



PARAAT VOOR PRIVACY

Bijlagen

L.M.C. (Lizette) Gevers

's-Hertogenbosch, 1 juni 2015

Bijlage I Standaard bewerkersovereenkomst Canon

Bewerkersovereenkomst

Behorende bij (Mantel) Overeenkomst met kenmerk, [(Mantel) Overeenkomst referentie]

Ondergetekenden

1. Canon Nederland N.V., statutair gevestigd te Amsterdam en kantoorhoudende aan de Brabantlaan 2, 5216 TV te 's-Hertogenbosch, geregistreerd onder Handelsregister nummer ..., te dezen rechtsgeldig vertegenwoordigd door ..., hierna te noemen "Bewerker"
2. [Stat. naam Klant], statutair gevestigd te [Stat. zetel] en kantoorhoudende aan de [Kantoor Adres], [Postcode Adres] te [Plaats], geregistreerd onder Handelsregister nummer [KvK nummer], te dezen rechtsgeldig vertegenwoordigd door [KlantGevolmachtigde1], [KlantGevolmachtigde2] en [KlantGevolmachtigde3], hierna te noemen "Verantwoordelijke"

In aanmerking nemende dat:

- Bewerker en Verantwoordelijke een overeenkomst hebben gesloten met referentie [(Mantel) Overeenkomst referentie] gedateerd [Datum(Mantel) Overeenkomst] hierna genoemd "Overeenkomst";
- Het verlenen van de service zoals overeengekomen in de Overeenkomst met zich meebrengt dat (persoons)gegevens van Verantwoordelijke ter beschikking of ter kennis komen van Bewerker;
- Bewerker ten behoeve van de Verantwoordelijke (persoons)gegevens verwerkt zonder dat de Bewerker onder het rechtstreekse gezag staat van Verantwoordelijke; *en*
- dat de Verantwoordelijke op grond van de Wet Bescherming Persoonsgegevens (de "WBP") verplicht is een bewerkersovereenkomst aan te gaan met de Bewerker.

Komen hierbij overeen:

1. Relatie tot (Mantel)Overeenkomst

Deze Bewerkersovereenkomst vormt een bijlage bij de Overeenkomst. De bepalingen uit de Overeenkomst zijn van toepassing op deze Bewerkersovereenkomst, tenzij daarvan is afgeweken in deze Bewerkersovereenkomst.

2. Positie partijen

Verantwoordelijke is "verantwoordelijke" in de zin van de WBP ten aanzien van door Verantwoordelijke in het kader van de Overeenkomst aan Bewerker beschikbaar gestelde (persoons)gegevens ("Persoonsgegevens"). Bewerker is terzake "bewerker" in de zin van de WBP en verwerkt de (persoons)gegevens in het kader van het doel als omschreven in artikel 3.

3. Verwerking

Het doel waarvoor Bewerker de (persoons)gegevens zal verkrijgen c.q. verzamelen vormt de uitvoering van de met Verantwoordelijke gesloten Overeenkomst, meer in het bijzonder ten behoeve van: [DoelGebruikGegevens].
Verwerking van (persoons)gegevens zal uitsluitend plaatsvinden in het kader van bovengenoemd doel, een en ander met inachtneming van de bepalingen van de WPB.

4. Nakoming WBP

Partijen zullen hun verplichtingen op grond van de WBP zorgvuldig nakomen. Doorgifte door Verwerker van (persoons)gegevens naar een ander land, dan wel het verlenen van toegang tot (persoons)gegevens vanuit een ander land is op generlei wijze toegestaan zonder de voorafgaande schriftelijke toestemming van Verantwoordelijke en zonder dat vooraf aan alle eisen die de WBP ten aanzien daarvan stelt, is voldaan.

5. Beveiliging

Bewerker zal de binnen het wettelijke kader voorgeschreven passende technische en organisatorische maatregelen ten uitvoer leggen om de (persoons)gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van (persoons)gegevens te voorkomen. Op eerste verzoek van Verantwoordelijke zal Bewerker haar informeren over de getroffen maatregelen.

6. Geheimhouding

Bewerker en de door haar ingezette personen zijn verplicht tot geheimhouding van (persoons)gegevens waarvan zij bij het verwerken ten behoeve van Verantwoordelijke kennisnemen, behoudens en voor zover enig wettelijk voorschrift hen tot openbaarmaking en/of afgifte verplicht. Bewerker zal er actief op toezien dat de door haar ingezette personen deze geheimhoudingsverplichting betrachten.

7. Informatieverstrekking

- 7.1. Het is Bewerker niet toegestaan om (persoons)gegevens derden te openbaren in welke vorm dan ook, tenzij de wet zulks voorschrijft of tenzij voorafgaande schriftelijke toestemming van Verantwoordelijke daarvoor is verkregen. Bewerker zal Verantwoordelijke onverwijld informeren indien een daartoe bevoegde overheidsinstantie een op de wet gebaseerd verzoek tot verstrekking van (persoons)gegevens heeft gedaan. Voorts is Bewerker gehouden Verantwoordelijke ervan in kennis te stellen wanneer een onbevoegde derde toegang tot de gegevens heeft gehad.
- 7.2. In geval van een verzoek als bedoeld in artikel 7.1 stelt Verwerker de toezichthoudende autoriteit(en) met betrekking tot het verwerken van (persoons)gegevens in kennis van het feit dat Verwerker (persoons)gegevens verwerkt, in welke hoedanigheid dan ook, voorzover dit is vereist op grond van toepasselijke wet- en regelgeving.

