C/M/S/
Law . Tax

Handboek Sport & Privacy

voor sportbonden en NOC*NSF

In opdracht van NOC*NSF

februari 2017

Colofon

De auteurs

Hendrik Struik
Advocaat | Partner
T +31 30 2121 726
M +31 6 54 243 245
E hendrik.struik@cms-dsb.com

Michiel van Dijk
Advocaat | Partner
T +31 30 2121 320
M +31 6 21 284 805
E michiel.vandijk@cms-dsb.com

Erik Jonkman
Advocaat
T +31 30 2121 336
M +31 6 319 015 71
E erik.jonkman@cms-dsb.com

Jurre Reus
Advocaat
T +31 30 2121 631
M +31 6 15 891 046
E jurre.reus@cms-dsb.com

Stephanie Dekker
Advocaat
T +31 20 3016 238
M +31 6 52 634 222
E stephanie.dekker@cms-dsb.com

© CMS Derks Star Busmann N.V., 2017

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van CMS Derks Star Busmann.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteurs en CMS Derks Star Busmann geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

Inhoudsopgave

I Inleiding 5
II Hoe gebruik je dit handboek? 6
III Voor bestuurders en managers: privacy management 6

Hoofdstuk 1: Kernbegrippen 8
1.1 Wat is privacy? 8
1.2 De Wet bescherming persoonsgegevens (Wbp) 8
1.3 Het verwerken van persoonsgegevens 8
1.4 De betrokkene 9
1.5 De verantwoordelijke 9
1.6 De bewerker 10
Hoofdstuk 2: Basisregels 11
2.1 Doel en grondslag 11
2.1.1 Mag ik persoonsgegevens verwerken? 11
2.1.2 Grondslagen 11
2.1.3 Grondslag: gerechtvaardigd belang 11
2.1.4 Grondslag: toestemming 12
2.1.5 Grondslag: overeenkomst 13
2.1.6 Grondslag: wettelijke plicht 13
2.1.7 Doelbinding: gebruik voor andere dan oorspronkelijke doeleinden? 13
2.2 Bewaren 14
2.2.1 Welke bewaartermijn moet ik hanteren? 14
2.2.2 Wettelijke plicht 14
2.2.3 Langer bewaren voor historische, statistische of wetenschappelijke doeleinden 14
2.2.4 Vrijstellingsbesluit als hulpmiddel 15
2.3 Bijzondere persoonsgegevens 15
2.3.1 Wat zijn bijzondere persoonsgegevens? 15
2.3.2 Wanneer mag ik bijzondere persoonsgegevens verwerken? 16
2.3.3 Gezondheidsgegevens 16
2.4 Beveiliging 17
2.4.1 Waar moet ik tegen beveiligen? 17
2.4.2 Wat zijn ‘passende’ beveiligingsmaatregelen? 17
2.4.3 Wat als wij geen kennis in huis hebben? 17
2.5 Meldplicht datalekken 18
2.5.1 Wat is een datalek? 18
2.5.2 Moet ik melden aan de Autoriteit Persoonsgegevens? 18
2.5.3 Moet ik melden aan de betrokkene? 18
2.6 Bewerkers en de bewerkersovereenkomst 19
2.6.1 Wat is een bewerker? 19
2.6.2 Bewerkersovereenkomst 19
2.6.3 Veelvoorkomende vragen over de bewerkersovereenkomst 20
2.7 Informeren 20
2.7.1 Wat houdt de informatieplicht in? 20
2.7.2 Op welk moment moet de betrokkene worden geïnformeerd? 20
2.7.3 Welke informatie moet worden verstrekt? 21
2.7.4 In welke vorm stel ik de informatie beschikbaar? 21
2.7.5 Moet de betrokkene altijd worden geïnformeerd? 21
2.8 Rechten van de betrokkene 22
2.8.1 Recht op inzage 22
2.8.2 Recht op verbetering, aanvulling en verwijdering 22
2.8.3 Recht van verzet 23
2.9 Doorgifte naar het buitenland 23
2.9.1 Het doorgifteverbod 23
2.9.2 Welke landen maken deel uit van de EER? 23
2.9.3 Is het doorgifteverbod relevant voor mijn organisatie? 23
2.10 Aanmelding bij de Autoriteit Persoonsgegevens 24
2.11 Functionaris gegevensbescherming 24
2.11.1 Wat is een Functionaris gegevensbescherming? 24
2.11.2 Is een Functionaris gegevensbescherming verplicht? 24
2.12 Toezicht, sancties en aansprakelijkheid 24
2.12.1 Handhaving door autoriteiten 24
2.12.2 Civiele aansprakelijkheid 25
2.12.3 Strafrecht 25
2.12.4 Verzekeren 25
Hoofdstuk 3: Het delen van persoonsgegevens 26
3.1 Delen met derden: 5 vuistregels 26
3.1.1 Regel 1: Bepaal of er een geldige grondslag is 26
3.1.2 Regel 2: Verstrek uitsluitend noodzakelijke gegevens 27
3.1.3 Regel 3: Zorg voor een veilige overdracht 27
3.1.4 Regel 4: Stel vast of je de betrokkene moet informeren 27
3.1.5 Regel 5: Documenteer de verstrekking 27
3.2 Delen binnen de organisatie 28
3.3 Beschikbaarstelling aan vrijwilligers 28
Hoofdstuk 4: Wedstrijdadministratie 29
4.1 Wedstrijduitslagen en standen 29
4.2 Gegevens van deelnemers en arbiters 29
4.3 Werken met vrijwilligers 30
4.4 Bewaartermijn 30
Hoofdstuk 5: Ledenadministratie 31
5.1 Welke gegevens neem je op in de ledenadministratie? 31
5.2 Gelaagde structuur: wat zijn ‘leden’? 31
5.3 Ledenlijst beschikbaar stellen aan leden 31

