbescherming (hierna: FG) aan te stellen, datalekken te melden, de begrippen Privacy by Design en Privacy by Default in acht te nemen en in bepaalde gevallen een Privacy Impact Assessment (hierna: PIA) uit te voeren. Ook worden de rechten van betrokkenen veranderd, het recht op correctie wordt uitgebreid met het recht om te wissen. En dan tot slot de boetes, de toezichthouder kan boetes tot € 1 miljoen of 5%[1] van de jaarlijkse omzet opleggen bij overtredingen.

De belangrijkste aanbeveling is om zo spoedig mogelijk een FG intern aan te nemen, deze FG kan Canon klaarstomen op de nieuwe wetgeving. Ook wordt aanbevolen om een protocol op te stellen met daarin een aantal actiepunten die moeten worden ondernomen op het moment dat sprake is van een datalek. Daarnaast is het verstandig om de bewerkersovereenkomst aan te passen. Hierin wordt duidelijk vastgelegd wie de verantwoordelijke en (sub)bewerker is. Daarnaast kunnen hierin aansprakelijkheden rondom het adequaat afwerken van datalekken worden vastgelegd. Tevens wordt aanbevolen om de beveiligingsmaatregelen kritisch te bekijken en zo mogelijk aan te passen zodat het beschermingsniveau optimaal is. Zo kunnen de eventuele hoge boetes worden voorkomen. Eveneens wordt aanbevolen om zo snel mogelijk een privacybeleid op te stellen en bewustwording van medewerkers te creëren door eventuele privacytrainingen en/of privacyvoorlichtingen die door de FG kunnen worden gegeven. Ook wordt aanbevolen om de 7 principes van Ann Cavoukian in acht te nemen bij het toepassen van de principes van Privacy by Design en Privacy by Default en in bepaalde gevallen een PIA uit te voeren. Aanbevolen wordt om in ieder geval PIA’s uit te voeren bij dienstverlening waar gevoelige persoonsgegevens worden verwerkt. Tot slot wordt aanbevolen om procedures in te richten om aan verzoeken van betrokkenen te kunnen voldoen.

[1] 5% van de jaarlijkse omzet op grond van de AVG, maar 10% op grond van de Meldplicht datalekken en uitbreiding boetebevoegdheid.

1 Inleiding

In dit hoofdstuk wordt eerst het probleem beschreven. Hierna wordt de centrale vraag gegeven die uit de probleembeschrijving is voortgevloeid met de bijbehorende deelvragen. Vervolgens komt de doelstelling aan bod. Daaropvolgend worden de methoden en technieken van het onderzoek beschreven, hierbij wordt ingegaan hoe het onderzoek is uitgevoerd. Tot slot de leeswijzer, dit geeft een weergave van het onderzoek.

1.1 Probleembeschrijving

Canon Nederland N.V. (hierna: Canon) is een leverancier op het gebied van Digital Imaging en Informatie Technologie, voor zowel particulieren als bedrijven. De activiteiten van Canon in Nederland richten zich voornamelijk op de zakelijke markt, ook wel Business Imaging genoemd. Dit houdt in het leveren van producten en diensten op het gebied van print- en documentmanagement voor kantoor- en productieomgevingen.

Naast het leveren en beheren van multifunctionals (printers bestemd voor de zakelijke markt) is Canon gespecialiseerd in de dienstverlening ten aanzien van print- en documentmanagement. Deze dienstverlening bestaat onder andere uit documentdiensten van de opmaak (waarbij Canon via diverse klantdatabases informatie ontvangt) tot archivering van documenten. Hieronder valt bijvoorbeeld ook het afdrukken en couverteren[2] van brieven. Canon heeft een oplossing ontwikkeld die controleert dat de gepersonaliseerde brieven in de juiste envelop worden geplaatst. Voor de uitvoering van deze gepersonaliseerde dienstverlening is het noodzakelijk om over de persoonsgegevens van de ontvanger van de (polis)brief te beschikken. De regels omtrent het verwerken en beschermen van persoonsgegevens spelen derhalve een grote rol bij deze vorm van dienstverlening. Tijdens de uitvoering van deze dienstverlening hebben zich in het verleden echter problemen voorgedaan. Zo zijn testbestanden met live-klantdata op een testserver, in het beheer van een derde partij, geplaatst. Door een fout werden de klantdata door Google geïndexeerd en was de klantdata in Google online benaderbaar. Daarnaast is het voorgekomen dat batches[3] dubbel of naar de verkeerde geadresseerden werd verzonden.

Deze gebeurtenissen hadden nadelige gevolgen voor de persoonlijke levenssfeer van betrokkenen. De Wbp stelt regels voor het opslaan, verzamelen, verstrekken en combineren (ook wel het verwerken) van persoonsgegevens. De Wbp bepaalt dat de verantwoordelijke[4] kan worden aangesproken indien iemand schade lijdt door de Wbp.[5] De vraag is welke verantwoordelijkheden partijen hebben wanneer zij door de Wbp worden aangemerkt als verantwoordelijke, bewerker of varianten hiervan. Het wordt ingewikkelder wanneer Canon persoonsgegevens gebruikt en verwerkt voor andere instellingen, maar een derde partij inschakelt voor het beheer[6] van de persoonsgegevens. De verantwoordelijke dient te voorzien in bescherming en juiste verwerking van de persoonsgegevens, maar ook diegene die de persoonsgegevens verwerkt heeft een bepaalde verantwoordelijkheid. De rolverdeling is belangrijk aangezien de schadeclaims omtrent de privacy inbreuk die werden ingediend bij opdrachtgevers van Canon, op haar beurt werden doorgelegd aan Canon.
Door de snelle technologische ontwikkelingen zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De snelheid en hoeveelheid waarin gegevens worden

2 Het couverteren bestaat uit het afdrukken van gepersonaliseerde documenten waarbij deze automatisch worden gevouwen en in een enveloppe worden geplaatst.
3 Een of meer taken van gegevensverwerking die zelfstandig door de afdrukapparatuur wordt verricht
4 In artikel 1 sub d Wbp wordt de verantwoordelijke gedefinieerd als: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
5 Zie artikel 49 Wbp.
6 Of op andere wijze namens Canon een deel van de dienstverlening uitvoert.

verzameld en gedeeld is enorm gestegen.[7] In januari 2012 presenteerde de Europese Commissie daarom een Algemene verordening gegevensbescherming (hierna: AVG) die de huidige privacyrichtlijn 95/46/EG en daarmee de Wbp (de richtlijn is in Nederland in de Wbp geïmplementeerd) gaat vervangen. De AVG zal naar verwachting in de loop van 2016 in werking treden. Daarnaast is in 2012 het wetsvoorstel meldplicht datalekken ingediend.[8] Het wetsvoorstel is op 26 mei 2015 aangenomen. Naar verwachting zal deze wet rond 1 januari 2016 in werking treden. De invoering van de AVG en de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP (hierna: Meldplicht datalekken en uitbreiding boetebevoegdheid) hebben gevolgen voor het privacy beleid van Canon.

De AVG brengt ingrijpende veranderingen met zich mee. Zo worden organisaties onder andere verplicht een intern privacy beleid vast te stellen, een FG aan te stellen en PIA's uit te voeren in bepaalde gevallen van veranderingen in diensten en producten, processen en informatiesystemen. Ook worden de rechten van betrokkenen veranderd. En dan tot slot de boetes, de toezichthouder kan boetes tot €1 miljoen of 5% van de jaarlijkse omzet opleggen bij overtredingen. Organisaties krijgen door de meldplicht datalekken een aantal nieuwe verplichtingen opgelegd wanneer inbreuken in de beveiliging van persoonsgegevens ontstaan. Door de uitbreiding van de bestuurlijke boetebevoegdheid van het College bescherming persoonsgegevens (hierna: CBP), kan het CBP meer en hogere boetes opleggen aan organisaties.

Aangezien Canon in verband met de uitvoering van haar overeenkomsten met opdrachtgevers persoonsgegevens verwerkt en deze gegevens intern en aan haar onderaannemers verstrekt, is het van belang deze gegevens te beschermen. Kortom, gezien de ingrijpende veranderingen van de AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid is een goede voorbereiding daarop voor Canon essentieel. In dit onderzoek wordt uiteengezet wat de nieuwe veranderingen van de AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid met zich meebrengen ten aanzien van de verwerking van persoonsgegevens tijdens het uitvoeren van overeenkomsten met haar opdrachtgevers. Uiteindelijk worden aanbevelingen gegeven op welke manier Canon zich op de nieuwe wetgeving kan aanpassen en voorbereiden.

1.2 Centrale vraag
Op basis van bovenstaande probleembeschrijving is de volgende centrale vraag geformuleerd: "Op welke wijze kan Canon voldoen aan de Meldplicht datalekken en uitbreiding boetebevoegdheid en de AVG ten aanzien van de verwerking van persoonsgegevens bij de uitvoering van overeenkomsten met haar opdrachtgevers?"

1.3 Deelvragen
Uit de centrale vraag zijn verschillende deelvragen voortgevloeid:

- Welke huidige privacy wet- en regelgeving is van toepassing op Canon bij het verwerken van persoonsgegevens bij de uitvoering van overeenkomsten met opdrachtgevers?
- Wat houdt de Meldplicht datalekken en uitbreiding boetebevoegdheid in en wat zijn de gevolgen hiervan voor Canon ten aanzien van de verwerking van persoonsgegevens bij uitvoering van overeenkomsten met opdrachtgevers?
- Wat houdt de AVG in en wat zijn de gevolgen hiervan voor Canon ten aanzien van de verwerking van persoonsgegevens bij uitvoering van overeenkomsten met opdrachtgevers?

1.4 Doelstelling
Op 1 juni 2015 wordt een scriptie overhandigd aan Canon Nederland N.V. met

[7] COM(2012)/0011 definitief.
[8] Kamerstukken II 2012/13, 33662, nr. 3, p. 1 (MvT)

aanbevelingen ten aanzien van de nieuwe gestelde eisen die de Meldplicht datalekken en uitbreiding boetebevoegdheid en de AVG met zich meebrengen ten aanzien van de verwerking van persoonsgegevens tijdens de uitvoering van overeenkomsten met haar opdrachtgevers.

1.5 Methoden en technieken

In dit onderzoek is gebruik gemaakt van de meest gebruikte strategie in een praktijk gericht juridisch onderzoek, namelijk het rechtsbronnen- en literatuuronderzoek. Rechtsbronnen in de vorm van de wet en jurisprudentie zijn onder de loep genomen en vervolgens geïnterpreteerd. Om een inzicht te krijgen in de huidige privacywetgeving in Nederland, is de Wbp, de Memorie van toelichting van de Wbp en literatuur inzake het privacyrecht geraadpleegd. De Meldplicht datalekken en uitbreiding boetebevoegdheid en de AVG zijn bestudeerd om een inzicht te krijgen in de nieuwe wetgeving.
Daarnaast is de Memorie van toelichting van de Meldplicht datalekken en uitbreiding boetebevoegdheid uitgebreid geanalyseerd. De tweede nota van wijziging naar aanleiding van het verslag is bekeken. Tot slot is gebruik gemaakt van elektronische bronnen. De bronnen zijn vergeleken en geanalyseerd. Vervolgens is alle informatie geïnterpreteerd en verwerkt in dit onderzoeksrapport. De informatie is bruikbaar en betrouwbaar aangezien zorgvuldig is gekeken naar de herkomst van de bron.

1.6 Leeswijzer

In hoofdstuk 2 staat de huidige privacywetgeving centraal. Om de gevolgen van de nieuwe wetgeving toe te lichten is het noodzakelijk om alvorens een goed beeld te schetsen van de huidige wetgeving. De Wbp wordt daarom hierin toegelicht met de daarbij behorende toepassing op Canon. Vervolgens wordt in hoofdstuk 3 duidelijk gemaakt wat de AVG inhoudt. Ook wordt in dit hoofdstuk verhelderd welke gevolgen de intreding van deze verordening heeft voor Canon. Daarna staat de AVG centraal in hoofdstuk 4. In dit hoofdstuk worden de gevolgen van de AVG weergegeven met weer de bijbehorende toepassing op Canon. Tot slot worden in het laatste hoofdstuk de conclusies en aanbevelingen van het onderzoek gegeven en dus wordt antwoord gegeven op de centrale vraag.

2 Juridisch kader

Persoonsgegevens nemen in onze complexe samenleving een steeds belangrijkere plaats in. Overheden en bedrijven willen meer weten van hun burgers of klanten teneinde hun producten en diensten beter af te stemmen op de behoeften van die burgers en klanten.[9] *Vaak wordt de levering van die producten of diensten helemaal of gedeeltelijk uitbesteed aan bedrijven zoals Canon. Deze diensten bestaan onder andere uit print- en documentverwerking en de daarbij behorende bedrijfsprocessen. Het komt vaak voor dat organisaties hele bedrijfsprocessen gericht op print- en documentmanagement uitbesteden aan Canon. Vaak brengt het verlenen van de dienstverlening met zich mee dat Canon over de persoonsgegevens van de klant moet beschikken. Zo heeft Canon bijvoorbeeld (dienstverlenings)overeenkomsten met financiële instellingen zoals pensioenmaatschappijen. Canon verzorgt voor hen documentdiensten van de opmaak tot archivering van onder andere polisbrieven. In deze brieven staan gevoelige (persoons)gegevens. Ook heeft Canon dienstverleningsovereenkomsten met onderwijsinstellingen. Canon verzorgt voor hen niet alleen de printvoorzieningen, maar ook de studentenpas met het daaraan gekoppelde betaaloplossing voor alle betaalde faciliteiten op de campus, waaronder printen, maar ook catering, campus winkels en parkeren.*
De regels omtrent het verwerken en beschermen van persoonsgegevens spelen derhalve een grote rol bij deze vorm van dienstverlening. In dit hoofdstuk komt aan de orde welke huidige wet- en regelgeving van toepassing is op het privacy recht met de daarbij behorende toepassing op de gegevensverwerking bij Canon.

2.1 Privacyregelgeving

De bescherming van persoonsgegevens in Nederland is geregeld in de Wbp. De wet is gebaseerd op bepalingen uit onze Grondwet en op Europese wetgeving. Artikel 10 van onze Grondwet brengt het fundamentele karakter van het recht op bescherming van persoonsgegevens tot uitdrukking. Dit artikel schrijft voor dat een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens de wet te stellen beperkingen. Op internationaal niveau is het recht op privacy verankerd in artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM). Hierin staat dat een ieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. De Europese Privacyrichtlijn uit 1995[10] is al jaren de basis van de huidige Europese wetgeving inzake persoonsgegevensbescherming. De Wbp is de Nederlandse uitwerking van de richtlijn. Elke Europese lidstaat heeft op basis van deze richtlijn een eigen privacywet opgesteld. De privacywetgeving is dus in de verschillende Europese lidstaten op een andere manier geïmplementeerd, wat rechtsongelijkheid met zich meebrengt. Daarnaast zijn door de snelle technologische ontwikkelingennieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De mate waarin gegevens worden verzameld en gedeeld, is enorm gestegen.[11] In januari 2012 presenteerde daarom de Europese Commissie een Algemene verordening gegevensbescherming (hierna: AVG) die de huidige privacyrichtlijn (en dus de Wbp) gaat vervangen. Door de directe werking van de Verordening in de lidstaten van de Europese Unie brengt dit uniformiteit met zich mee. Waarin eerst de mogelijkheid bestond de richtlijn op een eigen manier te implementeren in de nationale wetgeving en daarmee in een bepaalde mate af te wijken van de richtlijn, is dit niet meer mogelijk in de toekomst met de komst van de AVG. Naar verwachting zal de verordening in de loop van 2016 in werking treden. Deze nieuwe wet wordt dan direct van kracht in de Europese Unie, en dus ook in

[9] Mr. J.H.J. Terstegge, *Privacyclausules in dienstverleningscontracten*, Contracteren 63 2007/3.
[10] 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, PB L 281 van 23.11.1995.
[11] COM(2012)/0011 definitief.