8. Toezicht door Verantwoordelijke

- 8.1. In geval van gerede twijfel betreffende nakoming van verplichtingen door Bewerker zal op eerste verzoek van Verantwoordelijke Bewerker een door Verantwoordelijke aangewezen onafhankelijke derde de mogelijkheid geven te controleren of Bewerker de beveiligingsmaatregelen als voorzien in deze Bewerkersovereenkomst naleeft. Verantwoordelijke zal hiertoe Bewerker tijdig schriftelijk berichten wanneer de onafhankelijke derde de controle wenst uit te voeren. In gezamenlijk overleg zal hiervoor een datum worden bepaald. In beginsel zal een controle ingevolge dit artikel lid maximaal tweemaal per jaar plaatsvinden, tenzij Verantwoordelijke redelijke en te verantwoorden aanwijzingen heeft dat Bewerker haar verplichtingen terzake niet nakomt.
- 8.2. Bewerker zal aan Verantwoordelijke of de door haar aangewezen onafhankelijke derde, ten behoeve van de controle toegang verschaffen tot haar kantoren, werkruimten en systemen en zal op verzoek van Verantwoordelijke haar of de door haar aangewezen derde kosteloos assisteren bij deze controle en vragen terzake beantwoorden.

9. Aansprakelijkheid en vrijwaring

- 9.1. Bewerker is aansprakelijk voor aanspraken van betrokkenen in de zin van de WBP die het gevolg zijn van een schending of niet nakoming door Bewerker van haar verplichtingen voortvloeiend uit deze Bewerkersovereenkomst of uit de wettelijke bepalingen ter bescherming van (persoons)gegevens.
- 9.2. Indien Bewerker deze Bewerkersovereenkomst niet naleeft, dan geldt, onverminderd de andere wettelijke verhaalsmogelijkheden van Verantwoordelijke, dat:
 - i. Bewerker Verantwoordelijke daar onmiddellijk schriftelijk van in kennis dient te stellen;
 - ii. Bewerker zonder aanmaning of andere voorafgaande kennisgeving, een boete aan Verantwoordelijke verschuldigd is van EUR 25.000 per schending, onverminderd de andere wettelijke verhaalsmogelijkheden van Verantwoordelijke.
- 9.3. Bewerker vrijwaart Verantwoordelijke ter zake van alle aanspraken van derden, aansprakelijkheden, verliezen, schade en onkosten die voortvloeien uit of verband houden met schending door Bewerker van deze Bewerkersovereenkomst.

- 9.4. De aansprakelijkheid van bewerker is beperkt tot de directe schade en tot een bedrag van € 4.500.000,00 per gebeurtenis of reeks van gebeurtenissen. Bewerker is niet aansprakelijk voor enige andere schade dan genoemd in dit artikel. In het bijzonder is Bewerker ook niet aansprakelijk voor gevolg en/of bedrijfsschade en Verantwoordelijke vrijwaart Bewerker tegen zodanige aanspraken van derden.

10. Intellectuele eigendomsrechten

Alle intellectuele eigendomsrechten, waaronder in dit verband in ieder geval begrepen de databank-rechten, die verband houden met de (persoons)gegevens in de zin van deze Bewerkersovereenkomst berusten bij Verantwoordelijke en zullen te allen tijde bij Verantwoordelijke blijven berusten.

11. Duur, Toepasselijk recht en forumkeuze

- 11.1. Deze Bewerkersovereenkomst is accessoir aan de Overeenkomst hetgeen betekent dat:
- i. deze Bewerkersovereenkomst, vanaf zijn ondertekening datum, van kracht is en van kracht blijft, zolang de Overeenkomst nog van kracht is; en
 - ii. deze Bewerkersovereenkomst van rechtswege (automatisch, zonder dat opzegging of een andere handeling is vereist) eindigt op de einddatum van de Overeenkomst, tenzij na de einddatum van de Overeenkomst nog plichten inzake vernietiging, retour of migratie aangaande de (persoons)gegevens op Bewerker rusten, in welk geval deze Bewerkersovereenkomst automatisch (zonder dat opzegging of een ander handeling is vereist) eindigt op de datum waarop Bewerker de plichten inzake vernietiging, retour of migratie volledig is nagekomen, jegens Verantwoordelijke.
- 11.2. De volgende artikelen van deze Bewerkersovereenkomst zullen na het einde van de Bewerkersovereenkomst blijven gelden tussen Verantwoordelijke en Bewerker: artikel 6, artikel 7, artikel 9 en onderhavig artikel 11.
- 11.3. Op deze Bewerkersovereenkomst is Nederlands recht van toepassing.
- 11.4. Alle geschillen verband- houdende met of voortvloeiende uit deze Bewerkersovereenkomst vallen onder de exclusieve competentie van de bevoegde rechter in 's-Hertogenbosch.

Wijzigingen of aanpassingen op de Bewerkersovereenkomst of onderliggende documenten geschiedt schriftelijk door ondertekening van beide Partijen.

Deze Overeenkomst is opgemaakt in tweevoud en rechtsgeldig op iedere pagina geparafeerd en namens elk der partijen ondertekend en elk der partijen heeft één exemplaar.

d.d.

[Plaats]

d.d.

's-
Hertogenbosch

[Stat. naam Klant]

Canon Nederland N.V.

[KlantGevolmachtigde1]
[FunctieGevolmachtigde1]

J.M.G. van Boerdonk
Managing Director

en

[KlantGevolmachtigde2]
[FunctieGevolmachtigde2]

en

[KlantGevolmachtigde3]
[FunctieGevolmachtigde3]

Met de uitvoering van de overeenkomst wordt gestart zodra de twee exemplaren van de door u geparafeerde en ondertekende overeenkomst zijn ontvangen op onderstaand adres:

Canon Nederland N.V.
CS Solutions
Antwoordnummer 2100 (Een postzegel is niet nodig)
5200 VC 's-Hertogenbosch

Bijlage II Dienstverlening bewakingssysteem

FC Dordrecht breidt CCTV- bewakingssysteem uit met Canon

FC Dordrecht

Netwerkkamera's



Case Study

Organisatie	FC Dordrecht
Opgericht	1883
Locatie	Dordrecht, Nederland
Diensten	Voetbalstadion
Website	www.fcdordrecht.nl
Twitter	@fcdordrecht
Producten	Canon VB-H41 netwerkkamera's

“We zochten een oplossing om ons beveiligingssysteem volledig te vernieuwen,” zegt Jacques de Zeeuw, veiligheidsmanager bij FC Dordrecht. “We wilden op elk moment beelden met de hoogste kwaliteit kunnen vastleggen, vooral in delen van het stadion met minimale verlichting. We hadden het gevoel dat de overstap van analoog naar digitaal de enige manier was om dat te realiseren.”