© CMS Derks Star Busmann N.V., 2017

5.4 Online publicatie van de ledenlijst 31
5.5 Toegestaan gebruik binnen de organisatie 32
5.6 Delen met sponsoren voor marketingdoeleinden 32
5.7 Bewaartermijn 32
Hoofdstuk 6: Talent en topsport 33
6.1 Gezondheidsgegevens 33
6.2 Monitoring 33
6.3 Wearables 33
6.4 Minderjarig talent 33
6.5 Reizen 34
Hoofdstuk 7: Marketing 35
7.1 Elektronische direct marketing (o.a. mailings) 35
7.1.1 Wat is direct marketing? 35
7.1.2 Wanneer is het SPAM-verbod wel/niet van toepassing? 35
7.1.3 Heb je toestemming nodig voor het versturen van mailings? 35
7.1.4 Zijn er ook situaties waarin je geen toestemming nodig hebt? 36
7.1.5 Hoe zit het met gemengde nieuwsbrieven aan leden? 36
7.1.6 Informeren en opt-out 36
7.1.7 Targeted advertising 36
7.1.8 Externe partij als bewerker 36
7.1.9 Telemarketing 37
7.2 Sociale media 37
7.3 Winacties 37
7.4 Cookies 37
7.4.1 Wat zijn cookies? 37
7.4.2 Toestemming, informatieplicht en uitzonderingen 38
7.4.3 Verwerken van persoonsgegevens 38
Hoofdstuk 8: Beeldmateriaal 39
8.1 Publicatie van beeldmateriaal: privacy-regels 39
8.2 Publicatie van beeldmateriaal: portretrecht 39
8.2.1 Portretten in opdracht gemaakt 39
8.2.2 Portretten niet in opdracht gemaakt 40
Hoofdstuk 9: Webwinkels 41
9.1 Inleiding 41
9.2 Doel en grondslag 41
9.3 Direct marketing en cookies 41
9.4 Informatieplicht 41
9.5 Bewaartermijn 42
9.6 Delen met derden 42
9.7 Beveiliging 42
Hoofdstuk 10: Opleiding 43
10.1 Doel en grondslag 43
10.2 Verstrekking aan derden 43
10.3 Informatieplicht 43
10.4 Bewaartermijn 43
Hoofdstuk 11: Personeel 44
11.1 Sollicitanten 44
11.2 Personeelsadministratie 45
11.3 Zieke werknemers 45
11.4 Toezicht 46
11.5 Bring Your Own Device 48
11.6 De ondernemingsraad 48
11.7 Klokkenluiders 48

Bijlage: FAQ Privacy Impact Assessment 50
Bijlage: model bewerkersovereenkomst 51
Bijlage: model privacyverklaring 56
Bijlage: model kernprotocol datalekken 57
Bijlage: stroomschema's beleidsregels datalekken AP 59

Trefwoordenlijst 60

© CMS Derks Star Busmann N.V., 2017

I. Inleiding

In de sport draait vrijwel alles om winst en verlies. Die spanning verklaart deels waarom sport, media en commercie graag met elkaar optrekken. Met evenementen zoals de Olympische Spelen en de Tour de France worden immers niet alleen winnaars gecreëerd, maar ook een lucratieve branche vol met beroemdheden. Voor een gebrek aan aandacht hoeft de sport dan ook niet te vrezen.