Nederland. Lidstaten hebben dan nog een implementatietermijn van 2 jaar de tijd om volledig aan de wet te voldoen. In hoofdstuk 3 komt de AVG uitgebreid aan de orde en wordt dieper ingegaan op de gevolgen voor Canon. Om toe te groeien tot deze verordening is in Nederland een wetsvoorstel Meldplicht datalekken en uitbreiding boetebevoegdheid ingediend. In hoofdstuk 4 komt de Meldplicht datalekken en uitbreiding boetebevoegdheid uitgebreid aan de orde en wordt ingegaan op de gevolgen voor Canon voor de nieuwe wetgeving. In dit hoofdstuk komt de Wbp aan de orde, die op dit moment nog van toepassing is.

2.2 Verwerken van persoonsgegevens

De Wbp is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[12] Onder een 'persoonsgegeven' wordt verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[13] Hierin kan onderscheid gemaakt tussen direct en indirecte identificerende persoonsgegevens.[14] Van direct identificerende persoonsgegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder te veel omwegen eenduidig is vast te stellen, zoals naam, adres en geboortedatum. Van indirecte identificerende gegevens is sprake wanneer via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.[15] Degene op wie een persoonsgegeven betrekking heeft, wordt betrokkene genoemd.[16]
De Wbp definieert de 'verwerking' van persoonsgegevens als: 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.[17] Dit zijn slechts voorbeelden en deze opsomming is niet limitatief. 'Verwerken' is een begrip dat ruim wordt uitgelegd. Elke handeling met betrekking tot persoonsgegevens is een verwerking van persoonsgegevens.

De wet maakt onderscheid tussen geheel of gedeeltelijk geautomatiseerde verwerking en niet geautomatiseerde verwerking die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Dit onderscheid suggereert dat in het geval geheel of gedeeltelijke automatisering alle verwerkingen onder de wet vallen en in het geval van niet geautomatiseerde verwerkingen slechts die waarin sprake is van (voorgenomen) opslag in een bestand. De wettelijke definitie van het begrip 'bestand' is echter zo ruim dat het vrijwel altijd onder het begrip bestand valt.[18] De Wbp definieert een bestand namelijk als elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is, of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.[19]

[12] Artikel 2 lid 1 Wbp.
[13] Artikel 1 sub a Wbp.
[14] Artikel 2 onder a van de Richtlijn 95/46/EG.
[15] Kamerstukken II 1997/98, 25892, nr. 3, p. 48 (MvT).
[16] Artikel 1 sub f Wbp.
[17] Artikel 1 sub b Wbp.
[18] De Vey Mestdagh 2014, p. 26.
[19] Artikel 1 sub c Wbp.

Verwerkt Canon persoonsgegevens?

Organisaties besteden hele bedrijfsprocessen uit aan Canon. Bij het uitbesteden van de processen is het noodzakelijk voor Canon om onder andere over persoonsgegevens van medewerkers en/of het klantenbestand van de opdrachtgever te beschikken. Afhankelijk van de opdracht raadpleegt en bewaart Canon deze gegevens. Hierdoor valt het gebruiken van de persoonsgegevens onder de definitie "verwerken". De personen zijn op grond van de gegevens (naam, adres woonplaats) direct identificeerbaar. Hierbij gaat het om de verwerking van persoonsgegevens voor zakelijke doeleinden. Omdat de persoonsgegevens via software, hosting, computers en printers worden verwerkt is sprake van geheel geautomatiseerde verwerking.

Canon verwerkt daarnaast klantgegevens bij de verkoop van producten en werknemersgegevens in het kader van haar werkgeverschap. Dit zijn ook persoonsgegevens. In dit onderzoek wordt alleen ingegaan op de verwerking van persoonsgegevens waarover Canon noodzakelijkerwijs dient te beschikken bij de uitvoering van haar dienstverleningsovereenkomsten met de opdrachtgevers.

2.3 Voorwaarden voor verwerkingen

Elke verwerking van persoonsgegevens moet rechtmatig zijn. Een rechtmatige verwerking vindt plaats in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze.[20] Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld[21] en het verwerken ervan moet verenigbaar zijn met deze doeleinden.[22] Het vereiste van doelbinding verbiedt het gebruik van persoonsgegevens voor andere doeleinden dan waarvoor ze zijn verzameld.
De verwerking moet gerechtvaardigd zijn op grond van ten minste één van de in artikel 8 Wbp genoemde grondslagen. Zo is sprake van gerechtvaardigde verwerking wanneer ondubbelzinnige toestemming van de betrokkene is verleend[23] of dat verwerking noodzakelijk is voor de vervulling van een publiekrechtelijke taak.[24] De verdere verwerking is verenigbaar met de doeleinden waarvoor de persoonsgegevens zijn verkregen. De verantwoordelijke dient de nodige voorzieningen te treffen om te garanderen dat de verdere verwerking uitsluitend plaatsvindt ten behoeve van deze specifieke doeleinden. Tevens mogen de persoonsgegevens slechts worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.[25] Daarbij moet de verwerking juist en nauwkeurig zijn.[26]
In de Wbp staat geen concrete bewaartermijn voor persoonsgegevens. Er staat enkel dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is.[27] In bijvoorbeeld de Archiefwet, het Burgerlijk Wetboek of de onderwijs- en belastingwetgeving zijn wel specifieke regels omtrent bewaartermijnen opgesteld.

Verwerkt Canon persoonsgegevens rechtmatig?

Canon verwerkt persoonsgegevens omdat dit noodzakelijk is voor de uitvoering van de overeenkomst met opdrachtgever.[28] De opdrachtgever heeft een overeenkomst met de betrokkene. De opdrachtgever verwerkt deze persoonsgegevens rechtmatig aangezien de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is. Dit is een gerechtvaardigde verwerking op grond van artikel 8 sub b Wbp. Ondanks dat concrete bewaartermijnen voor persoonsgegevens ontbreken in de Wbp dient Canon rekening te houden met

[20] Artikel 6 Wbp.
[21] Artikel 7 Wbp.
[22] Artikel 9 lid 1 Wbp.
[23] Artikel 8 sub a Wbp.
[24] Artikel 8 sub e Wbp.
[25] Artikel 11 lid 1 Wbp.
[26] Artikel 11 lid 2 Wbp.
[27] Artikel 10 lid 1 Wbp.
[28] De opdrachtgever wordt meestal gezien als de verantwoordelijke. Zie paragraaf 2.5.2.

specifieke regels inzake bewaartermijnen voor bepaalde documenten in de verschillende wetten zoals de onderwijs- of belastingwetgeving.

2.4 Beveiliging persoonsgegevens

De verantwoordelijke dient technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Technische maatregelen betreffen de wijze waarop de techniek is ingericht en ingesteld. Organisatorische maatregelen beogen het handelen van de mensen zo te reguleren dat het gebruik van de techniek veiliger wordt.[29] De maatregelen garanderen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.[30]

De begrippen uit artikel 13 Wbp zijn erg abstract. Het CBP heeft daarom in 2013 richtsnoeren gepubliceerd voor de beveiliging van persoonsgegevens.[31] Deze richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren worden in samenhang gebruikt met de algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging. De Code voor informatiebeveiliging, zoals de NEN-ISO 27001 en de NEN-ISO 27002[32], zijn bekende voorbeelden van algemene erkende systemen voor informatiebeveiliging in een organisatie. Ook zijn er erkende specifieke systemen gericht op sectoren zoals de gezondheidszorg (zoals de NEN 7510[33]) of financiële instellingen (zoals de Controle- en overige standaarden: COS[34]).

Hoe garandeert Canon een passend beveiligingsniveau van haar maatregelen?
Per dienstverlening bekijkt Canon welke maatregelen te treffen zodat dit een passend beveiligingsniveau garandeert. Per overeenkomst wordt gekeken welke maatregelen worden getroffen. Hierbij wordt gekeken naar de fysieke beveiliging van de ruimtes/omgeving waar de machines zich bevinden, de bedrijfsmiddelen en de systemen maar ook naar de beveiliging van het personeel. Opdrachtgevers stellen soms bij een opdracht de eis voor een bepaald certificaat of een bepaald beveiligingsniveau. Canon heeft daarom bepaalde specifieke verklaringen ten aanzien van standaarden die bij de dienstverlening van de opdrachtgever wordt verwacht. Die desbetreffende verklaring geldt alleen voor de dienstverlening bij die opdrachtgever. Zo wordt de COS 3000 (Controle- en overige standaarden) als standaard gebruikt bij de overeenkomsten van Canon met de pensioenmaatschappijen. Dit is een kwaliteitsstandaard gericht op opdrachten voor financiële instellingen. Canon heeft op dit moment geen algemeen toepasbaar certificaat voor informatiebeveiliging, zoals de NEN-ISO 27001 of de NEN-ISO 27002.

---

[29] ICT-notaris <http://www.it-notaris.nl/275/beveiligen-van-ict-en-aansprakelijkheid>
[30] Artikel 13 Wbp.
[31] CBP-richtsnoeren: Beveiliging van persoonsgegevens, 2013 <www.cbpweb.nl>
[32] De NEN-ISO/IEC 27001 is een standaard voor het specificeren van eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System in het kader van de algemene bedrijfsrisico's voor de organisatie. De NEN-ISO/IEC 27002 is een standaard met richtlijnen en principes voor het initiëren, implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie.
[33] De NEN 7510 is een standaard bedoeld voor informatiebeveiliging in de zorg. Deze norm biedt een gemeenschappelijk kader voor het inrichten van de informatiebeveiliging in de gezondheidszorg.
[34] Nadere voorschriften COS zijn van toepassing voor opdrachten die uitgevoerd worden door een accountant en deze voorschriften hebben als doelstelling om de kwaliteit te waarborgen. Het Koninklijk NIVRA wil hiermee een accountantsberoep ontwikkelen en te bevorderen dat is staat is op uniforme wijze diensten te verlenen van hoge kwaliteit.

2.5 Bewerker en verantwoordelijke

Zowel de Europese als nationale wetgeving (de Wbp) maakt onderscheid tussen de begrippen ‘verantwoordelijke’ en ‘bewerker’.

2.5.1 Verantwoordelijke

De belangrijkste verplichtingen uit de Wbp rusten op de verantwoordelijke. Verantwoordelijke is diegene[35] die, al dan niet gezamenlijk met een ander, het doel en de middelen voor de werking van persoonsgegevens vaststelt.[36] De verantwoordelijke is, zoals de naam al doet vermoeden, in principe (eind)verantwoordelijk voor de verwerking van persoonsgegevens. De verantwoordelijke heeft veel (materiele) wettelijke verplichtingen, zoals het vaststellen van het doel en de middelen voor de verwerking. Ook heeft de verantwoordelijke een tweetal formele verplichtingen. Zo dient de verantwoordelijke in een aantal gevallen de voorgenomen verwerking melden (meldingsplicht)[37] en informeert hij in de meeste gevallen de betrokkene over de voorgenomen verwerking (informatieplicht)[38].

2.5.2. Bewerker

Een verantwoordelijke heeft zeggenschap over de gegevensverwerking, een bewerker niet. De bewerker is namelijk degene die ten behoeve van de verantwoordelijke de gegevens verwerkt, zonder aan het rechtstreeks gezag van de verantwoordelijke te zijn onderworpen.[39] Een bewerker handelt naar de instructies en onder de (uitdrukkelijke) verantwoordelijkheid van de verantwoordelijke. Bepalend is de positie tegenover de verantwoordelijke en de mate van zeggenschap die een bewerker heeft over de gegevensverwerking.[40] De bewerker mag de persoonsgegevens niet voor eigen doeleinden aanwenden. Een bewerker beperkt zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking. Beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz. worden niet door een bewerker genomen. Wanneer een bewerker deze zeggenschap wel zou verwerven, dient zij als verantwoordelijke worden aangemerkt.[41]

> ***Is Canon bewerker of verantwoordelijke?***
> *Meestal is de opdrachtgever verantwoordelijke en is Canon de bewerker. Maar niet altijd is duidelijk wie de verantwoordelijke en wie de bewerker is. In de literatuur is hiervoor een ezelsbruggetje gegeven. Wanneer een dienstverlener zijn diensten uitsluitend verleent aan zijn opdrachtgever, is hij in principe een bewerker. Heeft de dienstverlener daarentegen op basis van het contract met zijn opdrachtgever ook een rechtstreekste relatie met de betrokkenen dan is hij in beginsel een verantwoordelijke.[42] Canon heeft meestal geen rechtstreekse relatie met de betrokkenen, dat impliceert dat Canon in beginsel aangemerkt dient te worden als bewerker. Dit is meestal ook het geval.*
> *Echter, het is ook van belang wie de middelen voor de gegevensverwerking bepaalt. Degene die de middelen voor de gegevensverwerking bepaalt wordt in beginsel aangemerkt als de verantwoordelijke.*
>
> *Bij veel overeenkomsten die Canon sluit is het noodzakelijk om software te verstrekken zodat de dienstverlening juist kan worden uitgevoerd. Canon stelt meestal software beschikbaar aan de opdrachtgever op basis van Application Service Providing (hierna: ASP) of Software as a Service (hierna: SaaS). ASP en SaaS liggen in elkaars verlengde. Dit zijn begrippen om aan te geven dat Canon ‘op afstand’*

[35] Een natuurlijke persoon, rechtspersoon, ieder ander of een bestuursorgaan.
[36] Artikel 1 sub d Wbp.
[37] Artikelen 27-32 Wbp.
[38] Artikelen 33-34 Wbp.
[39] Artikel 1 sub e Wbp.
[40] Thole/van der Jagt/Roerdink 2014.
[41] Kamerstukken II 1997/98, 25892, nr. 3, p. 61/62 (MvT).
[42] Thole/van der Jagt/Roerdink 2014.

software beschikbaar stelt via internet of een ander netwerk. Hierbij wordt geen fysieke drager met software verstrekt.[43] *Software beschikbaar stellen via internet wordt ook wel Cloud computing genoemd. De software is in handen van Canon en de opdrachtgever heeft een gebruiksrecht voor een bepaalde tijd zodat zij gebruik kan maken van de software. Wie de middelen voor de gegevensverwerking bepaalt, ligt bij het uitbesteden van bedrijfsprocessen, waarin ASP, SaaS en Cloud computing deel van uitmaken, meestal iets ingewikkelder. De kern van het uitbesteden van deze bedrijfsprocessen is nu juist dat de opdrachtgever nog wel verantwoordelijk is voor het bepalen wat Canon dient te doen, maar niet hoe. Canon beslist dan over de wijze waarop de gegevensverwerking plaatsvindt. Is Canon daarmee (mede)verantwoordelijke? Dit hangt af van de relatie tussen partijen.*

Wanneer Canon werkzaamheden verricht voor de opdrachtgever en haar daarbij volledig aan de instructies van de opdrachtgever onderwerpt en uitsluitend onder diens verantwoordelijkheid gegevens opslaat, is de Canon geen (mede)verantwoordelijke, maar bewerker. De gegevensverwerking is echter meestal voor Canon slechts een uitvloeisel van een geheel bedrijfsproces. Canon is dan mogelijk zelf de (mede)verantwoordelijke omdat zij dan diegene is die de middelen voor de gegevensverwerking bepaalt.