Achtergrond

FC Dordrecht promoveerde onlangs naar de Eredivisie, de hoogste klasse in het betaald voetbal in Nederland. Om te zorgen dat het groeiend aantal fans de thuiswedstrijden veilig kan bijwonen, diende de club het beveiligingssysteem te vernieuwen. Daarnaast was het voor FC

Dordrecht belangrijk om intensiever met de lokale autoriteiten samen te werken om zowel de faciliteiten van de club als de fans beter te beschermen.

De huidige upgrade van het beveiligingssysteem is een tijdelijke oplossing voor een jaar, omdat de club plannen heeft voor de bouw van een nieuw, modern stadion dat aan meer fans plaats kan bieden en over een geavanceerd beveiligingssysteem beschikt dat op die aantallen is afgestemd. Het project was bedoeld om te testen hoe de technologie in de praktijk presteert, met daarbij het doel om het beveiligingssysteem in deze opzet ook toe te passen in het nieuwe stadion wanneer dat in 2016 is gebouwd.

Uitdagingen

FC Dordrecht heeft op dit moment circa 4.500 trouwe supporters. Nu de club in de hoogste klasse speelt, is de verwachting dat het aantal fans dat de wedstrijden wil bijwonen sterk zal toenemen. Zowel wat betreft de eigen supporters als die van bezoekende teams.

De club werd geconfronteerd met de noodzaak het bestaande beveiligingssysteem – een verzameling analoge camera's – te upgraden om deze hogere aantallen supporters te beschermen.

De Koninklijke Nederlands Voetbal Bond (KNVB) regelt de voetbalcompetities voor zowel betaald als amateurvoetbal in Nederland. Tot de verantwoordelijkheden van de KNVB behoort het reguleren en beoordelen van de veiligheid van de stadions waar de eredivisieclubs spelen om te Met het vorige systeem van beveiligingscamera's kon FC Dordrecht niet

voldoen aan de veiligheidseisen van de KNVB. Een upgrade van het systeem was onvermijdelijk nu de club in de hoogste divisie ging spelen.

Het beveiligingsteam had beveiligingscamera's nodig die in staat waren de actie op het veld, op de tribunes en in de parkeergarage te volgen om te zorgen dat alle bezoekers veilig konden genieten van de wedstrijden. Er was ook behoefte aan gezichtsherkenning van fans in het stadion, zodat de autoriteiten snel de identiteit van bepaalde personen kunnen vaststellen als zich incidenten voordoen waarbij inschakeling van de politie nodig is.

“We zochten een oplossing om ons beveiligingssysteem volledig vernieuwen,” zegt Jacques de Zeeuw, veiligheidsmanager bij FC Dordrecht. “We wilden op elk moment beelden met de hoogste kwaliteit kunnen vastleggen, vooral in delen van het stadion met minimale verlichting. We hadden het gevoel dat de overstap van analoog naar digitaal de enige manier was om dat te realiseren.”

Omdat het onderdeel uitmaakt van FC Dordrechts beveiligingsstrategie voor de lange termijn, had het beveiligingsteam een oplossing nodig die in staat is geavanceerde gezichtsherkenning te bieden in het nieuwe stadion dat staat gepland voor 2016. Om dit te realiseren, moest het team garanderen dat de voor dit project geselecteerde camera's de technische compatibiliteit bieden met specifieke software voor gezichtsherkenning. Dit aspect is vooral van belang voor de plaatselijke politie, die nauw samenwerkt met het beveiligingsteam om spelers en bezoekers van het stadion te beschermen.

waarborgen dat alle clubs in deze divisie over de juiste beveiligingsmaatregelen beschikken.

“De plaatselijke politie is blij met de gennstalleerde Canon-camera’s. Elke wedstrijd is een team van vijf agenten aanwezig om het terrein te bewaken en onze fans en spelers te beschermen. Het team roemt regelmatig de superieure beeldkwaliteit, beeldscherpte en zoommogelijkheden die onze nieuwe camera’s bieden. Al deze verbeteringen hebben een positieve invloed op de veiligheid in het stadion.”

Jacques de Zeeuw, veiligheidsmanager bij FC Dordrecht.



Canon Inc.
canon.com

Het beveiligingsteam van FC Dordrecht stelde vast dat er behoefte is aan camera’s die elk een breed beeldbereik hebben. Het liet zich adviseren door systeemintegrator CNI Europe BV en op basis van die gesprekken werd ook gekozen voor camera’s met PTZ-functionaliteit.

Na een test van camera’s die op markt verkrijgbaar zijn, selecteerden CNI Europe BV en FC Dordrecht vier Canon VB-H41 PTZ-camera’s. Deze modellen werden gekozen om hun SSC-functionaliteit (Smart Shade Control). De Canon-camera’s verbeteren de weergave van voorwerpen en personen op de voorgrond wanneer deze sterk vanaf de achterzijde worden belicht. Dit stelt het beveiligingsteam in staat voorwerpen te herkennen die het stadion in zijn gesmokkeld en ook gemakkelijk gezichten van bezoekers te herkennen. De prestaties van de VB-H41 camera’s in omgevingen met weinig licht maken het mogelijk de camera’s dag en nacht te gebruiken. De camera’s zorgen in de verschillende delen van het stadion voor zeer goede resultaten en de fans kunnen veilig van het voetbal genieten, ongeacht het tijdstip waarop de wedstrijden worden gespeeld. **Resultaten**

De Video Management Software (VMS) die tijdens de overgangperiode tussen het oude beveiligingssysteem en de upgrade voor de Canon-camera’s wordt gebruikt, stelt FC Dordrecht in staat de zeven nieuwe Canon-camera’s samen met de bestaande analoge camera’s te gebruiken, zodat bezoekers ook veilig zijn tijdens de upgrade van het systeem.