In een wereld die drijft op publiciteit lijkt privacy al snel een exotisch begrip. Toch valt ook op het terrein van privacy het nodige te winnen en verliezen. Een voorbeeld:

> *Toen een minderjarige sporter enkele jaren geleden positief testte tijdens een dopingprocedure, ontstond discussie of de test ongeldig moest worden verklaard. Op het afnemen van urinemonsters en de verwerking hiervan is immers privacywetgeving van toepassing, zodat de testresultaten mogelijk onrechtmatig waren verkregen. Omdat de sporter de leeftijd van 16 jaar nog niet had bereikt, kwam de vraag op tafel of de wettelijke vertegenwoordiger toestemming had moeten geven voor de test. Bovendien viel het nodige op te merken over de manier waarop de betrokken organisaties publiciteit hadden gegeven aan het positieve testresultaat.*
>
> *Uiteindelijk oordeelde de rechter in dit geval dat de gegevensverwerking rechtmatig had plaatsgevonden. Een flinke opluchting voor de Dopingautoriteit, want een ander oordeel zou haar taak behoorlijk hebben ondergraven. Tegelijkertijd bevestigt de uitspraak nog eens dat privacy-afwegingen een onderdeel moeten zijn van de besluitvorming. Het is goed om te zien dat NOC*NSF daar bijvoorbeeld op inhaakt met een communicatieplan voor dopingzaken.*

Het idee om een eigen privacy-handboek te publiceren bewijst dat Nederlandse sportbonden een proces van bewustwording doormaken. Daar moet direct bij worden opgemerkt dat dit boek op zichzelf uiteraard geen wondermiddel is waarmee je de organisatie snel en eenvoudig naar het gewenste *compliance*-niveau koerst (was dat maar zo). Er is immers lang niet altijd een pasklaar en eenduidig antwoord op dagelijkse vraagstukken: het opdoen van praktijkervaring zal nodig zijn om gevoel te krijgen voor het juist toepassen van de regels.

Dit handboek behandelt op laagdrempelige wijze de basisprincipes van het privacy-recht. Het is geschreven voor intern gebruik door sportbonden en NOC*NSF. Om de leesbaarheid te vergroten sluiten we daarbij aan bij de dagelijkse sportpraktijk, zodat vage begrippen hopelijk veranderen in begrijpelijke verplichtingen. Het handboek stimuleert daarmee niet alleen het bespreekbaar maken van privacy in alle Nederlandse sportbonden, maar ook het stellen van de juiste vragen.

Wij wensen je veel leesplezier.

© CMS Derks Star Busmann N.V., 2017

II. Hoe gebruik je dit handboek?

Indeling
Dit boek bestaat uit 11 hoofdstukken. Hoofdstuk 1 begint met een uitleg over de belangrijkste kernbegrippen uit het privacy-recht. Hoofdstuk 2 behandelt vervolgens de belangrijkste regels voor de omgang met persoonsgegevens. Daarna wordt in hoofdstuk 3 tot en met hoofdstuk 11 ingegaan op enkele praktijkthema's waar je als sportorganisatie zoal mee te maken krijgt.

Digitaal
Dit handboek is een digitale uitgave. De tekst bevat klikbare verwijzingen, waarmee je kunt navigeren tussen de verschillende plaatsen in het boek. Deze verwijzingen zijn steeds blauw onderstreept. Hier en daar wordt met hyperlinks verwezen naar externe bronnen.

Waar moet ik beginnen?
Dit handboek is zo opgezet dat het niet van voor naar achter hoeft te worden lezen. Ben je dus gericht op zoek naar informatie, kijk dan in de inhoudsopgave om op het gewenste onderdeel te klikken. Je kunt ook het trefwoordenregister raadplegen.

Is het privacy-recht geheel nieuw voor je, begin dan met lezen in hoofdstuk 1. We leggen daarin enkele kernbegrippen uit die je absoluut nodig hebt om met privacy-regels te kunnen werken. Ben je op zoek naar een algemeen overzicht van de privacy-regels, kijk dan in hoofdstuk 2.