Wanneer Canon als (mede)verantwoordelijke wordt aangemerkt, geeft dit meer verplichtingen. Zo is de verantwoordelijke verantwoordelijk voor de persoonsgegevens, ook als de gegevens feitelijk door (sub)bewerkers[44] *worden verwerkt. Ook heeft de verantwoordelijke de controleplicht dat de gemaakte afspraken worden nageleefd en vooral of de persoonsgegevens adequaat worden beveiligd. Bij een geschil of een fout van de eventuele (sub)bewerker wordt de verantwoordelijke daarop aangesproken door het CBP, niet de (sub)bewerkers. Canon wordt daarom graag als bewerker aangemerkt. De opdrachtgever blijft dan eindverantwoordelijk voor de persoonsgegevens.*

2.5.3. Subbewerkerschap

Voor de bewerker bestaat de mogelijkheid om nog een subbewerker in te schakelen. Uit de verantwoordelijkheid van de verantwoordelijke vloeit voort dat hij uitdrukkelijk heeft ingestemd met het subbewerkerschap. Indien de verantwoordelijke daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker delen van de verwerking uitbesteden aan subbewerkers. De bewerker behoudt wel zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke. De subbewerker treft daarbij passende beveiligingsmaatregelen. Deze maatregelen worden vastgelegd in de overeenkomst tussen de bewerker en de subbewerker. De verantwoordelijke moet in staat worden gesteld toe te zien op naleving.
De bewerker dient contractueel verzekerd te hebben dat de subbewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt.[45]

Heeft Canon te maken met subbewerkerschap?

Canon maakt vrijwel altijd gebruik van onderaannemers hetzij voor aanvullende benodigde software, hetzij voor serverruimte, hostingdiensten of databeheer, maar ook voor tal van andere diensten van derden. Canon heeft te maken met subbewerkerschap wanneer zij als bewerker wordt aangemerkt en gebruikt maakt van onderaannemers voor deze aanvullende diensten. De opdrachtgever geeft daarvoor in zijn overeenkomst met Canon uitdrukkelijk ruimte. De verantwoordelijke

[43] Zie artikel 1 algemene voorwaarden Canon.
[44] Zie meer informatie over subbewerkers in de volgende paragraaf.
[45] Kamerstukken II 1997/98, 25892, nr. 3, p. 63.

dient hiervan op de hoogte te worden gesteld zodat deze in staat is toe te zien op de naleving van zijn afspraken met de bewerker. Wanneer Canon als (mede)verantwoordelijke wordt aangemerkt, moeten deze externe partijen worden aangemerkt als bewerkers.

2.5.4 Tussenconclusie

Het is dus meestal niet op voorhand duidelijk wie waarvoor verantwoordelijkheid draagt, welke bevoegdheden heeft of wie de controle kan uitoefenen op bepaalde verwerkingen van gegevens en wat de rechten en plichten zijn van alle betrokken partijen.[46] In het bepalen van de rolverdeling van 'verantwoordelijke', 'bewerker' en 'subbewerker' is enige vrijheid, maar dit reikt niet zo ver dat partijen dit geheel zelf bepalen. Een analyse van de soort data en de herkomst ervan is dan ook vereist te bepalen welke schakel in het geheel aangemerkt wordt als 'verantwoordelijke', 'bewerker' en eventueel 'subbewerker'. De kaders van de wettelijke definities worden hierbij in acht genomen. Ook is de relatie met de verantwoordelijke de mate van zeggenschap waarmee de verwerking van persoonsgegevens gepaard gaat bepalend voor de afbakening.[47] Canon wordt graag als bewerker aangemerkt omdat dit minder vergaande verplichtingen met zich meebrengt. Dit kan worden vastgelegd in een bewerkersovereenkomst.

2.6 Bewerkersovereenkomst

Het sluiten van een bewerkersovereenkomst is wettelijk verplicht.[48] Indien een verantwoordelijke persoonsgegevens laat verwerken door een bewerker, draagt hij zorg dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van deze maatregelen. De invulling van de uitvoering van de maatregelen door een bewerker wordt geregeld in een bewerkersovereenkomst.[49]

In een bewerkersovereenkomst (of andere regeling) dient dus in ieder geval te worden opgenomen dat de bewerker de persoonsgegevens uitsluitend verwerkt in opdracht van de verantwoordelijke. Verder geldt als uitgangspunt dat het partijen vrijstaat om de inhoud van een overeenkomst te bepalen. Dit uitgangspunt vloeit voort uit het niet expliciet in de wet neergelegd beginsel van contractsvrijheid.[50] Dit biedt partijen een grote mate van vrijheid met betrekking tot de vorm en inhoud van een bewerkersovereenkomst.

De verantwoordelijke draagt zorg voor de naleving van zijn verplichtingen[51], dit kan nader worden toegelicht in de overeenkomst. De Wbp bepaalt dat de verantwoordelijke kan worden aangesproken indien iemand schade leidt wanneer de verantwoordelijke zijn verplichtingen niet nakomt.[52] De bewerker kan ook aansprakelijk worden gesteld, voor zover de schade is ontstaan door zijn werkzaamheid. Hiervan is bijvoorbeeld sprake als hij verantwoordelijk is voor de beveiliging, dit niet voldoende is gebeurd en hieruit schade voortvloeit. Over deze aansprakelijkheden kunnen afspraken worden gemaakt in de bewerkersovereenkomst.

Wat is van belang wat betreft de bewerkersovereenkomst bij Canon?
Canon heeft een standaard bewerkersovereenkomst opgemaakt die meestal onderdeel uit maakt van de gehele contractenset. Deze bewerkersovereenkomst is opgesteld uit het oogpunt van bewerker. In bijlage I is de standaard bewerkersovereenkomst van Canon toegevoegd.

---

[46] Contracteren maart 2015, nr.1, Contracteren in de cloud – ken uw risico's- K. Daniëls en P. Kits
[47] www.cbpweb.nl <https://cbpweb.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-e-wbp>
[48] Artikel 14 Wbp.
[49] Een andere regeling mag ook volgens artikel 14 lid 2 Wbp.
[50] Brahn/Reehuis 2010, p. 240.
[51] Artikel 15 Wbp
[52] Artikel 49 Wbp

Aangezien de opdrachtgever vaak wordt aangemerkt als verantwoordelijke en dus bepaalde verplichtingen oplegt aan Canon, wordt vaak de bewerkersovereenkomst van de opdrachtgever voorgesteld. Het is voor Canon belangrijk dat een goede bewerkersovereenkomst wordt opgesteld en ondertekend. Zo kan worden voorkomen dat later onduidelijkheden bestaan over verantwoordelijkheden, instructies (eventuele vrijwaring voor Canon indien instructies zijn opgevolgd maar in strijd blijken met de wet- of regelgeving) en natuurlijk dat geen verwarring bestaat over wie verantwoordelijke of bewerker is. Tevens is het belangrijk afspraken te maken omtrent de aansprakelijkheid. De verdeling van aansprakelijkheid is bijvoorbeeld belangrijk wanneer schadeclaims omtrent eventuele privacy inbreuken die worden ingediend bij de verantwoordelijke worden doorgelegd aan Canon.

2.7 Rechten van betrokkene

De Wbp heeft rechten aan de betrokkene toegekend om transparantie aan de gegevensverwerking te creëren en te waarborgen dat de persoonsgegevens op een juiste manier worden verwerkt. De betrokkene heeft recht van inzage in zijn gegevens[53], het recht van correctie van zijn gegevens[54] en het recht van verzet tegen verwerking.[55]

2.7.1 Recht van inzage

De betrokkene heeft het recht zich tot de verantwoordelijke te wenden met het verzoek hem mede te delen of zijn persoonsgegevens worden verwerkt.[56] De verantwoordelijke deelt hem verplicht schriftelijke binnen vier weken mee of zijn persoonsgegevens worden verwerkt. [57]

2.7.2 Recht van correctie

De betrokkene kan, nadat hij inzage heeft gekregen in zijn persoonsgegevens, de verantwoordelijke verzoeken de persoonsgegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen. Dit kan alleen indien de persoonsgegevens feitelijk onjuist zijn of voor het doel - of de doeleinden - van de verwerking onvolledig of niet ter zake dienend zijn of anderszins in strijd met een wettelijk voorschrift worden verwerkt.

2.7.3 Recht van verzet

Indien gegevens op grond van artikel 8 sub e en/of onder f Wbp worden verwerkt, kan de betrokkene daartegen bij de verantwoordelijke te allen tijde verzet aantekenen in verband met zijn persoonlijke omstandigheden.[58] Artikel 8 sub e Wbp heeft betrekking op gegevensverwerking die noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan. Artikel 8 sub f Wbp heeft betrekking op de gegevensverwerking die noodzakelijk is voor de behartiging van het gerechtvaardigde belang.

Welke invloed hebben de rechten van betrokkenen op Canon?

Wanneer Canon wordt aangemerkt als verantwoordelijke, kunnen betrokkenen hun rechten bij Canon uitoefenen. Wanneer Canon als bewerker wordt aangemerkt en een betrokkene doet een verzoek tot inzage bij de verantwoordelijke, dient Canon de verwerkingen te verstrekken aan de verantwoordelijke. De betrokkenen dienen namelijk hun rechten te blijven uitoefenen, ook wanneer een bewerker betrokken is bij de verwerking van zijn persoonsgegevens. Tot nog toe zijn er weinig tot geen verzoeken hieromtrent ingediend bij Canon. Medewerkers zijn niet ingericht op de afhandeling van dergelijke verzoeken.

---

[53] Artikel 35 Wbp.
[54] Artikel 36 Wbp.
[55] Artikel 40 & 41 Wbp.
[56] Artikel 35 lid 1 Wbp.
[57] Artikel 35 lid 2 Wbp.
[58] Artikel 40 Wbp.

Mogelijk gaat Canon hier meer mee te maken krijgen in de toekomst met nieuwe vormen van dienstverlening. Canon gaat zich bijvoorbeeld namelijk in de toekomst meer richten op de markt voor videosurveillance. Zo heeft Canon recentelijk een aantal leveranciers van videomanagement overgenomen en is Canon hiermee een belangrijke speler in de markt van videosurveillance-apparatuur. Zo heeft Canon een overeenkomst met een voetbalclub en voorziet zij het voetbalstadion van beveiligingscamera's.[59] *Meer informatie over deze dienstverlening van Canon bij deze voetbalclub is te vinden in bijlage II. Betrokkenen zullen mogelijk in het vervolg verzoeken tot inzage van de camera-opnames indienen bij (de opdrachtgevers van) Canon.*

2.8 Doorgifte van persoonsgegevens

Door de invoering van de Europese Privacyrichtlijn hebben persoonsgegevens binnen de Europese Unie een gelijkwaardig beschermingsniveau. Hierdoor kan juridisch gezien vrij verkeer van persoonsgegevens plaatsvinden. De Wbp stelt dat 'doorgifte' van persoonsgegevens in beginsel slechts naar 'derde landen' is toegestaan wanneer dat land een 'passend beschermingsniveau' waarborgt.[60] Doorgifte wordt nergens in de wet gedefinieerd. Het sdu-commentaar van de Wbp geeft aan dat met doorgifte wordt gedoeld op het ter kennis brengen van de gegevens aan een persoon die zich bevindt buiten de rechtsmacht van één van de landen van de Europese Unie. Derde landen zijn alle landen buiten de EU, met uitzondering van de landen in de Europese Economische Ruimte (hierna: EER). Dit zijn Noorwegen, Liechtenstein en IJsland. Deze drie landen hebben zich verplicht de Europese privacyrichtlijn te implementeren in eigen wetgeving, waardoor zij een gelijkwaardig beschermingsniveau kennen.[61] Persoonsgegevens binnen de Europese Unie, inclusief Noorwegen, Liechtenstein en IJsland, kunnen dus vrijelijk worden doorgeven.

2.8.1 Wanneer heeft een derde land een 'passend beschermingsniveau'?

De Wbp definieert niet wat als 'passend' wordt beschouwd. Of een land een passend beschermingsniveau heeft moet worden beoordeeld aan de hand van de omstandigheden die op de doorgifte van gegevens van invloed zijn. De Europese Commissie kan besluiten of het recht van het derde land een passende bescherming biedt. De Europese Commissie heeft een positief besluit hierover verleend aan Andorra, Argentinië, Australië, Canada[62], Faeröer Eilanden, Guernsey, Isle of Man, Israël, Jersey, Uruguay, Verenigde Staten[63] en Zwitserland en Nieuw-Zeeland.
Daarnaast heeft de Europese Commissie verschillende modelcontracten goedgekeurd en beschikbaar gesteld.[64] Deze contracten worden ook wel aangeduid als 'Standard Contractual Clauses'. Deze modelcontracten worden erkend als een passende beschermingsniveau.
Tot slot worden de Binding Corporate Rules (hierna: BCR) ook gezien als een passend beschermingsniveau. De Europese Commissie heeft voor grote multinationals in 2003 een leidraad gepubliceerd voor het opstellen van interne gedragscodes die als alternatief dienen voor de modelcontracten om de doorgifte van persoonsgegevens binnen de organisatie toe te staan. Een dergelijke set van regels wordt aangeduid als BCR. De BCR bevatten

[59] Verder wordt in dit onderzoeksrapport niet ingegaan op het verwerken van persoonsgegevens met het gebruik van camerabeelden. Hierbij gelden specifieke regels.
[60] Artikel 76 lid 1 Wbp.
[61] www.cbpweb.nl <https://cbpweb.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-naar-derde-landen>
[62] Dit geldt alleen voor de delen die vallen onder de Canadian Personal Information Protection and Electronic Documents (Beschikking 2002/2/EG 20 december 2011).
[63] Dit geldt alleen als het gaat om organisaties die de 'Safe Harbor Principles' hebben onderschreven. In de Verenigde Staten ontbreekt namelijk een algemene wetgeving voor de bescherming van persoonsgegevens. De Safe Harbor- regels zorgen voor een praktische oplossing die erin voorziet dat er op een eenvoudige wijze toch rechtmatig gegevens kunnen worden uitgevoerd naar de Verenigde Staten.
[64] Zie ook Artikel 77 lid 1 sub g Wbp.

voorschriften over de wijze waarop binnen de multinational de privacyregelgeving wordt nageleefd, en welke waarborgen daartoe in het leven zijn geroepen.[65]

Het kan ook zo zijn dat het derde land geen passend beschermingsniveau heeft, maar doorgifte is geoorloofd op basis van een wettelijke uitzondering[66] of een vergunning die is verleend[67]. Een vergunning voor doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt, kan namelijk worden aangevraagd bij het CBP. De Minister van Veiligheid en Justitie kan deze vergunning met de daaraan verbonden nadere voorschriften verlenen.