“CNI Europe BV werkt in Nederland al lange tijd samen met Canon en dankzij de PTZmogelijkheden van de VB-H41-camera’s vormden deze modellen de juiste oplossing voor de beveiligingsupgrade van het huidige stadion. Op basis van het succes van het project tot nu toe, kijken we uit naar de samenwerking met Canon wanneer het grotere beveiligingsproject voor het nieuwe stadion van FC Dordrecht van start gaat,” zegt Frank Goldewijk, eigenaar van CNI Europe BV.

Sinds de installatie van de Canon VB-H41 PTZ-camera’s zijn zowel de beveiligings- als detectiemogelijkheden volledig veranderd.

Canon Europe canon.europe.com



Dankzij de beeldkwaliteit en de PTZ-functionaliteit van de camera’s is het beveiligingsteam nu in staat om in te zoomen op andere delen van het stadion om mogelijk verdachte activiteiten tijdig te signaleren. Het beveiligingsteam had in het verleden problemen met mensen die vuurwerk meenamen naar bepaalde delen van het stadion. Na de installatie van de Canon-beveiligingscamera’s is het team veel sneller in staat mensen te identificeren die proberen verboden voorwerpen mee naar binnen te nemen.

Ook het politieteam dat met FC Dordrecht samenwerkt, is blij met de resultaten die worden behaald na de installatie van de nieuwe camera’s in het stadion. Dankzij de uitstekende resultaten tot nu toe, is de verwachting dat de samenwerking

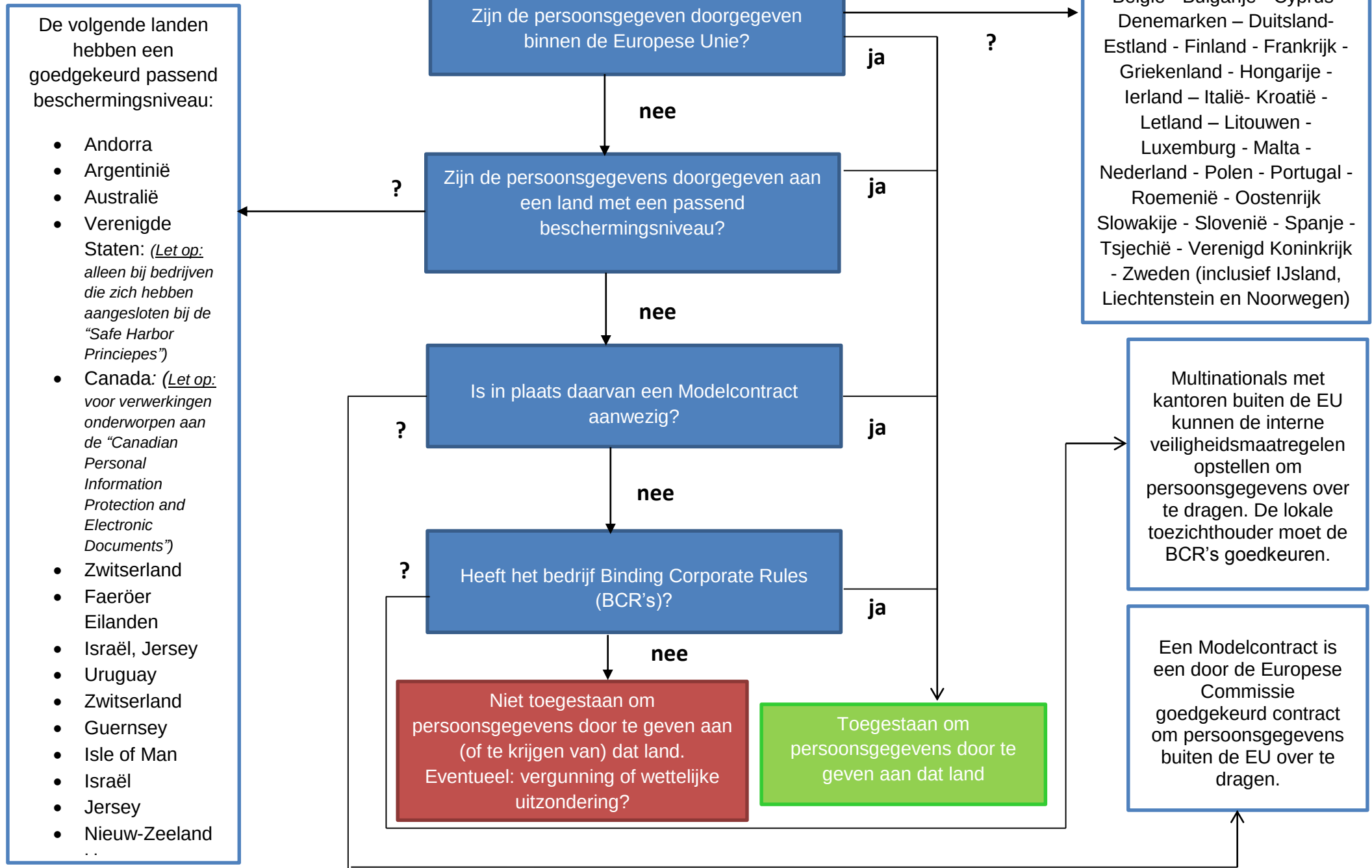
Dutch edition
©Canon Europe N.V., 2014

wordt uitgebreid en dat de politie in de toekomst de live-beelden van de Canon-camera’s vanuit het plaatselijke politiebureau gaat bekijken. Het doel van dit project is ervoor te zorgen dat de camera’s compatibel zijn met het gehele netwerk van de club en het politieteam, zodat een goede bescherming van de fans mogelijk is en de politie direct kan vaststellen of extra ondersteuning nodig is wanneer zich onvoorziene situaties voordoen.