Bijlagen
Dit handboek bevat ook een aantal bijlagen. Je kunt de daarin opgenomen modellen naar eigen wens gebruiken. Zorg wel dat je de toelichting bij de modellen goed bestudeert alvorens je ermee aan de slag gaat.

Symbolen en kaders
De symbolen die in dit handboek terugkeren hebben de volgende betekenis:

De kernboodschap van een hoofdstuk.

Let op! Hier wijzen we je op belangrijke valkuilen.

Theorie wordt regelmatig toegelicht door een voorbeeld.

Praktische tips voor de praktijk.

III. Voor bestuurders en managers: privacy management

Inleiding
Zoekt u op het internet naar privacy management, dan stuit u op bergen literatuur over het organiseren en uitvoeren van informatieprocessen. Zulke materie is niet terug te vinden in dit handboek. Dat is een bewuste keuze: privacy management is anno 2017 een vak apart, dat behoorlijk wat privacy-kennis vereist. Wij gaan er in dit handboek juist vanuit dat de lezer deze kennis nog niet bezit, en vooral de rode draad van het privacy-recht wil oppikken.

Een reden om toch kort stil te staan bij het 'managen' van privacy, is het hardnekkige misverstand dat privacy een kwestie is van het naleven van een paar spelregels. Die benadering is niet alleen onjuist, maar ook risicovol. Doet een incident zich eenmaal voor, dan is het kwaad vaak al geschied. Torenhoge boetes voor datalekken zijn vaak het schoolvoorbeeld, maar de gevolgen van slecht beleid zijn niet alleen financieel. U loopt tevens het risico op een serieuze vertrouwensbreuk met het publiek en op langdurige negatieve aandacht in de media.

Om te voorkomen dat uw organisatie achter de feiten aanloopt, zult u dus aan de slag moeten. Maar waar begint u?

Stap 1: wie doet wat?
Om als organisatie in de juiste richting te (blijven) bewegen moeten allereerst taken en verantwoordelijkheden in het leven worden geroepen. Dat begint formeel bij het bestuur en MT, die beslissen over de koers van de organisatie. Er zijn echter weinig personen die 'privacy' expliciet in hun portefeuille aantreffen. Als bestuurder bent u bovendien niet slechts op privacy gefocust, en schakelt u voor dit soort kwesties wellicht liever stafleden in. Dat laatste is bij privacy helaas om twee redenen niet zo eenvoudig:

1. Sportbonden beschikken doorgaans niet over personeel met privacy-expertise; en
2. Privacy duikt in allerlei vormen op in verschillende organisatieonderdelen, zodat het zich niet zonder problemen ergens laat parkeren bij één persoon (bijvoorbeeld een beleidsadviseur of een jurist).

De neiging om een 'ongrijpbaar' dossier zoals privacy weinig gerichte aandacht te geven is dan ook geen uitzondering. Ironisch genoeg dreigt daar echter het grootste risico, namelijk een *gebrek aan aandacht en bewustzijn* voor privacy compliance.

Om te bewaken dat er iets van de grond komt is het dus van groot belang dat een bestuurder of senior-staflid de uitdrukkelijke verantwoordelijkheid krijgt toebedeeld om het privacy-dossier op orde te brengen en te houden. Deze persoon moet vervolgens een antwoord formuleren op twee vragen:

- Handelt de organisatie in overeenstemming met de geldende eisen? (Stap 2)
- Zo nee, wat moet er dan gebeuren om dit alsnog te bereiken? (Stap 3)

© CMS Derks Star Busmann N.V., 2017

Stap 2: hoe staan we ervoor?
Het lezen van dit handboek geeft een aardig beeld van de belangrijkste eisen die aan uw sportorganisatie worden gesteld. Vervolgens wilt u natuurlijk weten of u aan die eisen voldoet. Maar hoe stelt u dat vast?

Om het niveau van privacy compliance te meten moet in ieder geval éérst worden achterhaald welke informatiestromen er zoal zijn binnen de organisatie. In privacy-jargon heet dat het 'analyseren van de verwerkingsprocessen'. Welke persoonsgegevens worden binnen welke afdelingen door wie gebruikt? Hoe vindt dat gebruik plaats? En voor welk doel wordt die informatie eigenlijk gebruikt?