> ***Geeft Canon persoonsgegevens door naar derde landen?***
> *Canon slaat haar gegevens op in de Cloud. De onderaannemers die Canon inschakelt, zijn meestal gevestigd in Nederland of binnen de Europese Unie. De vestigingsplaats zegt bij sommige bedrijven echter niets over de daadwerkelijke plaats waar de persoonsgegevens worden verwerkt. Zo kan het zijn dat een hostingbedrijf is gevestigd in een land binnen Europa, maar dat de daadwerkelijke hosting plaatsvindt in de Verenigde Staten. De Europese Commissie heeft enkel voor bedrijven gevestigd in de VS een positief besluit genomen wanneer dat bedrijf de Safe Harbor-regels in acht neemt. Het is voor Canon belangrijk om altijd na te gaan waar de bedrijven zijn gevestigd en in welk land de uiteindelijke verwerking plaatsvindt. In bijlage III staat een schematisch overzicht wanneer doorgifte van persoonsgegevens aan landen buiten de Europese Unie is toegestaan voor Canon.*
>
> *Canon neemt altijd in een bewerkersovereenkomst met haar onderaannemers een clausule op, waarin uitdrukkelijk staat dat de gegevens niet in een land buiten de Europese Unie mogen worden verwerkt om onduidelijkheid hierover te voorkomen en te voldoen aan de afspraken met haar opdrachtgevers*.

2.9 Handhaving

Handhaving van de Wbp kan op drie verschillende manieren plaatsvinden. Ten eerste heeft de betrokkene de mogelijkheid zijn rechten in te roepen bij de bestuursrechter[68] of bij de burgerlijker rechter.[69] Daarnaast biedt het wetboek van strafrecht op zekere hoogte al strafrechtelijke bescherming van de Wbp door het strafbaar stellen van het schenden van de geheimhoudingsplicht[70] en het in strijd handelen met de in artikel 75 lid 1 Wbp genoemde bepalingen. De in artikel 75 lid 1 Wbp genoemde bepalingen betreffen de verplichting om een persoon of instantie aan te wijzen in Nederland die namens een in het buitenland gevestigde verantwoordelijke handelt, de meldingsplicht en de doorgifte van gegevens aan een land buiten de EU met een niet passend beschermingsniveau. Een derde manier van handhaving is het toezicht door het CBP en toezicht in de vorm van een FG.

2.9.1 CBP

Het CBP is een onafhankelijke[71] instantie die tot taak heeft toe te zien op de verwerking van persoonsgegevens.[72] Het CBP wordt om advies gevraagd over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens.[73] Het CBP heeft een uitgebreide toezichthoudende taak met stevige onderzoeks- en handhavingsbevoegdheden.[74] Zo heeft het CBP de bevoegdheid een woning te betreden

[65] Thole/van der Jagt/Roerdink 2014.
[66] Artikel 77 lid 1 Wbp.
[67] Artikel 77 lid 2 Wbp.
[68] Als de verantwoordelijke een bestuursorgaan is.
[69] Zie artikel 45-50 Wbp.
[70] Artikel 272 Wetboek van Strafrecht.
[71] Zie artikel 52 lid 2 Wbp.
[72] Zie artikel 51 lid 2 Wbp.
[73] Artikel 51 lid 2 Wbp.
[74] De Vey Mestdagh 2014, p. 44.

zonder toestemming van de bewoner.[75] Ook is het CBP bevoegd tot oplegging van een last onder bestuursdwang om zo iemand te verplichten tot het verlenen van medewerking.[76] Daarnaast kan het CBP een last onder dwangsom opleggen en in een beperkt aantal gevallen ook een bestuurlijke boete. Een bestuurlijke boete van ten hoogste €4.500 kan opgelegd worden aan de verantwoordelijke ter zake van een overtreding van een administratieve verplichting, bijvoorbeeld de meldingsplicht. Een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden is bestemd, wordt namelijk gemeld bij het CBP (of bij de FG wanneer deze is aangesteld).[77] De Meldplicht datalekken en uitbreiding boetebevoegdheid geeft het CBP de bevoegdheid om in de toekomst aanzienlijke hogere boetes op te leggen. Hierover meer in hoofdstuk 4.

2.9.2 Functionaris voor de gegevensbescherming

Een verantwoordelijke of een organisatie waarbij verantwoordelijken zijn aangesloten hebben de mogelijkheid een eigen FG te benoemen.[78] Een natuurlijk persoon[79] kan hiertoe worden benoemd die voor de vervulling van zijn taak over toereikende kennis[80] beschikt en voldoende betrouwbaar kan worden geacht.[81] Een FG ziet, net zoals het CBP ook toe op de verwerking van de persoonsgegevens overeenkomstig het bij de wet bepaalde. De FG ziet toe op verwerking van persoonsgegevens binnen de organisatie. Dit systeem van interne toezichthouders komt oorspronkelijk voort uit het Duitse recht. Het toezicht van een FG strekt zich uit tot de verwerking van de persoonsgegevens door de verantwoordelijke die hem heeft benoemd of door de verantwoordelijken die zijn aangesloten bij de organisatie die hem heeft benoemd.[82]
De werkzaamheden van een FG kunnen onder meer zijn: toezicht houden, inventarisaties van gegevensverwerkingen maken, meldingen van gegevensverwerkingen bijhouden, vragen en klachten van mensen binnen en buiten de organisatie afhandelen, interne regelingen ontwikkelen, adviseren over technologie en beveiliging en input leveren bij het opstellen of aanpassen van een gedragscode. Heeft een organisatie een FG, dan behoudt het CBP als nationale toezichthouder alle bevoegdheden. Maar het CBP stelt zich terughoudend op bij organisaties met een FG.[83] Een organisatie kan één of meerdere FG's aanstellen. De organisatie moet de functionaris(sen) vervolgens aanmelden bij het CBP. Het CBP houdt een publieke lijst van aangemelde FG's bij.[84]

De aanstelling van een FG bescherming is op dit moment niet verplicht, organisaties mogen zelf bepalen of ze een FG benoemen. Dit verandert wanneer de AVG in werking treedt. Zie meer hierover in paragraaf 3.8.

> ***Heeft Canon een FG?***
> *Canon heeft geen intern toezicht in de vorm van een FG. Vanuit Canon Europa zijn wel interne richtlijnen uitgegeven. Op Europees niveau is er namelijk een interne expert groep voor privacy (binnen Canon EMEA: Europe Middle East and Africa), waarin privacy issues worden besproken. Zo wordt bijvoorbeeld uitgebreid onderzoek gedaan naar verwerking van persoonsgegevens binnen de verschillende business units.*

[75] Artikel 61 lid 2 Wbp.
[76] Artikel 61 lid 4 Wbp.
[77] Artikel 27 Wbp.
[78] Artikel 62 Wbp.
[79] Een ondernemingsraad of commissie komt hiervoor dus niet in aanmerking.
[80] Om dit te garanderen kunnen FG's lid worden van het Nederlands Genootschap van Functionarissen voor de gegevensbescherming (NGFG). Het NGFG heeft een aantal doelstellingen die bijdragen aan een goede taakvervulling van de FG.
[81] Artikel 63 lid 1 Wbp.
[82] Artikel 64 lid 1 Wbp.
[83] www.cbpweb.nl <https://cbpweb.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming>
[84] Artikel 63 lid 3 Wbp

2.10 Privacy beleid

Organisaties kunnen een privacy beleid opstellen. Door middel van dit privacy beleid kan aan de informatieplicht worden voldaan. De open normen uit de privacy wet- en regelgeving zoals de Wbp kunnen hiermee worden vertaald naar de specifieke situatie van de organisatie. Hierin wordt onder andere aangegeven hoe wordt omgegaan met persoonsgegevens, op welke manier verwerking plaatsvindt en welke middelen hierbij worden gebruikt.

Heeft Canon een (intern) privacy beleid?

Canon Inc. heeft Océ-Nederland B.V. (hierna: Océ) overgenomen. In 2012 zijn de bedrijfsactiviteiten van Océ samengevoegd met de activiteiten van Canon in Nederland. Océ had destijds een privacy commissie waar privacy issues werden overlegd, het privacy beleid werd opgesteld en gecontroleerd. Ook werden in deze commissie eventuele klachten behandeld. Sinds de overname is geen lokale privacy commissie aanwezig bij Canon Nederland en ontbreekt een goed privacy beleid binnen de organisatie.

Op dit moment is een privacy beleid niet verplicht. Dit wordt anders na inwerkingtreding van de verordening. De verantwoordelijke wordt verplicht een actief passend beleid vast te stellen en dient hierbij aantoonbare technische en organisatorische maatregelen uit te voeren om ervoor te zorgen en op een transparante manier te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Hierbij wordt rekening gehouden met de stand van techniek, het soort verwerking van persoonsgegevens, de context, de omvang en het doel van de verwerking, de risico's voor de rechten en vrijheden van betrokkenen en het type organisatie, zowel bij de vaststelling van de middelen voor de verwerking als bij de verwerking zelf.[85] *Dit beleid moet transparant zijn en toegankelijk voor iedereen.*

Medewerkers van Canon zijn op dit moment vaak niet bewust van het feit dat zij persoonsgegevens verwerken. Ook zijn zij vaak niet bekend met de Wbp. Zij weten daarom niet wat wel en wat niet is toegestaan.

De overige veranderingen die de AVG met zich meebrengt komt aan de orde in het volgende hoofdstuk.

[85] Artikel 22 lid 1 AVG.

3 Algemene verordening gegevensbescherming

De richtlijn waarop de Wbp is gebaseerd stamt uit 1995. Door de snelle technologische ontwikkelingen zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De Europese Commissie presenteerde daarom in 2012 de AVG die Wbp gaat vervangen. Eenmaal aangenomen zal dit verstrekkende gevolgen hebben. Wat de AVG precies inhoudt en welke gevolgen dit heeft voor Canon komt in dit hoofdstuk aan de orde.

3.1 AVG

De Europese Commissie heeft op 25 januari 2012 een omvangrijk wetgevingspakket ingediend: het nieuwe gegevensbeschermingsrecht. Het pakket bestaat uit een Algemene verordening gegevensbescherming[86], richtlijn bescherming persoonsgegevens opsporing en vervolging[87], een overkoepelende mededeling van de commissie[88] en enkele bijlagen[89]. Dit pakket moet het geldende EU-recht voor gegevensbescherming gaan vervangen.[90] Het voorstel voor de verordening is op 12 maart 2014 door het Europees Parlement met een grote meerderheid van de stemmen aangenomen. Naar verwachting zal de AVG in de loop van 2016 in werking treden. De wetgeving wordt ingrijpend gewijzigd. Omdat de AVG direct van toepassing is in alle lidstaten zorgt dit voor één samenhangend rechtskader. Lidstaten krijgen tijdens een implementatietermijn van 2 jaar de tijd om volledig aan de wet te voldoen, nadat deze in werking is getreden. De Wbp is op dat moment niet meer leidend in Nederland en de regels voor het verwerken van persoonsgegevens veranderen hierdoor volledig.

Uitgaande van de voorgestelde tekst van COM (2012)/0011 definitief[91], worden de belangrijkste veranderingen in de volgende paragrafen beschreven en wordt toegelicht welke gevolgen dit heeft voor Canon ten aanzien van de gegevensverwerking bij de uitvoering van de dienstverlening.

3.2 Toepassing verordening

De verordening is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen.

3.3 Privacy by Design en Privacy by Default

Zoals in paragraaf 2.4 al aan de orde kwam, dient de verantwoordelijke op grond van de Wbp passende technische en organisatorische beheersmaatregelen te nemen. Dit blijft bestaan maar de AVG voegt hieraan iets toe. Op grond van de AVG dient de verantwoordelijke namelijk te zorgen dat is voldaan aan de beginselen van “Privacy by Design en Privacy by Default” bij zowel het ontwerpen als bij het uitvoeren van deze passende technische en organisatorische maatregelen.[92] Privacy by Design en Privacy by Default waren al niet- gecodificeerde principes van gegevensbescherming, maar dit wordt op grond van de AVG expliciet verplicht.

---

[86] COM (2012) 11 def.
[87] COM (2012) 10 def.
[88] COM (2012) 9 def.
[89] Het betreft een impact assessment en een afzonderlijke samenvatting van dat stuk, SEC (2012)73, respectievelijk SEC (2012)72
[90] J.P. de Jong *De Algemene verordening gegevensbescherming, de rechtsopvolger van de Wbp*, RegelMaat 2015 (30) 1
[91] En de tekst met de daarbij behorende amendementen die is aangenomen op 12 maart 2014.
[92] Artikel 23 AVG.

Deze begrippen houden in dat de verantwoordelijke of bewerker[93] zowel bij de vaststelling van de doeleinden en de middelen van de verwerking als bij de eigenlijke verwerking, zodanig passende maatregelen ten uitvoer leggen, zodat de verwerking aan de voorwaarden van de AVG voldoet. Tevens moeten deze maatregelen de rechten van de betrokkenen waarborgen.

Het komt er bij Privacy by Design op neer dat gedurende de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, rekening wordt gehouden met de privacyaspecten. Gegevensbescherming moet worden ingebouwd van het allereerste ontwerpstadion tot aan de feitelijke uitrol, het gebruik en de uiteindelijke vernietiging daarvan. De essentie van Privacy by Design is het onderkennen van privacyaspecten in alle handelingen.[94] Hierbij moet stelselmatig aandacht worden besteed aan allesomvattende procedurele waarborgen met betrekking tot de nauwkeurigheid, de vertrouwelijkheid, de integriteit, de fysieke veiligheid en de verwijdering van persoonsgegevens.[95] Ann Cavoukian[96] heeft 7 fundamentele principes geïntroduceerd die invulling geven aan de gedachtegang van Privacy by Design. In bijlage IV zijn deze 7 principes met de daarbij behorende toelichting weergegeven.

Privacy by Default heeft een andere dimensie dan Privacy by Design.[97] Bij Privacy by Default ligt de nadruk op de waarborging van privacy door middel van systeeminstellingen en dat dit voor zover mogelijk door het systeem wordt afgedwongen.[98] Gegevensminimalisering en beperking van de doeleinden is hierbij ook van belang.

Wat betekent dit voor Canon?