“De plaatselijke politie is blij met de gennstalleerde Canon-camera’s. Elke wedstrijd is een team van vijf agenten aanwezig om het terrein te bewaken en onze fans en spelers te beschermen. Het team roemt regelmatig de superieure beeldkwaliteit, beeldscherpte en zoommogelijkheden die onze nieuwe camera’s bieden. Al deze verbeteringen hebben een positieve invloed op de veiligheid in het stadion,” concludeert de Zeeuw.

Canon Nederland N.V.	Canon NV/SA	Belgium
Bovenkerkerweg 59	Berkenlaan 3	
1185 XB Amstelveen	1831 Diegem	
Tel: +31 (0)20 721	Tel: +32 (0)2 722	
9103 canon.nl	0411 canon.be	

Bijlage III Naar welke landen kan Canon persoonsgegevens doorgeven?



Bijlage IV 7 fundamentele principes van Ann Cavoukian



Privacy by Design

De 7 Fundamentele Principes

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is een concept dat ik in de jaren 90 heb ontwikkeld met als doel een antwoord te bieden op de constant groeiende systematische effecten van informatie- en communicatietechnologieën en van grootschalige genetwerkte datasystemen.

Privacy by Design ontwikkelt het inzicht dat privacy in de toekomst niet slechts kan worden gewaarborgd door uitsluitend het naleven van wettelijke kaders, maar dat de verzekering van privacy in eerste instantie moet komen van een standaard wijze van opereren binnen organisaties.

Aanvankelijk werd de toepassing van Privacy-Enhancing Technologies (PETs) gezien als de oplossing. Vandaag realiseren we echter dat een meer fundamentele benadering nodig is: het uitbreiden van het gebruik van PETs naar PETs PLUS. Daarbij moeten we kiezen voor de 'Positive Sum'-benadering (volledige functionaliteit, $1-1>0$) en niet de 'Zero Sum' ($1-1=0$): 'Positive Sum', en niet de keuze 'óf de ene óf de andere' van de 'zero sum'.

Privacy by Design strekt zich uit tot een "Trilogie" van samenhangende toepassingen: 1) IT systemen; 2) verantwoorde handelspraktijken; 3) het fysieke ontwerp van de techniek en de genetwerkte infrastructuur.

De principes van *Privacy by Design* kunnen toegepast worden op alle vormen van persoonlijk informatie, maar zouden extra stringent moeten worden nageleefd indien er sprake is van gevoelige gegevens, zoals medische en financiële data. De zwaarte van maatregelen ter bescherming van de privacy zouden in verhouding moeten zijn met de gevoeligheid van de gegevens.

Het doel van *Privacy by Design*, zijnde voor individuele personen het verzekeren van de controle over de eigen persoonlijke gegevens en voor organisaties het verkrijgen van een duurzame concurrentiepositie, kan bereikt worden door het toepassen van de 7 hiernavolgende fundamentele principes.



De 7 Fundamentele Principes

1. **Proactief** ipv reactief; **Preventief** ipv herstellend

De *Privacy by Design* (PbD) benadering wordt gekarakteriseerd door het nemen van proactieve maatregelen in plaats van reactieve. Het anticipeert op en voorkomt inbreuken op iemands privacy *voordat* deze feitelijk plaatsvinden. PbD wacht niet totdat privacyrisico's een feit zijn, noch biedt zij oplossingen voor privacyschendingen die reeds hebben plaatsgevonden. Het doel is om te voorkomen dat zij gebeuren. In kort: Privacy by Design vindt vooraf plaats, niet achteraf.

2. Privacy als **Standaard**

Van één ding kunnen we zeker zijn: de standaard is de regel! *Privacy by Design* streeft naar een maximale privacy door te verzekeren dat persoonlijke gegevens in een gegeven IT-systeem of handelspraktijk automatisch afdoende beveiligd zijn. Ook als het individu zelf niets onderneemt zal toch zijn privacy zijn gewaarborgd. Van het individu wordt geen specifieke actie gevraagd om de privacy te beschermen; het is ingebouwd in het systeem, bij wijze van standaard.

3. Privacy **Geïntegreerd** in het ontwerp

Privacy by Design is geïntegreerd in het ontwerp en de architectuur van IT-systemen en handelspraktijken. Het is er niet als een los onderdeel aan vast geplakt, bijvoorbeeld nadat er een privacyschending heeft plaatsgevonden. Het resultaat daarvan is privacy een essentieel onderdeel vormt van de kernfunctionaliteit. Privacy is geïntegreerd in het systeem, zonder aan functionaliteit te hoeven inleveren.

4. Volledige functionaliteit – **Positive-Sum** ipv Zero-Sum

Privacy by Design streeft ernaar om alle legitieme belangen en doelstellingen op de wijze van een 'positive sum' (ofwel 'win-win') te faciliteren, en niet door middel van de ouderwetse 'zero sum' benadering, waar onnodige compromissen worden gemaakt. *Privacy by Design* vermijdt valse dichotomieën, zoals privacy tegenover veiligheid, door te demonstreren dat een combinatie van beiden weldegelijk mogelijk is.

5. Veiligheid van begin tot eind – **Bescherming tijdens de volledige levenscyclus**

Privacy by Design, geïntegreerd in een systeem nog voordat er enige informatie is verzameld, verspreidt zich over de gehele levenscyclus van de betrokken gegevens; krachtige veiligheidsmaatregelen zijn essentieel voor het behoud van privacy, van begin tot eind. Dit geeft namelijk de garantie dat alle gegevens op een veilige wijze zijn verkregen en op een tijdige en veilige wijze zijn vernietigd aan het eind van het proces. Zodoende verzorgt *Privacy by Design* een juiste behandeling van gegevens en een veilige omgang met informatie van begin tot eind.