Zijn de processen eenmaal in kaart gebracht (meestal via spreadsheets), dan kunnen de wettelijke eisen daar als het ware 'overheen' worden gelegd. Mogen de gegevens inderdaad voor het beoogde doel worden gebruikt? Worden ze niet te lang bewaard? Is de beveiliging op orde? Etc.

U zult al gauw merken dat u sommige zaken redelijk snel kunt afvinken, terwijl u bij andere kwesties geen idee hebt hoe daarmee te beginnen. Zo komt u er bijvoorbeeld snel achter of de website al dan niet een privacyverklaring heeft, maar het beoordelen van waarborgen in de contracten met IT-leveranciers is al een stuk ingewikkelder.

Als u ook nog eens bedenkt dat een organisatie continu in beweging is, dan begrijpt u waarom privacy compliance voortdurend aandacht nodig heeft. Zodra de organisatie immers nieuwe software aankoopt, een toernooi organiseert of een app wil lanceren, heeft dat allerlei implicaties voor de verwerkingsprocessen. Stap 2 ('hoe staan we ervoor?') is dus zeker geen eenmalige exercitie, maar stelt u doorlopend voor allerlei uitdagingen.

> **CMS Privacy Compliance Check**
> De advocaten van CMS zijn ervaren in het adviseren van sportorganisaties. Speciaal voor sportbonden voert CMS tegen een verlaagd tarief de zogeheten Privacy Compliance Check uit. In de Compliance Check onderzoekt CMS door middel van o.a. vragenlijsten en interviews in hoeverre de privacy-regels worden nageleefd. Daarbij is veel ruimte voor maatwerk: sportbonden mogen zelf bepalen waar de focus van het onderzoek ligt. Aan het einde van het onderzoek rapporteert CMS in begrijpelijke taal hoe de organisatie scoort op de belangrijkste risico's, en waar de kansen liggen voor verbetering. Op verzoek kan CMS bovendien direct helpen bij het doorvoeren van benodigde maatregelen.
>
> Benieuwd wat CMS voor uw organisatie kan betekenen? Neem gerust contact op voor een vrijblijvend gesprek.

Stap 3: risk based privacy compliance als uitgangspunt
Het doorlopen van stap 2 kan (zeker de eerste keer) een lange lijst van verbeterpunten opleveren.

Laat u hierdoor vooral niet ontmoedigen, en realiseer u dat 100% compliance van de totale organisatie in de praktijk niet bestaat. Een gezonde ambitie is wat ons betreft een benadering van ***risk based compliance.*** Dat houdt in dat u het beschikbare budget voor privacy compliance inzet om ***reële risico's*** op te sporen, te ontzenuwen of te beperken. Een goede uitvoering van stap 2 helpt daarbij: adresseer in eerste instantie de processen waarvan blijkt dat ze aanmerkelijke risico's bevatten.

Slot
Als er één boodschap is die we willen overbrengen, is het dat privacy compliance een permanent onderwerp moet zijn binnen iedere sportorganisatie. Besef echter ook dat privacy slechts een facet tussen meerdere belangen is. Voorkom dus dat u die andere belangen schade toebrengt met een te rigoureuze of ongeclausuleerde toepassing van wettelijke regels. De kunst is uiteindelijk om een scherp oog te ontwikkelen voor de daadwerkelijke risico's, zonder daarbij mooie initiatieven te hoeven torpederen. Met een flexibele houding zult u merken dat voor vrijwel ieder privacy-issue een oplossing bestaat.

Veel succes!

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 1: Kernbegrippen

In 't kort:

- Privacy is het recht om met rust gelaten te worden. Informationele privacy (of: de bescherming van persoonsgegevens) gaat over de vraag wat je wel/niet mag doen met informatie over een persoon. In dit handboek staat dat laatste centraal.
- De regels voor de bescherming van persoonsgegevens staan in de Wet bescherming persoonsgegevens (Wbp). De Wbp is zeer snel van toepassing, zodat je daarmee in de praktijk constant rekening moet houden. De belangrijkste begrippen uit de Wbp leggen we uit in dit hoofdstuk.
- Bijna alle verplichtingen uit de Wbp rusten op de 'verantwoordelijke'. Dat is degene die beslist over het doel van en de middelen voor de verwerking van persoonsgegevens. Ook jouw sportorganisatie is in veel gevallen verantwoordelijke.