Canon dient bij het selecteren van haar maatregelen om persoonsgegevens te beveiligen rekening te houden met de principes van Privacy by Design en Privacy bij default. Canon dient dus tijdens de gehele levenscyclus van de diensten die zij verleent, een bedrijfsproces wat zij verzorgt of een informatiesysteem dat zij toepast bij de dienstverlening rekening te houden met de privacyaspecten. Al bij de beginfase van het installeren en aanbrengen van print- en documentsystemen bij de opdrachtgever moet Canon rekening houden met de privacyaspecten.
Ook bij de ontwikkeling van nieuwe producten en diensten dient Canon al in een vroegtijdig stadium na te denken over de bescherming van persoonsgegevens. Hierbij kan Canon gebruik maken van de 7 fundamentele principes.

Ten aanzien van Privacy by Default moet rekening gehouden worden met de waarborging van privacy bij systeeminstellingen. Dit betekent dat deugdelijke virusscanners, firewalls aangebracht worden in de systemen om bijvoorbeeld hacken te voorkomen. Ook dient de opdrachtgever bescherming aan te brengen in het netwerk waarop de printer is aangesloten. Afspraken hierover moeten worden vastgelegd in de bewerkersovereenkomst.

Deze principes moeten niet alleen worden toegepast bij nieuwe dienstverlening, maar deze principes moeten ook bij de huidige dienstverlening in acht worden genomen. Canon dient na te denken over de bescherming van persoonsgegevens bij gebruik van verouderde printers die achter lopen op de huidige stand van techniek en bij niet-standaard dienstverlening. Een PIA kan ook nuttig zijn bij het bepalen van eventuele

---

[93] De Nederlandse vertaling van de verordening gebruikt de term ‘verwerker’ in plaats van ‘bewerker’. In deze scriptie wordt de term ‘bewerker’ gehanteerd om verwarring te voorkomen.
[94] M. Veltman MMO*, Privacy by Design en Privacy by Default (PbD*2)*, Duthler associates, p. 56.
[95] Artikel 23 lid 1 AVG.
[96] Ann Cavoukian is Information & Privacy Commissioner in Canada en heeft een website gemaakt gericht op privacy by Design <www.privacybydesign.ca>.
[97] M. Veltman MMO, *Privacy by Design en Privacy by Default (PbD*2)*, Duthler associates, p. 58.
[98] A.W. Duthler, A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.

nieuwe beschermingsmaatregelen. Meer over de PIA is te lezen in de volgende paragraaf.

3.4 Privacy Impact Assessment

Wanneer persoonsgegevens worden verwerkt moeten risico's met betrekking tot de rechten en vrijheden van betrokkenen, met name het recht op bescherming van persoonsgegevens, in het oog worden gehouden.[99] De verantwoordelijke of de bewerker voert een risicoanalyse uit van de mogelijke effecten van de gegevensverwerking. In een aantal gevallen wordt een privacyeffectenbeoordeling, of wel een PIA verplicht. Een PIA is een instrument om de risico's met de betrekking tot de privacy bloot te leggen. De mogelijke gevolgen van het gebruik van persoonsgegevens voor de betrokkenen worden opgesomd en de risico's worden bepaald.
Een PIA wordt onder andere verplicht bij de verwerking van persoonsgegevens van meer dan 5000 betrokkenen gedurende een achtereenvolgende periode van 12 maanden of indien een inbreuk in verband met persoonsgegevens waarschijnlijk negatieve gevolgen heeft voor de bescherming van persoonsgegevens van de betrokkene.[100] De AVG geeft hierbij aan dat een enkele beoordeling voldoende is in het geval van een reeks vergelijkbare verwerkingen die vergelijkbare risico's inhouden.[101]

3.4.1 Resultaten PIA

Bij het uitvoeren van een PIA worden de beoogde verwerkingen op de bescherming van persoonsgegevens onderzocht en beoordeeld. Het draagt bij aan het vermijden en/of verminderen van deze privacyrisico's. Op basis van de resultaten van de PIA wordt duidelijk gemaakt of er een kans is dat de privacy van betrokkenen wordt aangetast, hoe hoog deze kans is en op welke gebieden dat is.[102] De beoordeling heeft betrekking op de gehele levenscyclus van persoonsgegevens. De FG in de organisatie wordt betrokken bij de uitvoering van de PIA.[103]

Wat betekent dit voor Canon?

Canon verwerkt in totaal van meer dan 5000 betrokkenen persoonsgegevens in één jaar bij verschillende soorten dienstverlening. Het wordt dus verplicht voor Canon om bij bepaalde vormen van dienstverlening PIA's uit te voeren. Niet bij iedere overeenkomst c.q. opdrachtgever afzonderlijk, is het uitvoeren van een PIA noodzakelijk. Wanneer die dienstverlening bij meerdere opdrachtgevers wordt gebruikt, is een enkele beoordeling voldoende om de risico's in kaart te brengen. PIA's worden uitgevoerd bij nieuwe systemen, specifieke vormen van dienstverlening of geheel nieuwe vormen van dienstverlening. Voorbeelden van dienstverlening waarbij het uitvoeren van een PIA aan te raden is, is de dienstverlening die Canon uitvoert bij de Nationale Politie, financiële instellingen, ziekenhuizen of voetbalstadions. Canon verwerkt hierbij gevoelige informatie zoals camerabeelden, gegevens over de economische situatie of gezondheid van personen. Het in kaart brengen van de risico's is hierbij essentieel.

Hierbij worden privacyrisico's vroegtijdig in kaart gebracht. De resultaten die hieruit voortkomen, kan Canon gebruiken om de dienstverlening aan te passen of noodzakelijke privacybeschermende maatregelen door te voeren in de technologie. Een FG moet betrokken worden bij de uitvoering van de PIA. Ook kan deze bepalen bij welke dienstverlening een PIA wel en niet wordt uitgevoerd. Meer over de taken van de FG in paragraaf 3.8.

---

[99] Artikel 32 bis lid 1 jo artikel 33 AVG.
[100] Zie artikel 32 bis lid 2 onder a en c AVG.
[101] Artikel 33 lid 1 AVG.
[102] NOREA - de beroepsorganisatie voor IT-auditors, *Privacy Impact Assessment: introductie, handleiding en vragenlijst*, <www.norea.nl>
[103] Artikel 33 lid 3 bis AVG.

3.5 Rol van bewerker en verantwoordelijke

In de AVG wordt een apart hoofdstuk gewijd aan de rollen van verantwoordelijke en bewerker. Er is onder meer verduidelijking over deze rolverdeling. Een bewerker die niet uitsluitend op instructie van de verantwoordelijke handelt, wordt als een (gezamenlijke) verantwoordelijke beschouwd in plaats van als bewerker.

3.5.1 Verplichtingen bewerker

De AVG legt een aantal verplichtingen op aan de bewerker.[104] Zo moet de bewerker adequate beveiligingsmaatregelen nemen[105] en een geheimhoudingsplicht opleggen aan zijn personeel.[106] Op grond van de huidige wetgeving worden deze verplichtingen in een bewerkersovereenkomst vastgelegd onder verantwoordelijkheid van de verantwoordelijke. Naleving is hierdoor een privaatrechtelijke aangelegenheid. Bij overtreding van de verplichtingen uit de AVG kan aan de bewerker dezelfde hoge boetes[107] als de verantwoordelijke, worden opgelegd.

> ***Wat betekent dit voor Canon?***
> *Canon wordt vaak aangemerkt als bewerker. Wanneer de AVG intreedt, krijgt de bewerker meer wettelijke verantwoordelijkheden. De overtreding van verplichting tot het nemen van adequate beveiligingsmaatregelen en de geheimhoudingsplicht is onder de huidige wetgeving privaatrechtelijk van aard. Wanneer de AVG van kracht is, is dit een wettelijke overtreding. De hoge boetes ten aanzien van deze overtredingen gelden dan niet alleen voor de verantwoordelijke, maar daarentegen ook voor bewerker.*

3.7 Rechten van betrokkenen

De rechten van betrokkenen worden uitgebreider. De rechten van betrokkenen uit de Wbp, zie paragraaf 2.7, gelden ook in de AVG. Deze rechten worden echter versterkt. Zo wordt het huidige recht van correctie uitgebreid met het ‘recht om wissen’[108].

3.7.1 Recht om te wissen

Een van de centrale onderdelen van de verordening is het recht om te wissen. In beginsel werd dit in de AVG het ‘recht om vergeten te worden’ genoemd, maar dit is later gewijzigd naar het ‘recht om te wissen’.

Het recht om te wissen is een nadere uitwerking en invulling van huidige recht van correctie. De betrokkene krijgt het recht om te vragen dat de op hem betreffende gegevens worden gewist die openbaar zijn gemaakt en de verdere verspreiding van dergelijke gegevens achterwege blijft. Dit verzoek geldt voornamelijk wanneer:

- Gegevens niet langer noodzakelijk zijn in verband met de doeleinden waarvoor ze werden verzameld of verwerkt;
- De betrokkene zijn toestemming intrekt;
- De betrokkene bezwaar maakt tegen de verwerking van de gegevens;
- Een rechtbank of regelgevende instantie in de Europese Unie de rechtsgeldige uitspraak heeft gedaan dat de betreffende gegevens moeten worden gewist;
- De gegevens onrechtmatig zijn verwerkt. [109]

Deze verplichting houdt in dat verdere verspreiding van de gegevens niet meer is toegestaan. De verantwoordelijke is verplicht om alle redelijke maatregelen te nemen - waaronder technische maatregelen - om (sub)bewerkers die de gegevens verwerken ervan

---

[104] Artikel 26 AVG.
[105] Artikel 26 lid 2 sub c AVG.
[106] Artikel 26 lid 2 sub b AVG.
[107] Een geldboete van € 1.000.000 of 5% van de jaarlijkse omzet
[108] Artikel 17 AVG. In het COM(2012)11 def. staat nog ‘het recht om vergeten te worden’. In het aangenomen stuk is dit gewijzigd (amendement) naar ‘het recht om te wissen’, zie artikel 17 AVG (amendement).
[109] Artikel 17 lid 1 AVG.

op de hoogte te stellen dat een betrokkene hen verzoekt iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.[110] Dit heeft al voor veel discussie gezorgd omdat het te moeilijk zou zijn om aan dit recht te voldoen in de tijd waar technologie een belangrijke rol speelt. Het werd zelfs een utopie genoemd.[111]
De bepaling laat wel ruimte voor uitzonderingen. De gegevens moeten bijvoorbeeld worden bewaard wanneer dit nodig is om het recht op vrijheid van meningsuiting uit te oefenen of omdat redenen van algemeen belang op het gebied van de volksgezondheid dit vereisen.[112]

Het recht om vergeten te worden, zoals het toen nog werd genoemd, heeft al veel stof doen opwaaien. In mei 2014 deed het Europees hof een belangrijke uitspraak in dit kader. In het Costeja-arrest[113] erkent een Europese rechtbank het 'recht om vergeten te worden' onder het huidige recht. Het ging hierbij om een Spaanse man die een zaak aanspande tegen de grote online zoekmachine Google. Wanneer de man zijn naam in de zoekmachine invoerde, weergaf de zoekmachine meteen de koppeling naar een krantenartikel uit 1998, waaruit bleek dat de man destijds in de schulden zat. Zijn schulden had hij al meerdere jaren volledig afbetaald en de vermelding ervan had dus volgens hem elke relevantie verloren. Daarnaast schond het zijn reputatie. Google was het hier niet mee eens en stelde dat het artikel rechtmatig was gepubliceerd. Uiteindelijk oordeelde het Europese Hof dat koppelingen en informatie uit de resultatenlijst van de zoekmachine verwijderd dienen te worden wanneer deze gegevens ontoereikend, niet of niet meer ter zake dienend of bovenmatig zijn ten aanzien van het doel waarvoor zij zijn verwerkt en de verstreken tijd. Dit arrest zorgde voor veel discussie met name voor de relatie tussen het recht op vrijheid van meningsuiting, informatievrijheid en het recht op privacy.

Wat betekent dit voor Canon?

Het recht om te wissen is vooral belangrijk bij persoonsgegevens die te zien zijn op openbare websites of als resultaat worden weergegeven bij een zoekmachine zoals Google. Betrokkenen vanuit heel Europa dienden massaal 'verzoeken om vergeten te worden' in bij Google na het bovenstaande Costeja-arrest. Sinds mei 2014 kwamen er 15.028 verzoeken alleen al vanuit Nederland binnen.[114] Google heeft daarom specifieke procedures ingericht hoe met deze verzoeken wordt omgegaan.
Canon maakt nooit (bewust) persoonsgegevens openbaar bij de dienstverlening en verspreidt deze gegevens ook niet. Canon zal daarom niet snel te maken krijgen met dit soort verzoeken.
Wanneer het toch voorkomt dat een betrokkene van mening is dat de op hem betreffende gegevens moeten worden gewist en de verdere verspreiding achterwege moet blijven, moet (de opdrachtgever van) Canon wel aan dit verzoek kunnen voldoen. Een verzoek moet afzonderlijk worden behandeld waarbij een belangenafweging wordt gemaakt. Wanneer het verzoek wordt gehonoreerd door Canon (of de opdrachtgever) dient Canon (samen met de opdrachtgever) ervoor te zorgen dat iedere koppeling naar, of kopie of reproductie van die persoonsgegevens wordt gewist. Aangezien zulke verzoeken incidenteel zullen voorkomen, is het inrichten van een specifieke procedure zoals bij Google overbodig.

Op dit moment is het de vraag of Canon aan 'het recht om vergeten te worden' kan voldoen, in verband met back-ups. Het inrichten van de systemen hierop is dus noodzakelijk.

---

[110] Artikel 17 lid 2 AVG.
[111] Zoals in het artikel wordt geschreven op de site van advocaten- en notariaskantoor Ploum Lodder Princen, <http://www.ploum.nl/doc/The-right-to-be-forgotten.--Een-utopie>
[112] Artikel 17 lid 2 AVG.
[113] HvJ EU 13 mei 2014 (*Google Spanje/AEPD en Costeja*)
[114] Nu.nl, 8 mei 2015 <http://www.nu.nl/internet/4045474/nederlanders-verzoeken-google-relatief-vaak-paginas-verwijderen.html>

Omdat de rechten van betrokkenen worden versterkt en omdat dit recht uitgebreid in het nieuws is geweest, zijn betrokkenen zich mogelijk meer bewust van hun rechten. Dit betekent waarschijnlijk ook dat zij sneller verzoeken zullen indienen bij bedrijven om hun gegevens op te vragen en eventueel te wissen of aan te vullen. In de toekomst zal Canon mogelijk daarom met (meer) verzoeken te maken krijgen.