6. **Zichtbaarheid** en **Transparantie** – Houd het **Open**

Privacy by Design streeft ernaar om alle belanghebbenden bij welke technologie of handelspraktijken dan ook ervan te verzekeren dat het systeem feitelijk opereert conform de oorspronkelijk geclaimde beloftes en doelstellingen, dit geheel ter verificatie door onafhankelijke derden. De technische componenten en het operationeel handelen blijven zichtbaar en transparant voor zowel de gebruikers als de dienstverleners. Onthoud: vertrouwen is de basis, maar nooit zonder controle.

7. **Respect** voor de privacy – laat de gebruiker **centraal** staan

Privacy by Design heeft boven alles architecten en exploitanten nodig die de belangen van het individu als hoogste prioriteit beschouwen, door maatregelen in te stellen zoals het instellen van krachtige privacy instellingen, passende informatievoorziening en gebruikersvriendelijke opties. Houd de gebruiker centraal.

Published: February 2011

Translation provided by: Mr. Max Snijder, Managing Director,
European Biometric Group

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400 • Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073

Web: www.ipc.on.ca • www.privacybydesign.ca E-mail:

info@ipc.on.ca

Bijlage V Overzicht uitbreiding boetebevoegdheid CBP

Het College bescherming persoonsgegevens krijgt een uitgebreidere bestuurlijke boetebevoegdheid. Hieronder staat op welke overtredingen ze een boete mogen opleggen. In de lichtblauwe tabel staat het wetsartikel wat de bevoegdheid geeft aan het CBP, daarbij staat ook de hoogte van de geldboete. Daaronder staan in de linkse tabel de overtredingen (artikelen uit de Wet bescherming persoonsgegevens) en aan de rechterkant van de tabel de uitleg van het desbetreffende artikel.

Artikel 66 lid 1: Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (**€20.250**) ter zake van overtreding van het bepaalde bij of krachtens de artikelen 4, derde lid, of 78, tweede lid, aanhef en onder a.

Artikel 4 lid 3 Wbp	↓ Verantwoordelijke die persoonsgegevens verwerking die geen vestiging heeft in de EU moet een persoon of instantie aanwijzen in Nederland die namens hem handelt overeenkomstig de bepalingen uit de wet.
Artikel 78 lid 2 onder a Wbp	Doorgifte naar een land buiten de EU dat de minister van justitie bij ministeriele regeling of bij besluit heeft bepaald, is verboden.

Artikel 66 lid 2: Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (**€ 810.000**)* ter zake van overtreding van het bepaalde bij of krachtens de artikelen 6 tot en met 8, 9, eerste en vierde lid, 10, eerste lid, 11 tot en met 13, 16, 24, 33, 34, eerste, tweede en derde lid, 34a, 35, eerste lid, tweede volzin, tweede, derde en vierde lid, 36, tweede, derde en vierde lid, 38 tot en met 40, tweede en derde lid, 41, tweede en derde lid, 42, eerste en vierde lid, 76, 77 of 78, derde en vierde lid, alsmede van artikel 5:20 van de Algemene wet bestuursrecht.

*Eerst moet een bindende aanwijzing worden gegeven bij opzettelijk (of ernstig verwijtbare nalatigheid) gepleegde overtredingen (artikel 66 lid 3 Wbp). Wanneer de bindende aanwijzing niet wordt nagekomen kan het CBP een boete opleggen van € 810.000. Artikel 23 lid 7 van het Wetboek van Strafrecht is overeenkomstig van toepassing (artikel 66 lid 5). Dit artikel bepaalt dat bij veroordeling van een rechtspersoon, wanneer hierboven genoemd geldbedrag geen passende bestraffing toelaat, een geldboete kan worden opgelegd tot ten hoogste **10% van de jaaromzet** van de rechtspersoon.

Artikel 6 Wbp	↓ Persoonsgegevens moeten in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.
Artikel 7 Wbp	Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.
Artikel 8 Wbp	Persoonsgegevens mogen slechts worden verwerkt indien (één van de) in artikel 8 genoemde gronden van toepassing is.
Artikel 9 lid 1 Wbp	Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
Artikel 9 lid 4 Wbp	De verwerking van persoonsgegevens blijft achterwege voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.
Artikel 11 Wbp	Persoonsgegevens worden slechts verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn. Persoonsgegevens moeten juist en nauwkeurig zijn.

Artikel 12 Wbp	(Medewerkers van) de verantwoordelijke en (medewerkers van de) bewerker verwerken de persoonsgegevens slechts in opdracht van de verantwoordelijke en hebben een geheimhoudingsplicht.
Artikel 13 Wbp	De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen een passend beveiligingsniveau. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
Artikel 16 Wbp	Verwerking van bijzondere persoonsgegevens zijn verboden. Bijzondere persoonsgegevens zijn: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
Artikel 24 Wbp	Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven (bijvoorbeeld BSN), wordt bij de verwerking van persoonsgegevens alleen onder bepaalde bij de wet voorgeschreven omstandigheden/doeleinden gebruikt.
Artikel 33 Wbp	De informatieplicht bij verkrijging van persoonsgegevens van de betrokkene.
Artikel 34 lid 1 Wbp	De informatieplicht bij verkrijging van persoonsgegevens van iemand anders dan de betrokkene.
Artikel 34 lid 2 Wbp	De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.
Artikel 34 lid 3 Wbp	De verantwoordelijke is verplicht tot het verstrekken van nadere informatie wanneer dat nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
Artikel 34a Wbp	Meldplicht datalekken: De verantwoordelijke moet datalekken melden. Hij stelt het CBP onverwijld in kennis van inbreuken op de beveiliging indien deze inbreuk leidt tot de aanzienlijke kans op ernstige gevolgen voor de bescherming van persoonsgegevens of waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer. Ook moet deze melding aan de betrokkene plaatsvinden.
Artikel 35 lid 1 2 ^e volzin Wbp	Op een verzoek om inzage van een betrokkene dient de verantwoordelijke binnen 4 weken te reageren.
Artikel 35 lid 2 Wbp	Indien blijkt dat zulke gegevens worden verwerkt, bevat de mededeling: een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.
Artikel 35 lid 3 Wbp	Een derde die naar verwachting bedenkingen zou hebben tegen de mededeling moet in de gelegenheid gesteld worden zijn zienswijze naar voren te brengen.
Artikel 35 lid 4 Wbp	Op verzoek doet de verantwoordelijke mededelingen inzake de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de betreffende gegevens.