1.1 Wat is privacy?

Het recht op privacy kun je eenvoudig uitleggen als het recht om met rust gelaten te worden. Het recht op privacy is in de meeste landen een grondrecht. Het wordt gezien als een basisvoorwaarde in een vrije samenleving, waarin mensen tot op zekere hoogte vrij kunnen kiezen hoe zij hun leven inrichten. Die vrijheid kun je op meerdere manieren benaderen:

1. Ruimtelijk: de vrijheid om zelf te bepalen waar je verblijft;
2. Lichamelijk: de vrijheid om zelf te beslissen over jouw lichaam;
3. Relationeel: de vrijheid om zelf te kiezen met wie je omgaat; en
4. Informationeel: wat mag een ander met jouw persoonlijke informatie?

Dit handboek staat volledig in het teken van dat laatste, namelijk *informationele privacy*, ook wel *de bescherming van persoonsgegevens* genoemd. Van de vier genoemde privacy-aspecten zal dit onderdeel het meeste terugkeren in de dagelijkse praktijk van jouw organisatie.

1.2 De Wet bescherming persoonsgegevens (Wbp)

Spreek je met iemand over (informationele) privacy, dan duurt het nooit lang voordat de term 'Wbp' voorbij komt, de afkorting voor *Wet bescherming persoonsgegevens*. Dat is logisch, want de Wbp is de bron van bijna iedere privacy-verplichting. Althans, tot mei 2018. Dan wordt de Wbp namelijk vervangen door Europese regels, die zijn opgenomen in de *Algemene Verordening Gegevensbescherming* (hierna spreken we over de "Verordening"). In deze brochure van CMS kun je alvast lezen welke gevolgen dit heeft voor de huidige regels. De tekst van de Verordening kun je hier raadplegen.

In dit handboek geven we uitleg over de regels van de huidige Wbp. Wil je deze regels daadwerkelijk kunnen toepassen, dan is enige basiskennis van de Wbp onmisbaar. We bedoelen daarmee niet dat je de Wbp van A tot Z moet doorspitten. Belangrijk is vooral dat je leert dat het in het privacy-recht gaat om een aantal kernbegrippen, die we hierna toelichten. Begrijp je eenmaal hun betekenis, dan ben je een heel eind op weg. De toekomstige Verordening kent gelukkig vrijwel dezelfde begrippen.

Let op!
in dit handboek nemen we om praktische redenen steeds aan dat de Wbp van toepassing is, en niet een buitenlandse wet. Toch is dat in de praktijk niet altijd vanzelfsprekend, bijvoorbeeld wanneer je te maken hebt met buitenlandse organisaties. Laat je daarom bij twijfel hierover altijd adviseren. Zo weet je zeker dat je de juiste wetten naleeft.

1.3 Het verwerken van persoonsgegevens

Om te weten of je rekening moet houden met de regels uit de Wbp, moet je vaststellen of de Wbp van toepassing is op wat je doet, of van plan bent om te doen. De Wbp is enkel van toepassing als er sprake is van een *verwerking van persoonsgegevens*.

Wat is een persoonsgegeven?

Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Het gaat dus ten eerste om álle informatie over een persoon. Het maakt niets uit of de informatie wel of niet 'privé', oud of nieuw, of misschien zelfs volstrekt onbelangrijk is. Een paar willekeurige voorbeelden van persoonsgegevens: voor- en achternaam, adres, telefoonnummer, lichaamslengte, hobby, land van herkomst, lidmaatschapsnummer, e-mailadres, locatie, haarkleur, dieetwens, outfit, favoriete film, etc.

Voorbeeld: mailadres bestuurslid
Een mailadres hoeft niet altijd een persoonsgegeven te zijn. Het is bijvoorbeeld onwaarschijnlijk dat het adres secretaris@sportbond.nl herleidbaar is tot een persoon. Heet de secretaris echter Jan de Vries en gebruikt hij daarvoor het adres jan.devries@sportbond.nl, dan is dat e-mailadres wel een persoonsgegeven.

Traditioneel denk je bij persoonsgegevens aan statische gegevens, maar ook gegevens over gedrag en zelfs voorspellingen daarover kunnen een persoonsgegeven zijn. Ook kun je denken aan allerlei metadata zoals de duur van een telefoongesprek, de locatie waarvandaan wordt gebeld, of een analyse van iemands fysieke inspanning. In een tijdperk van big data is dat belangrijk om je te beseffen. Gedragsgegevens en metadata worden door analyse namelijk steeds waardevoller, maar ook privacygevoeliger dan 'traditionele' persoonsgegevens.