3.8 Functionaris voor de gegevensbescherming

De mogelijkheid tot het aanstellen van een FG bestaat al bij de Wbp (zie paragraaf 2.9.2). De positie en het takenpakket van de FG worden versterkt met de komst van de AVG. Wanneer de AVG van kracht is, is de aanstelling van een FG verplicht voor overheidsinstanties, voor ondernemingen die betrekking heeft op meer dan 5000 betrokkenen gedurende een achtereenvolgende periode van 12 maanden, organisaties die hoofdzakelijk zijn belast met verwerkingen die regelmatige en stelselmatige observatie van betrokkenen vereisen of de kernactiviteiten van de verantwoordelijke of bewerker bestaat uit verwerkingen van bijzondere categorieën.[115] Wanneer dit niet gebeurd, kan dit worden bestraft met een boete van €1 miljoen.[116]

3.8.1 Taken FG

Volgens de AVG wordt de FG aangewezen op grond van zijn professionele kwaliteiten, en in het bijzonder zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 37 bedoelde taken te vervullen.[117] In dat artikel staan de taken die de FG ten minste op zich neemt. Dit betreft onder andere het informeren en adviseren van de verplichtingen op grond van de verordening en het documenteren van deze activiteiten en de ontvangen antwoorden. Ook ziet de FG toe op de uitvoering en de toepassing van het privacy beleid en het toezicht op de uitvoering van de toepassing van de AVG, zoals de vereisten van privacy by design, privacy by default en het informeren van betrokkenen en hun verzoeken.[118] Dit betekent dat de FG niet alleen dient te beschikken over de juridische deskundigheid, maar hij dient ook verstand te hebben van ICT en informatiebeveiliging. De FG moet vakinhoudelijke kennis en ervaring hebben. Bovendien moet hij de compliance rol vervullen. Hij moet dus toe zien op de (nieuwe) privacywet- en regelgeving binnen de organisatie. De FG kan de organisatie voorbereiden op de AVG. Daarnaast heeft de FG een dubbelrol als adviseur en toezichthouder, hierbij dient hij dus ook over bijzondere persoonlijke kwaliteiten te beschikken.[119] De FG moet met name worden geraadpleegd voordat systemen voor de geautomatiseerde verwerking van persoonsgegevens worden ontworpen, aangekocht, ontwikkeld en opgezet, om de beginselen van privacy by design en privacy by default te kunnen naleven.[120] Kortom, het takenpakket van de FG wordt erg uitgebreid.

3.8.2 Positie FG

De positie van de FG wordt beschreven in de AVG. Hierin staat onder andere dat de verantwoordelijke ervoor zorgt dat de FG zijn plichten en taken onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitvoering van zijn functie. De FG brengt rechtstreeks verslag uit aan de directie. Hieruit blijkt de toezichthoudende rol van de FG.

3.8.3 Intern of extern?

De FG hoeft niet in dienst te zijn bij de organisatie. Een FG kan ook een externe zijn en zijn taken verrichten op grond van een dienstverleningscontract. Een FG wordt aangewezen voor een periode van ten minste vier jaar in het geval van een werknemer of twee jaar in het geval

---

[115] Artikel 35 aangenomen verordening. In het eerste voorstel van de verordening werd het niet afhankelijk gesteld van het aantal gegevens dat werd verwerkt maar van het aantal medewerkers (minimaal 250) dat het bedrijf in dienst had.
[116] Artikel 79 lid 5 AVG.
[117] Artikel 35 lid 5 AVG.
[118] Artikel 37 lid 1 AVG.
[119] Mr. P.L. Coté, *De functionaris voor de gegevensbescherming: een schaap met vijf poten*, Duthler associates, p. 30.
[120] Amendement 49 AVG.

van een externe dienstencontractant. De FG kan worden herbenoemd. Tijdens zijn ambtstermijn heeft de FG een ontslagbescherming: hij kan alleen worden ontslagen wanneer hij niet langer voldoet aan de voorwaarden voor de uitvoering van zijn taken.[121] Of een FG nu in dienst is van de verantwoordelijke of niet en of hij deze opdracht nu voltijds uitvoert of niet, ze dient de FG te genieten van speciale bescherming tegen ontslag. De uiteindelijke verantwoordelijkheid moet bij de leiding van de organisatie blijven berusten.[122]

Wat betekent dit voor Canon?

Canon in Nederland verwerkt meer dan 5000 gegevens van betrokkenen gedurende een achtereenvolgende periode van 12 maanden bij de uitvoering van haar dienstverlening. Op grond van de AVG wordt het dus verplicht voor Canon om een FG aan te stellen. Een FG kan Canon klaarstomen ten aanzien van de gehele toekomstige privacywetgeving. Daarnaast kan de FG Canon helpen met het opstellen van het privacy beleid. Ook kan een FG bepalen of, wanneer en hoe een PIA uitgevoerd moet worden bij (grote) projecten.

Een FG moeten worden geselecteerd en aangesteld. Canon dient de onafhankelijkheid van FG te waarborgen. De AVG heeft hier al in bepaalde mate rekening mee gehouden door hem ontslagbescherming te geven. Daarnaast nadenken óf hij onder gezag van een manager staat, zo ja, onder wie?
Een medewerker kan niet zomaar worden aangesteld als FG, aangezien de uitgebreide kwaliteiten die een FG moet bezitten. De AVG geeft als mogelijkheid om een FG extern aan te stellen op grond van een dienstverleningscontract.

De FG moet ook rekening houden met de (interne) privacyregelgeving binnen Canon Europa. Hij moet de contacten behouden met Canon Europa en de mogelijke andere FG's in Europa. Zij kunnen samenwerken zodat de gehele privacywetgeving wordt gewaarborgd in alle business units.

3.9 Doorgifte naar derde landen

Volgens de AVG mag doorgifte plaatsvinden indien de Europese Commissie heeft besloten dat een 'passend beschermingsniveau' bestaat[123], passende garanties worden geboden voor de doorgifte[124], doorgifte wordt gebaseerd op BCR of een beroep kan worden gedaan op een uitzonderingsbepaling.[125] Deze mogelijkheden zijn niet nieuw. Deze mogelijkheden bestaan ook al onder het huidige recht. Al wordt de mogelijkheid om BCR te gebruiken nu wettelijk vastgelegd. Ook worden de bepalingen uitgebreid en wat onderdelen toegevoegd.

3.9.1 Besluit van een passend beschermingsniveau

Zoals in paragraaf 1.8.1 al werd beschreven, kan de Europese Commissie besluiten of een land een passend beschermingsniveau heeft. Het toepassingsbereik van dit besluit wordt uitgebreid. Deze besluiten kunnen niet langer uitsluitend ten aanzien van een derde land worden genomen, maar nu ook ten aanzien van een gebied, of een verwerkingssector in dat derde land, of de betrokken internationale organisatie.

3.9.2 Passende garanties

Een verantwoordelijke of een bewerker mag persoonsgegevens naar een derde land of internationale organisatie doorgeven indien hij in een juridisch bindend instrument (zoals een bewerkersovereenkomst) passende garanties biedt voor de bescherming van de persoonsgegevens.[126]

---

[121] Artikel 35 lid lid 7 AVG.
[122] Amendement 49 AVG.
[123] Artikel 41 AVG.
[124] Artikel 42 AVG.
[125] Artikel 44 AVG.
[126] Artikel 42 lid 1 AVG.

Deze passende garanties zijn met name:

- Bindende bedrijfsvoorschriften (BCR). Meer hierover in paragraaf 3.9.3.
- Modelbepalingen die door de Europese Commissie zijn vastgesteld.
- Modelbepalingen die door een toezichthoudende autoriteit zijn vastgesteld in het kader van de conformiteitstoetsing, wanneer die door de Commissie algemeen geldig zijn verklaard.
- Contractuele bepalingen tussen de verantwoordelijke (of de bewerker) en de ontvanger van de gegevens, die door een toezichthoudende autoriteit zijn goedgekeurd.

Deze bepalingen zijn tevens direct van toepassing op bewerkers. Zij kunnen dus zelf ook gebruik maken van deze passende garanties.

3.9.3 Binding Corporate Rules

BCR bevatten voorschriften over de wijze waarop de privacyregelgeving wordt nageleefd. In de AVG wordt een specifieke bepaling opgenomen over het instrument BCR. Hierin staat onder welke voorwaarden de BCR moeten voldoen om voor goedkeuring in aanmerking te komen.

> ***Wat betekent dit voor Canon?***
> *Omdat Canon in de bewerkersovereenkomst de doorgifte van persoonsgegevens buiten de Europese Unie uitsluit, zijn de beschermingsmaatregelen zoals hierboven omschreven overbodig.*
>
> *BCR zijn bedoeld voor multinationals. Canon is een multinational, de dienstverlening van Canon is echter op zichzelf niet gericht op doorgifte van dataverwerking aan bedrijven die zijn gevestigd in derde landen zonder passend beschermingsniveau. Het is daarom niet noodzakelijk om BCR aan te vragen.*

3.10 Sancties

De hoge boetes staan centraal in de AVG. Op grond van de AVG gelden hogere boetebepalingen bij een overtreding dan onder de huidige wetgeving. De Europese Commissie is van mening dat doeltreffende, afschrikkende sancties van groot belang zijn om de handhaving van de voorschriften te garanderen.

De sancties worden opgelegd door de toezichthouder.[127] De hoogste categorie betreft een boete van 1 miljoen euro of 5% van de wereldwijde omzet.[128] Zo kan onder andere een boete van de hoogste categorie worden opgelegd wanneer persoonsgegevens worden verwerkt zonder toereikende rechtsgrondslag[129], wanneer een intern beleid ontbreekt[130] of wanneer een organisatie de toezichthoudende autoriteit niet waarschuwt bij een datalek.[131]

> ***Wat betekent dit voor Canon?***
> *Wanneer Canon zich niet houdt aan de verplichtingen kunnen hoge boetes worden opgelegd.*
>
> *Considerati is een juridisch advieskantoor dat adviseert over alle aspecten van privacy compliance. De privacychecker[132] is een initiatief van Considerati en is*

[127] Artikel 79 lid 1 AVG.
[128] Artikel 79 lid 6 AVG. In COM(2012)/11 def. staat in dit artikel dat de maximale boete 2% van de wereldwijde jaarlijkse omzet betreft. Op een aantal (kleine) punten is dit voorstel gewijzigd, waaronder deze verhoging naar 5%. Dit gewijzigde voorstel is aangenomen door het Europees Parlement.
[129] Artikel 79 lid 6 sub a AVG.
[130] Artikel 79 lid 6 sub e AVG.
[131] Artikel 79 lid 6 sub h AVG.
[132] De Privacychecker, geeft een inzicht in het privacy beleid voor organisaties <www.privacychecker.nl>

bedoeld om een inzicht in het privacybeleid van bedrijven te geven. De boetemeter is een onderdeel van de privacychecker. Door het invullen van een aantal vragen over het privacybeleid van het bedrijf geeft deze aan wat de potentiële boete bedraagt. Wanneer Canon niets doet aan het privacy beleid, riskeert Canon onder de toekomstige privacywetgeving een boete van maximaal €6.500.000.000 volgens de privacychecker. In bijlage IV is het rapport van de boetemeter toegevoegd. Dit is echter een grove indicatie van een potentiële boete en is bedoeld om weer te geven dat een goede voorbereiding op de nieuwe wetgeving noodzakelijk is.

Om vooruit te lopen op de AVG, wordt in Nederland de boetebevoegdheid van het CBP uitgebreid. De gevolgen hiervan voor Canon worden in het volgende hoofdstuk toegelicht.

3.11 Meldplicht datalekken

De AVG voert een meldplicht datalekken in. In geval van een inbreuk van de persoonsgegevens meldt de verantwoordelijke aan de toezichthoudende autoriteit de inbreuk zonder onnodige vertraging, zo mogelijk niet later dan 24 uur na kennisname.[133]
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk negatieve gevolgen heeft voor de betrokkene, meldt de verantwoordelijke de inbreuk ook aan de betrokkene.[134]
De verantwoordelijke documenteert daarbij alle inbreuken, met inbegrip van de feiten omtrent de inbreuk, de gevolgen van de inbreuk en de corrigerende maatregelen die zijn genomen.[135]

Wat betekent dit voor Canon?

Om vooruit te lopen op de AVG, wordt in Nederland al een meldplicht datalekken ingevoerd. De gevolgen hiervan voor Canon worden daarom in het volgende hoofdstuk toegelicht.

[133] Artikel 31 lid 1 AVG.
[134] Artikel 32 lid 1 AVG.
[135] Artikel 31 lid 4 AVG.

4 Meldplicht datalekken en uitbreiding boetebevoegdheid

De AVG zal in 2016 in werking treden. Hierin wordt een meldplicht datalekken geïntroduceerd en wordt de bevoegdheid om boetes uit te delen door de toezichthouder uitgebreid. Om vooruit te lopen op deze Europese ontwikkelingen is in Nederland in 2012 het wetsvoorstel meldplicht datalekken ingediend.[136] Daarna[137] is dit wetsvoorstel aangevuld met een uitbreiding van de bestuurlijke boetebevoegdheid voor het CBP.[138] Het wetsvoorstel is op 10 februari 2015 aangenomen. Naar verwachting zal deze wet op 1 juli 2015 van kracht zijn. Met de invoering van de nationale meldplicht voor datalekken en de uitbreiding van de bestuurlijke boetebevoegdheid van het CBP wordt beoogd toe te groeien naar de nieuwe EU-verordening. Wat de Meldplicht en de uitbreiding boetebevoegdheid inhoudt en welke gevolgen dit heeft voor Canon wordt in dit hoofdstuk toegelicht.

4.1 Aanleiding

Op dit moment geldt al een aantal vergelijkbare meldplichten in Nederland voor een inbreuk op de beveiliging van persoonsgegevens. Zo geldt er een meldplicht die is gericht op openbare elektronische communicatiediensten. Deze meldplicht is opgenomen in de Telecommunicatiewet.[139] Deze meldplicht wordt in deze wetswijziging aangevuld met een meldplicht voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector.[140] Het doel van deze meldplicht is om voor alle bedrijven de beveiliging van informatie, in het bijzonder de beveiliging van persoonsgegevens, op orde te brengen. Tevens biedt de verantwoordelijke zo transparantie over de verwerkingen van de persoonsgegevens.

Naast de meldplicht wordt met deze wetswijziging uitvoering gegeven aan het regeerakkoord van het kabinet-Rutte II “Bruggen slaan” van 29 oktober 2012.[141] In dit regeerakkoord werd al bepleit voor een uitbreiding van de bevoegdheden van het CBP. Met de versterking ofwel uitbreiding van de sanctiemogelijkheden in de Meldplicht datalekken en uitbreiding boetebevoegdheid wordt beoogt de naleving van de Wbp te bevorderen.

4.2 Meldplicht datalekken

De meldplicht datalekken werd naar aanleiding van een groot aantal incidenten waarbij door een inbreuk van de beveiliging van, onder meer, websites persoonsgegevens vrijkwamen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen.[142]
De meldplicht houdt in dat de verantwoordelijke bij een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens, een melding maakt bij de toezichthouder. De toezichthouder is het CBP.[143]

---

[136] Kamerstukken II 2012/13, 33662, nr. 3, p. 1 (MvT).
[137] Op 24 november had staatssecretaris Teeven een tweede nota van wijziging ingediend bij het wetsvoorstel 33662 (Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP).
[138] Kamerstukken II 2012/13, 33662 (tweede nota van wijziging).
[139] Artikel 11.3a Telecommunicatiewet.
[140] Kamerstukken II 2012/13, 33662, nr. 3, p. 7 (MvT).
[141] Kamerstukken II 2012/13, 33662 (tweede nota van wijziging).
[142] Kamerstukken II 2012/13, 33662, nr. 3, p. 1 (MvT).
[143] Het Cbp zal na de inwerkingtreding als ‘Autoriteit Persoonsgegevens’ worden aangeduid om aan te sluiten bij de terminologie van de Europese ontwikkelingen. Dit maakt tegelijkertijd een einde aan de verwarring met het Centraal Planbureau (CPB). Zie artikel 51 lid 4 Wbp (nieuw).