Artikel 36 lid 2 Wbp	Verzoek tot correctie: Binnen 4 weken na ontvangst moet de verantwoordelijke de verzoeker laten weten in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
Artikel 36 lid 3 Wbp	De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
Artikel 36 lid 4 Wbp	Informatieplicht aan de betrokkene wanneer persoonsgegevens onmogelijk kunnen worden gecorrigeerd.
Artikel 38 Wbp	De verantwoordelijke die aan een verzoek tot correctie heeft voldaan, is verplicht om aan derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis te geven hiervan.
Artikel 39 Wbp	De kosten van een verzoek van een betrokkene bedraagt maximaal € 5, -.
Artikel 40 lid 2 Wbp	De verantwoordelijke beoordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is beëindigt hij onmiddellijk de verwerking.
Artikel 40 lid 3 Wbp	De verantwoordelijke kan voor het in behandeling nemen van een verzet een vergoeding van kosten verlangen. De vergoeding wordt teruggegeven in geval het verzet gegrond wordt bevonden.
Artikel 41 lid 2 Wbp	Indien gegevens worden verzameld voor een commercieel of charitatief doel heb je het absoluut recht van verzet. Kennisgeving binnen vier weken na ontvangst van verzoek.
Artikel 41 lid 3 Wbp	Indien gegevens worden verzameld voor een commercieel of charitatief doel heeft de verantwoordelijke de verplichting tot het vermelden van het recht van verzet.
Artikel 42 lid 1 Wbp	Geautomatiseerde individuele besluitvorming is verboden.
Artikel 42 lid 4 Wbp	In geval van de uitzonderingen zoals bedoeld in artikel 42 lid 2, deelt de verantwoordelijke de betrokkene de logica mee die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.
Artikel 76 Wbp	Doorgifte naar niet EU-landen is slechts toegestaan indien een passend beschermingsniveau is gewaarborgd.
Artikel 77 Wbp	Hierin staan de criteria voor de doorgifte naar niet EU-landen zonder passend beschermingsniveau.
Artikel 78 lid 3 Wbp	Aan een derde land, waarvan de Commissie van de Europese Gemeenschappen of de Raad van de Europese Unie heeft vastgesteld dat het een passend beschermingsniveau heeft kunnen persoonsgegevens worden doorgegeven.
Artikel 78 lid 4 Wbp	Doorgifte naar een land als bedoeld in artikel 78 lid 3 kan alsnog worden opgeschort op last van de Minister van Justitie.
Artikel 5:20 Awb	Verplichting tot verlening van medewerking

Bijlage VI Privacychecker



Rapport

Boetemeter

Dank u voor het invullen van de boetemeter. Uw totale potentiële boete bedraagt:

Totale boete: € 6.500.000.000,00

1. Algemene juridische eisen

1 Heeft u een privacy policy in duidelijke en begrijpelijke taal?

☐

Ja

☒

Nee

Het juiste antwoord is Ja

De Verordening eist dat u uw identiteit bekend maakt aan de betrokkene, de doelen waarvoor u gegevens verwerkt, welke gegevens u verwerkt en hoe lang u ze opslaat (in de praktijk: een privacy policy). Daarnaast eist de verordening dat u deze informatie in duidelijke en begrijpelijke taal meedeelt

2 Heeft u een legitieme reden voor het verwerken van persoonsgegevens?

☒

Ja

☐

Nee

Het juiste antwoord is Ja

U moet een rechtmatige grondslag hebben voor de verwerking van persoonsgegevens. Zonder rechtmatige grondslag voor uw verwerkingsdoel mag u geen persoonsgegevens verwerken. Rechtmatige grondslagen zijn onder andere de toestemming van de betrokkene, het feit dat de gegevens noodzakelijk zijn voor de uitvoering van een overeenkomst, een wettelijke plicht, of de noodzakelijkheid voor het goed uitoefenen van een publiekrechtelijke taak.

3 Verwerkt u de gegevens voor andere doelen dan waarvoor ze oorspronkelijk verzameld zijn en is dit doel niet verenigbaar met het oorspronkelijke doel?

☐

Ja

☒

Nee

Het juiste antwoord is Nee

U mag gegevens alleen gebruiken voor de doelen waarvoor u ze oorspronkelijk heeft verzameld. Gebruikt u de gegevens toch voor andere doeleinden dan mag dit alleen wanneer deze doelen verenigbaar zijn met het oorspronkelijke doel.

4 Verwerkt u bijzondere persoonsgegevens (gezondheid, seksuele leven, religie etc.) zonder toestemming van de betrokkene en bent u geen organisatie die hiervoor specifiek bedoeld is (bijv. ziekenhuis, politie of kerk)?

☐

Ja

☒

Nee

Het juiste antwoord is Nee

Het verwerken van bijzondere persoonsgegevens (gegevens die gezien hun aard als gevoelig worden beschouwd zoals gegevens over gezondheid, seksuele voorkeur, religie, politieke voorkeur of strafrechtelijk verleden) mogen niet worden verwerkt tenzij u de toestemming heeft van de betrokkene, of u bent een organisatie die daar speciaal op is gericht (zoals bijvoorbeeld medische informatie door een ziekenhuis)

2. Rechten van de betrokkene

1 Heeft u procedures waarmee u betrokkenen inzicht kunt geven in de verwerking van hun persoonsgegevens? ☐ Ja

 ☒ Nee

Het juiste antwoord is Ja

Als een betrokkene daarom vraagt, dan moet u de betrokkene informatie verschaffen over de gegevens die u van de betrokkene verwerkt. Hiervoor moet u een specifieke procedure inrichten.