Identificeerbaar

Een gegeven is pas een persoonsgegeven als dit herleidbaar is tot een persoon. Meestal is informatie eenvoudig gekoppeld aan een naam of aan een uniek nummer, zodat je een persoon direct kunt identificeren. Soms is identificatie weliswaar niet direct, maar wel indirect mogelijk. Denk bijvoorbeeld aan een teamfoto. Hoewel er misschien geen namen onder de foto staan, kun je daar met een eenvoudige zoekopdracht op internet meestal snel achter komen. De foto is dan alsnog een persoonsgegeven.

© CMS Derks Star Busmann N.V., 2017

Valt er écht niet te achterhalen op wie informatie betrekking heeft, dan is sprake van 'anonimiteit'. In theorie is de Wbp dan dus niet van toepassing. Je spreekt dan immers niet langer over een 'persoonsgegeven'. Vertrouw er echter niet zomaar op dat je de Wbp met een paar handigheidjes buitenspel zet. Het is tegenwoordig steeds lastiger (of zelfs onmogelijk) om te zorgen dat informatie in geen enkel opzicht meer is gelinkt aan een individu.

Voorbeeld: anonimiseren
Een bekend misverstand is het 'anonimiseren' door openbare informatie te linken aan een (lid)nummer in plaats van een naam. Zo'n nummer leidt soms namelijk eenvoudig terug naar een achternaam, zodat ook het nummer een persoonsgegeven is.

Let op!
We raden aan om informatie waarvan je *vermoedt* dat die herleidbaar is, te behandelen alsof het persoonsgegevens betreft.

Wanneer worden persoonsgegevens verwerkt?
Ook het begrip 'verwerken' is zeer breed. *Iedere* handeling met een persoonsgegeven is in de praktijk een verwerking. Denk dus aan het verzamelen, opslaan, bewaren, verplaatsen, wissen, doorsturen of aanpassen, maar ook aan het kwijtraken, lekken of manipuleren van persoonsgegevens, etc.

Voorbeeld:
De vereniging "Sportbond" neemt de persoonsgegevens van een nieuw lid ("Kees") op in het ledenbestand van Sportbond. De vereniging factureert Kees jaarlijks voor het lidmaatschapsgeld. Sportbond verstuurt bovendien maandelijks een nieuwsbrief aan Kees. De opname in het ledenbestand, de facturatie en de verzending van een nieuwsbrief zijn voorbeelden van een "verwerking" van persoonsgegevens.

Verwerkingen vinden in de praktijk niet alleen digitaal plaats, maar ook op papier. Als gegevens op papier worden gezet om in een bestand te worden opgenomen, is er ook sprake van een verwerking. Denk bijvoorbeeld aan de papieren leden-, personeels- en wedstrijdadministratie. Niet-elektronische verwerkingen die niet bestemd zijn om in een bestand te worden opgenomen (zoals een persoonlijke telefoonnotitie die je kort daarna weggooit) zijn strikt genomen geen *verwerking*. In de praktijk is dat onderscheid echter lastig te maken. Ben je dus van plan om een dergelijke notitie te bewaren, dan is het meestal verstandiger om aan te nemen dat er wel sprake is van een verwerking.

1.4 De betrokkene
De eerste belangrijke partij in het privacy-recht is de zogeheten betrokkene. Dit is namelijk de persoon op wie een persoonsgegeven betrekking heeft. Hij is dus uiteindelijk degene van wie de privacy moet worden beschermd.

Voorbeeld:
Kees wordt als lid opgenomen in het ledenbestand van Sportbond. Kees is betrokkene bij de verwerkingen van de persoonsgegevens die op hem betrekking hebben, zoals zijn naam, lidnummer, adres, geboortedatum en bankrekeningnummer.

Let op:
Alleen gegevens over *natuurlijke* personen zijn persoonsgegevens. Rechtspersonen zijn geen betrokkene. Rechtspersonen zijn bijvoorbeeld verenigingen die lid zijn van jouw sportbond.

1.5 De verantwoordelijke
Naast de vraag of de Wbp een rol speelt, wil je natuurlijk ook weten wie zich vervolgens aan welke regels moet houden. In de Wbp is dat steeds één figuur, namelijk degene die *beslist over het doel van en de middelen voor* een verwerking. De Wbp noemt deze figuur de *verantwoordelijke*. Je kunt de verantwoordelijke eigenlijk zien als de baas van een verwerking van persoonsgegevens: hij bepaalt *waarom* en *hoe* bepaalde gegevens wel of juist niet worden gebruikt.