4.2.1 Wanneer wordt een datalek gemeld?

Niet iedere datalek behoeft te worden gemeld. Wanneer iedere datalek wordt gemeld, zou dit leiden tot onnodige belasting van het bedrijfsleven en de overheid. Alleen de inbreuken waarvan 'redelijkerwijs' kan worden aangenomen dat die leiden tot een 'aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens' worden gemeld.

De meldplicht staat in nauw verband met de beveiligingsverplichting van artikel 13 van de Wbp. Die bepaling verplicht de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Van een onder de meldplichtbepaling vallend datalek is pas sprake, wanneer de technische en organisatorische maatregelen niet hebben gefunctioneerd en de persoonsgegevens zijn blootgesteld aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Er behoeft niet noodzakelijkerwijs sprake te zijn van tekortschietende beveiligingsmaatregelen. Van een inbreuk op de beveiliging kan ook sprake zijn indien de beveiliging van voldoende niveau is, maar de beveiligingsmaatregelen worden teniet gedaan of omzeild. De memorie van toelichting geeft hierbij als voorbeeld een hack van een ICT-systeem dat persoonsgegevens bevat of de diefstal van een laptop uit een afgesloten locker. Er zijn ook situaties denkbaar waarin de inbreuk op de beveiligingsmaatregelen wel het gevolg zijn van een tekortschietende beveiliging, die de verantwoordelijke zelf kan worden aangerekend. Hier geeft de memorie van toelichting als voorbeeld wanneer er sprake is van bestanden en/of gegevens die niet adequaat worden beveiligd of menselijke fouten van ondergeschikten.[144] Zie figuur 1 voor een schematische weergave wanneer melding van een datalek nodig is.

Er gekozen voor een risicocriterium. Dit betekent dat objectief moet worden bekeken of de inbreuk heeft geleid tot het intreden van een aannemelijk risico dat de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, nadat is vastgesteld dat sprake is van een inbreuk op de beveiliging.

Figuur 1. Wanneer is de meldplicht van toepassing? Beslismodel wanneer een datalek wordt gemeld.

De verantwoordelijke is verplicht zonder onnodige vertraging en uiterlijk binnen 24 uur nadat hij ervan kennis heeft genomen, een datalek te melden bij het CBP.

4.2.2 Wie meldt het datalek?

De meldplicht in de Wbp richt zicht tot verantwoordelijken voor de verwerking van persoonsgegevens. De verantwoordelijke heeft per slot van rekening de zorgplicht om de nodige beveiligingsmaatregelen te treffen.[145] De bewerker zal de partij zijn die daadwerkelijk belast is met het ten uitvoer leggen van deze maatregelen, maar de Wbp legt de verantwoordelijke expliciet de zorgplicht op.

De wet stelt geen instrumenten beschikbaar om meer invloed op de bewerker uit te oefenen. De memorie van toelichting geeft aan dat dit geen taak is voor de wetgever, maar dat dit een aangelegenheid is tussen verantwoordelijke en bewerker. De partijen dienen zelf hierover af spraken te maken in de bewerkersovereenkomst. De rechtsbetrekking tussen verantwoordelijke en bewerker is immers van privaatrechtelijke aard.[146]

[144] Kamerstukken II 2012/13, 33662, nr. 3, p. 3 (MvT).
[145] Op grond van artikel 13 Wbp.
[146] Kamerstukken II 2012/13, 33662, nr. 3, p. 6 (MvT).

Artikel 14 Wbp wordt gewijzigd. De verantwoordelijke draagt er zorg voor dat de bewerker ook de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van datalekken. Wanneer een bewerker is ingeschakeld, moet de bewerker onmiddellijk na vaststelling van een datalek de verantwoordelijke waarschuwen en informeren. Hieruit volgt een ketenaansprakelijkheid.

4.2.3 Aan wie wordt de datalek gemeld?

Het nieuwe artikel 34a Wbp stelt dat een verantwoordelijke onverwijld een melding moet doen bij het CBP indien een datalek plaatsvindt. Ook de betrokkenen van wie persoonsgegevens gelekt zijn, moeten op de hoogte worden gebracht. De melding aan het CBP en de betrokkene omvat in ieder geval de aard van de inbreuk, het contactpunt waar meer informatie kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.[147]

4.2.4 Logboek datalekken

De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens met betrekking tot de aard van de inbreuk en de tekst van de kennisgeving aan de betrokkene.[148]

4.2.5 Nalaten van de meldplicht

Het nalaten van het melden van een datalek kan worden gesanctioneerd met een bestuurlijke boete, op te leggen door het CBP. De boete kan oplopen tot € 810.000,- en wanneer deze geldboete geen passende bestraffing toelaat volgens het CBP, kan een geldboete worden opgelegd van ten hoogste 10% van de jaaromzet van een rechtspersoon.[149] Deze boete staat los van de mogelijkheid om door een betrokkene aansprakelijk te worden gesteld voor de geleden schade op grond van artikel 49 Wbp. De verantwoordelijke kan eventueel regres nemen op een bewerker. Een melding kan wel zorgen dat wordt voldaan aan de schadebeperkingsplicht. De kennisgeving aan de betrokkene is namelijk een uiting van de algemene verplichting tot schadebeperking.

De verantwoordelijke krijgt de taak zorg te dragen dat de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van diens meldplicht. Dit betekent dat deze verplichting in de bewerkersovereenkomst zal moeten worden opgenomen. Dit is ook noodzakelijk omdat de verantwoordelijke anders geen weet heeft van een eventueel datalek. Hij zou dan niet eens in staat zijn dit te melden.

> ***Wat betekent de meldplicht datalekken voor Canon?***
> *Met het intreden van de meldplicht datalekken dient Canon in het vervolg datalekken te melden, wanneer zij wordt aangemerkt als verantwoordelijke. De melding moet binnen 24 uur plaatsvinden. Afspraken omtrent het waarschuwen met (sub)bewerkers kunnen worden vastgelegd in een bewerkersovereenkomst.*
> *Het aanpassen bewerkersovereenkomst is daarom noodzakelijk. Afspraken omtrent datalekken moeten hierin worden vastgelegd. Canon krijgt dan de verplichting om ervoor te zorgen dat de meldplicht wordt nagekomen. Alle inbreuken moeten worden bijgehouden door Canon in een logboek.*

[147] Artikel 34a lid 3 Wbp (nieuw).
[148] Artikel 34a lid 8 Wbp (nieuw).
[149] Zie volgende paragraaf over de uitbreiding van deze boetebevoegdheid van het CBP.

4.3 Uitbreiding boetebevoegdheid CBP

Het CBP krijgt de bevoegdheid toegekend om veel hogere (bestuurlijke) boetes op te leggen bij overtredingen van de hoofdverplichtingen van de Wbp. Zoals in paragraaf 2.9.1 al aan de orde kwam, kan het CBP op dit moment uitsluitend een bestuurlijke boete opleggen in geval van een overtreding van administratieve verplichtingen. Deze boete is maximaal € 4.500,- en wordt niet vaak opgelegd. Met inwerkingtreding van de Meldplicht datalekken en uitbreiding boetebevoegdheid worden de boetes verhoogd naar maximaal € 810.000,- of 10% van de jaaromzet van een rechtspersoon. De gevallen waarin een boete kan worden opgelegd worden ook uitgebreid. Zo kan het CBP in het vervolg niet alleen bij overtredingen van administratieve verplichtingen een boete worden opgelegd maar ook bij overtreding van de materiële normen uit de wet. In bijlage V staat een overzicht van de overtredingen. Hierin is schematisch opgenomen voor welke overtredingen het CBP in het vervolg boetes uit kan delen.

4.3.1 Bindende aanwijzing

Het CBP zal echter bij een vermoeden van niet-opzettelijke overtredingen niet onmiddellijk een bestuurlijke boete opleggen maar eerst een bindende aanwijzing geven. Een bindende aanwijzing houdt een zelfstandige last in die wegens een overtreding wordt opgelegd. Deze zelfstandige last[150] is een enkele last tot het verrichten van bepaalde handelingen ter bevordering van de naleving van wettelijke voorschriften. In die aanwijzing zal het CBP aangeven welke wettelijke bepalingen zijn overtreden en hem zo mogelijk moeten opdragen wat de overtreder dient te doen om de overtreding geheel of gedeeltelijk te herstellen.[151] Hierin kan het CBP de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.[152] Indien de aanwijzing niet wordt opgevolgd, kan het CBP een bestuurlijke boete opleggen.

Als een organisatie willens en wetens ofwel opzettelijk[153] de Wbp overtreedt om hier bijvoorbeeld zelf financieel beter van te worden, kan het CBP zonder bindende aanwijzing overgaan tot oplegging van een boete.
Omdat de bindende aanwijzing een zelfstandige last is die wordt opgelegd bij besluit van de toezichthouder, kan de overtreder tegen het besluit in bezwaar (en eventueel beroep) gaan.

4.3.2 Waarom een bindende aanwijzing?

Nu het in de Wbp over het algemeen om abstracte ofwel vage normen gaat, is het ongewenst om simpelweg meteen een bestuurlijke boete op te leggen. Eventuele nadere regels, richtsnoeren van het CBP of gedragscodes kunnen dit probleem slechts deels oplossen.[154] Het gaat vaak om vaag omschreven gebeurtenissen die pas in het concrete geval in een organisatie betekenis krijgen. De bindende aanwijzing is een geschikt middel om in concrete gevallen nadere invulling te geven aan de normen van de Wbp. Het kan worden gezien als een (in beginsel) verplichte tussenstap.

Het invoeren van de bindende aanwijzing is ook in harmonie met het lex certa-beginsel. Het lex certa beginsel houdt hierbij in dat alleen boetes kunnen worden opgelegd als vooraf voldoende voorzienbaar is op welke wijze de wet had moeten worden nageleefd. Inhoudelijke eisen ten opzichte van die strafbepaling moeten worden afgeleid. Het is dus vereist dat de toezichthouder de vage wettelijke normen concretiseert en duidelijk maakt wat wordt verwacht van de verwerker van de persoonsgegevens.

Het CBP daarentegen was minder enthousiast over de invoering van de bindende aanwijzing. Dit zou niet leiden tot een betere naleving van de Wbp vond de voorzitter van het

[150] Als bedoeld in artikel 5:2 lid 2 Algemene wet bestuursrecht (hierna: Awb).
[151] Zie artikel 1 onder q en r en artikel 66 lid 3 en 4 Wbp (nieuw).
[152] Artikel 66 lid 3 Wbp (nieuw).
[153] Zie artikel 66 lid 4 Wbp (nieuw).
[154] Volgens de Afdeling, zie Kamerstukken II 2012/13, 33662 (tweede nota van wijziging), p. 17.

CBP, Jacob Kohnstamm. “De roep in de samenleving is om een waakhond met tanden,’ Aldus Kohnstamm, ‘Nu worden we tandeloos aan banden gelegd waardoor bedrijven en organisaties niet de druk zullen voelen om de wet na te leven.”[155]

4.3.3 Aan wie kan een bestuurlijke boete worden opgelegd?

Op dit moment zijn de boetes gericht aan de verantwoordelijke. Dit wordt vervangen door ‘overtreder’. Op grond van artikel 5:1 lid 2 Awb wordt onder ‘overtreder’ verstaan zowel degene die overtreding pleegt of de medepleger. In veel gevallen zal de verantwoordelijke worden aangemerkt als degene die een overtreding in de zin van de Wbp pleegt. Niet uitgesloten is, dat bijvoorbeeld de ingeschakelde (sub)bewerker als wordt medepleger aangemerkt.[156]

Wat betekent de uitbreiding van de boetebevoegdheid van het CBP voor Canon?

Wanneer Canon zich niet houdt aan de verplichtingen uit de Wbp kunnen hoge boetes worden opgelegd. Deze boetes kunnen worden opgelegd aan de overtreder (meestal de verantwoordelijke), maar ook aan de medepleger (de (sub)bewerker).

Uit eerdere zaken blijkt dat het CBP zich onder de huidige wetgeving coöperatief opstelt. Het CBP vindt het belangrijk wanneer bedrijven de intentie hebben om aan privacy wetgeving te voldoen. Het CBP komt graag met bedrijven tot een oplossing om alsnog aan de privacyaspecten te voldoen. Zo was dit ook begin dit jaar bij Facebook. Het CBP dreigde met een boete van miljoenen euro’s maar Facebook kreeg uiteindelijk nog de tijd om de overtredingen te beëindigen.[157] Ook de grote fabrikant van navigatiesystemen, Tomtom, kreeg alsnog de tijd om aan de privacywetgeving te voldoen.[158]

Het CBP gaat waarschijnlijk handhaving strikter regelen met de komst van deze wetswijziging. Het CBP kan dan hogere bestuurlijke boetes opleggen voor meer (materiele) bepalingen. Wanneer Canon niet voldoet aan de wetgeving en een boete ontvangt, zal dit leiden tot reputatieschade.

[155] www.cbpweb.nl <https://cbpweb.nl/nl/nieuws/cbp-zet-grote-vraagtekens-bij-wetsvoorstel-boetebevoegdheid>
[156] Kamerstukken II 2012/13, 33662 (tweede nota van wijziging)
[157] www.bloomberg.com <http://www.bloomberg.com/news/articles/2015-05-06/facebook-privacy-fine-threat-suspended-in-dutch-watchdog-probe>
[158] www.cbpweb.nl <https://cbpweb.nl/nl/nieuws/overtredingen-tomtom-be%C3%ABindigd-na-onderzoek-cbp>

5 Conclusies en aanbevelingen

Op basis van het uitgevoerde onderzoek kunnen een aantal conclusies worden getrokken die van belang zijn voor Canon om te voldoen aan de nieuwe privacywetgeving. Op basis van deze conclusies worden een aantal aanbevelingen gedaan aan Canon. In dit hoofdstuk worden de belangrijkste conclusies en aanbevelingen gegeven.