2 Gaat u in op verzoeken van betrokkenen die willen weten welke gegevens u van hen verwerkt?

 ☐ Ja
☒ Nee

Het juiste antwoord is Ja

Als een betrokkene daarom vraagt, dan moet u de betrokkene informatie verschaffen over de gegevens die u van de betrokkene verwerkt.

3 Heeft u procedures waarmee u op verzoek van de betrokkene gegevens kunt corrigeren en aanpassen?

 ☐ Ja
☒ Nee

Het juiste antwoord is Ja

Als een betrokkene daarom vraagt, dan moet u gegevens die incorrect of incompleet zijn aanpassen. Hiervoor moet u een specifieke procedure inrichten.

4 Heeft u procedures waarmee u ervoor zorgt dat op het verzoek van de betrokkene gegevens niet langer verwerkt en verspreid worden (recht om vergeten te worden)?

☐ Ja
 ☒ Nee

Het juiste antwoord is Ja

Betrokkenen hebben het recht om "vergeten te worden". Hiervoor moet u een specifieke procedure inrichten.

5 Heeft u procedures waarmee u de betrokkene de mogelijkheid biedt om een afschrift van zijn gegevens te verkrijgen in een bruikbaar formaat (data portabiliteit)?

☐ Ja
☒ Nee

Het juiste antwoord is Ja

Betrokkenen hebben het recht om een afschrift te krijgen van hun gegevens in een gangbaar en bruikbaar formaat, zodat zij deze gegevens mee kunnen nemen naar een andere dienst. Hiervoor moet u een specifieke procedure inrichten.

6 Reageert u binnen een maand op verzoeken tot inzage, wijziging, verwiidering of data portabiliteit?

☐ Ja
☒ Nee

Het juiste antwoord is Ja

U moet binnen een maand de betrokkene op de hoogte stellen van de behandeling van hun verzoek en de voortgang daarvan.

7 Brengt u kosten in rekening voor de uitvoering van verzoeken tot inzage, wijziging of verwiidering?

☒ Ja
 ☐ Nee

Het juiste antwoord is Nee

U mag geen kosten in rekening brengen voor verzoeken tot inzage, wijziging of verwijdering.

3. Verantwoording en documentatie

1 Heeft u documentatie waaruit blijkt welke persoonsgegevens u verwerkt, waarom u dit doet en wie verantwoordelijk is voor de gegevens?

☒ Ja

 ☐ Nee

Het juiste antwoord is Ja

U moet vastleggen waarom u gegevens verwerkt, welke gegevens dit zijn en wie de verantwoordelijkheid heeft voor de verwerking.

2 Als u met meerdere partners samenwerkt, legt u dan concreet vast wie voor welk deel van de verwerking verantwoordelijk is?

☒ Ja

 ☐ Nee

Het juiste antwoord is Ja

Wanneer u met verschillende partijen samenwerkt (bijvoorbeeld binnen een joint venture) dan moet u met deze partijen afspraken maken over de verdeling van de verantwoordelijkheid voor de verwerking.

3 Heeft u een duidelijk omschreven privacybeleid?

 ☒ Ja

 ☐ Nee

Het juiste antwoord is Ja

U bent verplicht een privacybeleid te formuleren.

4 Heeft u een duidelijk omschreven beleid voor de privacy-vriendelijke ontwikkeling van producten of diensten (privacy by design & privacy by default)?

☐ Ja

 ☒ Nee

Het juiste antwoord is Ja

U bent verplicht een beleid te formuleren waarmee u invulling geeft aan de principes van Privacy by Design en Privacy by Default.

5 Heeft u een duidelijk omschreven beleid voor informatiebeveiliging?

☐ Ja

 ☒ Nee

Het juiste antwoord is Ja

U bent verplicht een beleid te formuleren voor de bescherming van persoonsgegevens.

6 Documenteert u alle inbreuken in verband met persoonsgegevens, inclusief alle feiten, gevolgen en genomen maatregelen?

☐ Ja

☒ Nee

Het juiste antwoord is Ja

U bent verplicht inbreuken in verband met persoonsgegevens te documenteren inclusief de feiten en omstandigheden, de gevolgen die opgetreden zijn en de maatregelen die genomen zijn om schade te voorkomen/vermindern en toekomstige inbreuken te voorkomen.

7 Meldt u datalekken aan de toezichhouder en aan betrokkenen?

- ☒ Ja
 ☐ Nee

Het juiste antwoord is Ja

U bent verplicht inbreuken in verband met persoonsgegevens te melden aan de toezichhouder en onder omstandigheden aan de betrokkenen wiens gegevens geëkt zijn.

8 Doet u een privacy impact assessment bij nieuwe toepassingen en diensten?

-  ☒ Ja
 ☐ Nee

Het juiste antwoord is Ja

U bent verplicht voor nieuwe diensten en toepassingen een privacy effect beoordeling te doen (privacy impact assessment).

Neem contact met ons op voor advies

Geschrokken van de hoogte van mogelijke toekomstige boetes? Bereid u nu alvast voor op de gevolgen van deze nieuwe wetgeving en verbeter uw privacybeleid! Considerati staat u hier graag in bij. Interesse? Neem dan vrijblijvend contact op met Considerati via 020- 737 0069 of schermer@considerati.com



Voor meer informatie zie onze [site](#)

Een initiatief van Considerati.

Mr. Dr. Bart W.

Schermer

Specialist privacyrecht bij

Considerati



+31 (0)6-13433437



CONSIDERATI

schermer@considerati.com