5.1 Conclusies

In hoofdstuk 2 is naar voren gekomen dat Canon voldoet aan de huidige Wbp. Organisaties besteden hele bedrijfsprocessen uit aan Canon. Bij het uitbesteden van deze processen is het soms onvermijdelijk om over de persoonsgegevens van de opdrachtgever te beschikken. Canon verwerkt deze persoonsgegevens omdat dit noodzakelijk is voor de uitvoering van de dienstverlening voor de opdrachtgever. Het kan bij cloud-computing moeilijk zijn vast te stellen wie welke rol vervult in het geheel en dus vast te stellen of Canon de verantwoordelijke of bewerker is. Een analyse van de soort data en de herkomst ervan is dan ook vereist om te bepalen welke schakel in het geheel aangemerkt moet worden als verantwoordelijke en (sub)bewerker. Het kan dus per situatie verschillen of Canon wordt aangemerkt als bewerker of (mede)verantwoordelijke. Wanneer Canon als (mede)verantwoordelijke wordt aangemerkt, geeft dit meer verplichtingen. Zo is verantwoordelijke eindverantwoordelijk voor de persoonsgegevens, ook als de gegevens feitelijk door (sub)bewerkers worden verwerkt. Ook heeft de verantwoordelijke de controleplicht dat de gemaakte afspraken worden nageleefd en vooral of de persoonsgegevens adequaat worden beveiligd. Bij een geschil, of een fout van de eventuele (sub)bewerker wordt de verantwoordelijke daarop aangesproken door het CBP en niet de (sub)bewerkers. Canon wordt daarom graag als bewerker aangemerkt. De opdrachtgever blijft dan eindverantwoordelijk voor de persoonsgegevens.

De AVG treedt waarschijnlijk in werking in de loop van 2016. Deze verordening heeft implementatietermijn van 2 jaar. De Meldplicht datalekken en uitbreiding boetebevoegdheid is op 26 mei 2015 aangenomen door de eerste kamer en zal omstreeks 1 januari 2016 in werking treden. Hierop dient Canon zich voor te bereiden. De AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid brengen voor Canon een aantal verplichtingen met zich mee.

Hierna wordt in hoofdlijnen aangegeven waaraan Canon zich moet houden, om te kunnen voldoen aan de toekomstige privacywetgeving.

- ***FG aanstellen***
  Een FG wordt verplicht voor Canon.

- ***Privacy beleid vaststellen***
  Het wordt voor Canon verplicht een actief passend privacy beleid vast te stellen. Hierbij dient Canon aantoonbare technische en organisatorische maatregelen te nemen om ervoor te zorgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Met het opstellen van dit beleid wordt rekening gehouden met de stand van techniek, het soort verwerking van persoonsgegevens, de context, de omvang en het doel van de verwerking, de risico's voor de rechten en vrijheden van betrokkenen en het type organisatie, zowel bij de vaststelling van de middelen voor de verwerking als bij de verwerking zelf.

- ***De begrippen Privacy by Design en Privacy by Default in acht nemen***
  De begrippen Privacy by Design en Privacy by Default dienen bij de gegevensverwerking in acht te worden genomen. Dit betekent dat Canon tijdens de gehele levenscyclus van de diensten die zij verleent, een bedrijfsproces wat zij verzorgt of een informatiesysteem dat zij toepast bij de dienstverlening rekening houden met de privacyaspecten. Ook moet een goede beveiliging in systemen worden aangebracht.

- ***Het uitvoeren van een Privacy Impact Assessment***
  In bepaalde gevallen wordt het uitvoeren van een PIA verplicht. Uitvoerige PIA's worden uitgevoerd om mogelijke bedreigingen en risico's die optreden bij de verwerking van persoonsgegevens bij verschillende soorten dienstverlening in kaart te brengen. Een PIA hangt samen met Privacy by Design. Op grond van de resultaten van de PIA kan worden bepaald hoe Privacy by Design wordt toegepast bij de informatiebeveiliging.

- ***Meldplicht datalekken***
  De meldplicht in de Wbp richt zicht tot verantwoordelijken voor de verwerking van persoonsgegevens. De verantwoordelijke dient de datalek te melden. Dus als Canon wordt aangemerkt als verantwoordelijke en een datalek wordt ontdekt, dient zij de dit te melden aan het CBP en de betrokkene(n). Alle de inbreuken waarvan 'redelijkerwijs' kan worden aangenomen dat die leiden tot een 'aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens' die door de verantwoordelijke worden verwerkt worden gemeld. Wanneer Canon dit verzuimt riskeert zij een bestuurlijke boete, op te leggen door het CBP. De boete kan oplopen tot € 810.000,- en wanneer deze geldboete geen passende bestraffing toelaat volgens het CBP, kan een geldboete worden opgelegd van ten hoogste 10% van de jaaromzet van een rechtspersoon. Deze boete staat los van de mogelijkheid om door een betrokkene aansprakelijk te worden gehouden voor de geleden schade op grond van artikel 49 Wbp. De verantwoordelijke kan eventueel regres nemen op een bewerker, als deze hiervoor (mede)aansprakelijk is. Een melding kan wel zorgen dat wordt voldaan aan de schadebeperkingsplicht. Alle inbreuken moeten tevens worden bijgehouden door Canon in een logboek.

- ***Uitbreiding boetebevoegdheid***
  Hoge boetes worden opgelegd door het CBP wanneer Canon zich niet houdt aan de verplichtingen uit de Wbp. Op grond van de huidige wetgeving kan het CBP uitsluitend een bestuurlijke boete opleggen in geval van een overtreding van administratieve verplichtingen. Deze boete is maximaal € 4.500,- en wordt zelden opgelegd. Met de inwerkingtreding van de Meldplicht datalekken en uitbreiding boetebevoegdheid kunnen de boetes kunnen oplopen tot € 810.000,- en wanneer deze geldboete geen passende bestraffing toelaat volgens het CBP, kan een geldboete worden opgelegd van ten hoogste 10% van de jaaromzet van een rechtspersoon. Een overzicht van de overtredingen staan in bijlage V. Deze boetes kunnen worden opgelegd aan de overtreder (meestal de verantwoordelijke), maar ook aan de medepleger (de (sub)bewerker). Dus of Canon wordt aangemerkt als verantwoordelijke of als bewerker maakt dat voor het opleggen van boetes niets uit. Voordat deze boete wordt opgelegd zal het CBP bij een niet-opzettelijke overtreding eerst een bindende aanwijzing moeten geven. Met de tussenstap in de vorm van een bindende aanwijzing zal Canon eerst nog de kans krijgen om de situatie te herstellen. De kans dat uiteindelijk zo'n hoge boete wordt opgelegd wordt hierdoor kleiner.

5.2 Slotconclusie

Kortom, Canon is verplicht een FG aan te stellen, een privacybeleid vast te stellen en de begrippen privacy by Design en Privacy by Default in acht te nemen. Daarnaast dient zij bij (nieuwe) dienstverlening PIA's uitvoeren. Ook moet Canon in het vervolg datalekken gaan melden en hiervan een logboek gaan bijhouden. Wanneer Canon deze maatregelen treft, voldoet zij aan de toekomstige privacywetgeving. Hierdoor worden de hoge, door het CBP op te leggen boetes voorkomen.

5.2 Aanbevelingen

Uit bovenstaande conclusies kunnen een aantal aanbevelingen worden gedaan:

- **FG**
  De belangrijkste aanbeveling is om zo spoedig mogelijk, in ieder geval nog in 2015 een FG aan te stellen. De AVG zal pas in werking treden in de loop van 2016. Het aanstellen van een FG zal dan pas een verplichting zijn. Maar afgezien van de verplichting, is een FG aan te raden bij Canon. Wanneer Canon namelijk op tijd een FG aanstelt, kan hij Canon voorbereiden op de AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid. Daarnaast zullen veel organisaties op zoek gaan naar een FG, dus het is verstandig om zo snel mogelijk te beginnen met zoeken. Aanbevolen wordt om de FG intern aan te stellen. Niet een willekeurige werknemer die al in dienst is kan worden aangesteld als een FG. Door de vele kwaliteiten die de FG moet bezitten met betrekking tot zijn wettelijke takenpakket is dit niet wenselijk. Bovendien moet hij nog worden opgeleid waar veel tijd in gaat zitten. Het aanstellen van een goed opgeleide, ervaren, deskundige FG is aanbevelingswaardig. Een fulltime aanstelling is niet overbodig, gezien het uitgebreide takenpakket en de verwerking van de hoeveelheid persoonsgegevens gedurende de verschillende soorten dienstverlening. Let wel op dat een interne FG wordt benoemd voor ten minste 4 jaar. Daarnaast heeft een FG ontslagbescherming: hij kan alleen worden ontslagen wanneer hij niet langer voldoet aan de voorwaarden voor de uitvoering van zijn taken. Een FG die bij het bedrijf past is daarom belangrijk.

- **Protocol opstellen**
  Wanneer een datalek zich voordoet, dienen de toezichthoudende autoriteiten en vaak de betrokkenen, onverwijld op de hoogte te worden gesteld. Voor het doen van deze melding is het noodzakelijk bepaalde informatie voor handen te hebben. Het is daarom aan te bevelen om een protocol op te stellen met daarin een aantal actiepunten die moeten worden genomen op het moment dat (waarschijnlijk) sprake is van een datalek. Aanbevolen wordt om hierin uitgebreid op te nemen hoe met een datalek wordt omgegaan. Ook kunnen hierin schadebeperkende maatregelen worden opgenomen voor een aantal mogelijke scenario's die plaats kunnen vinden. Tevens staat hierin aangegeven wie als aanspreekpunt geldt. De FG kan dit protocol opstellen en beslissingen hierover nemen. Dit protocol zorgt ervoor dat het lek tijdig kan worden gemeld.

- **Aanpassen bewerkersovereenkomst**
  Aanbevolen wordt om op een aantal zaken te letten wanneer een bewerkersovereenkomst wordt gesloten:

  - Ter voorkoming van onduidelijkheden is het verstandig om uitdrukkelijk vast te leggen in een bewerkersovereenkomst wie verantwoordelijke en (sub)bewerker is.

  - Afspraken maken omtrent worden hoe partijen omgaan met een datalek. Verantwoordelijke is verantwoordelijk en aansprakelijk voor het adequaat afwerken van datalekken. De verantwoordelijke krijgt de taak zorg te dragen dat

de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van diens meldplicht.

De FG kan de standaard bewerkersovereenkomst aanpassen zodat deze volledig voldoet aan de wetgeving per 1 januari 2016.

- **Voorkomen van boetes**
  Aanbevolen wordt om de beveiligingsmaatregelen kritisch te bekijken en zo mogelijk deze aan te passen zodat het beschermingsniveau van de persoonsgegevens optimaal zijn. Wanneer het beschermingsniveau van hoog niveau is, kunnen boetes worden voorkomen. Aan te raden is om de FG bij dit proces te betrekken. De huidige privacyaspecten kunnen worden bekeken door de FG. De FG kan de nulsituatie vaststellen en aan de hand daarvan kan hij de te nemen maatregelen bepalen.

- **Privacy beleid en bewustwording medewerkers**
  Aanbevolen wordt om zo spoedig mogelijk te beginnen met het opstellen van het privacybeleid. Het is aan te raden om dit beleid zo helder en transparant mogelijk te formuleren. Vage begrippen en normen moeten worden vermeden. Medewerkers van Canon dienen dit beleid volledig te begrijpen. Zij moeten immers de uitgangspunten hiervan kennen en in lijn met dit beleid hun werkzaamheden gaan uitvoeren. Zij dienen goed voor ogen te hebben wat het privacybeleid is en wat wel en niet is toegestaan met de persoonsgegevens.

  Het is belangrijk dat medewerkers zich bewust worden van het feit dat gewerkt wordt met (gevoelige) persoonsgegevens en een zorgvuldige omgang met persoonsgegevens vereist is. Dit bewustzijn kan worden gecreëerd door middel van privacy-trainingen/voorlichtingen. Deze trainingen en voorlichtingen kunnen door de FG worden georganiseerd.

- **Privacy by design en Privacy by Default en de PIA**
  Canon dient verantwoordelijkheid te nemen voor de naleving van de principes Privacy by Design en Privacy by Default. Aanbevolen wordt om hierbij de 7 principes in acht te nemen. In bijlage III staat een uitleg van deze principes. Daarnaast wordt aanbevolen bij het toepassen van Privacy by Design PIA’s uit te voeren, in ieder geval bij dienstverlening waar gevoelige persoonsgegevens worden verwerkt zoals bij dienstverlening bij de Nationale Politie, financiële instellingen, ziekenhuizen of de voetbalstadions. Door het uitvoeren van PIA’s worden de privacyrisico’s vroegtijdig in kaart gebracht. Aanbevolen wordt om de FG te laten bepalen wanneer en bij welke (soort) dienstverlening een PIA wordt uitgevoerd.

- **Inrichten procedures verzoeken betrokken**
  Omdat de rechten van betrokkenen worden versterkt met de komst van de AVG en betrokkenen steeds meer bekend raken met verzoeken is het verstandig om procedures in te richten. Medewerkers zijn hierdoor voorbereid op eventuele aanvragen. Door middel van deze procedures kan snel op dergelijke verzoeken worden gereageerd.

Literatuurlijst

Boeken

Brahn/Reehuis 2010
W.H.M. Reehuis, Zwaartepunten van het vermogensrecht, Deventer: 2010

Duthler Associates
Duthler Associates, Privacy, cybersecurity en identity management worden volwassen, Den Haag: 2013

Kranenborg/Verhey 2011
Mr. H.R. Kranenborg, Prof. Mr. L.F.M. Verhey, Wet bescherming persoonsgegevens in Europees perspectief, Deventer: 2011

Tekst & commentaar
Wet bescherming persoonsgegevens, Kluwer Navigator

Thole/van der Jagt/Roerdink 2014
Elisabeth Thole, Friederike van der Jagt en Herwin Roerdink, 50 vragen over privacy, Deventer: 2014

De Vey Mestdagh 2014
Dr. Mr. C.N.J. de Vey Mestdagh, Inleiding IT-recht, Groningen: 2014

Handleidingen:

Memorie van toelichting Wet bescherming persoonsgegevens, Kamerstukken II 1997/98, 25892, nr. 3 (MvT)

Memorie van toelichting Wet meldplicht datalekken, Kamerstukken II 2012/13, 33662, nr. 3 (MvT)

Europese Commissie, *voorstel voor een Verordening van het Europese parlement en de raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming)*, Brussel: januari 2012/0011

Mr. L.B. Sauerwein en Mr. J.J. Linnemann Ministerie van Justitie, *Handleiding wet bescherming persoonsgegevens,* Den Haag: april 2002

College bescherming persoonsgegevens*, CBP Richtsnoeren beveiliging van persoonsgegevens,* 2013

NOREA – de beroepsorganisatie van IT-auditors, *Privacy Impact Assessment: introductie handleiding en vragenlijst,* 2013

Tijdschriften

K. Daniëls en P. Kits*, Contracteren in de Cloud- ken uw risico's,* Contracteren, maart 2015 nr. 1

J.P. de Jong*, De Algemene verordening gegevensbescherming: de rechtsopvolger van de Wbp,* RegelMaat 2015 (30) 1

Mr. J.H.J. Terstegge, *Privacyclausules in dienstverleningscontracten*, Contracteren, 2007/3

Mr. C.M.M. Zwinkels*, Artikel 13 Wbp: de zorgplicht en informatiebeveiliging,* Privacy & Informatie 2014/3 (juni)

Jurisprudentie

HvJ EU 13 mei 2014 (*Google Spanje/AEPD en Costeja*)