Voorbeeld:
Sportbond is verantwoordelijke voor de verwerkingen die zij uitvoert met de persoonsgegevens van Kees. Sportbond bepaalt namelijk hoe en waarom bepaalde verwerkingen plaatsvinden (zoals ledenbeheer, facturatie en nieuwsvoorziening van leden).

Ook jouw sportorganisatie is in heel veel situaties 'verantwoordelijke', zoals in de verschillende hoofdstukken van dit handboek nog zal blijken.

Het is mogelijk dat dezelfde persoonsgegevens door meerdere partijen worden verwerkt voor verschillende doeleinden. Deze partijen zijn dan meestal ieder zelfstandig verantwoordelijke voor wat zij zélf met die persoonsgegevens doen.

Voorbeeld: meerdere sportorganisaties betrokken
De persoonsgegevens van Kees (zoals zijn e-mailadres) zijn vaak niet alleen bekend bij Sportbond, maar ook bij een sponsor, de lokale vereniging, NOC*NSF of een andere koepelorganisatie. Deze organisaties hanteren vaak een eigen doel bij het verwerken van die persoonsgegevens. Ieder van deze overige partijen blijft dus zelf verantwoordelijke, omdat zij zelf (en niet Sportbond) het doel en de middelen bij een verwerking vaststellen.

Let op!
Een sportbond is niet automatisch verantwoordelijke voor verwerkingen die plaatsvinden door derde partijen die dat doen voor hun eigen doeleinden, ook al heeft deze derde de persoonsgegevens wellicht verkregen via de sportbond.

© CMS Derks Star Busmann N.V., 2017

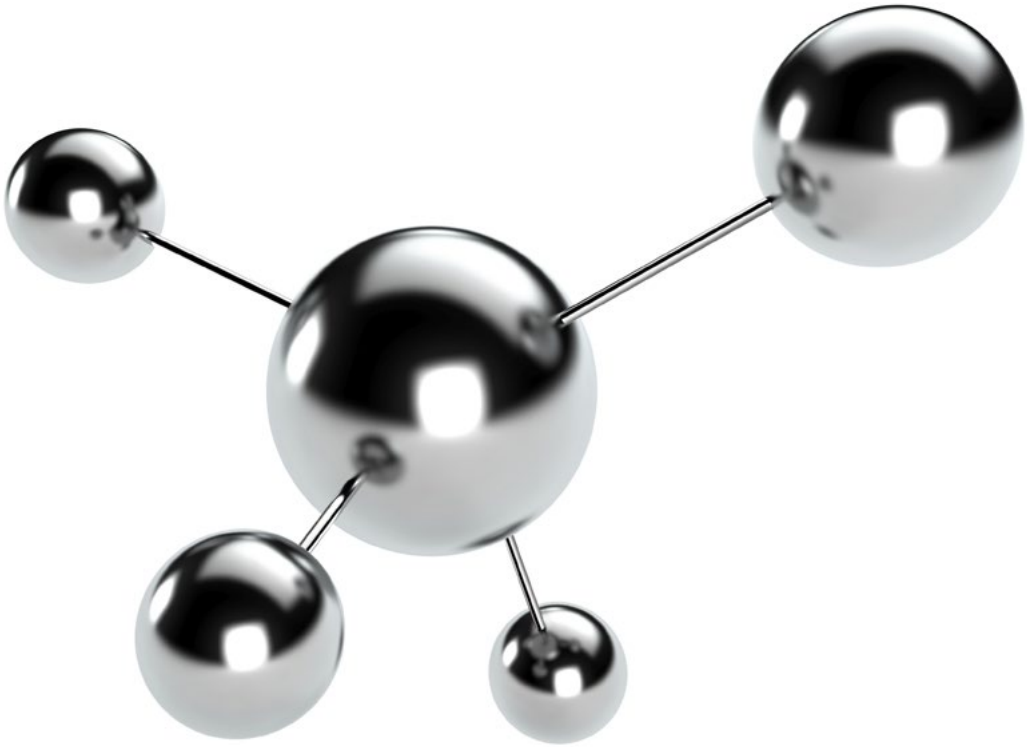
Vaak kun je makkelijk aanwijzen wie verantwoordelijke is, maar er zijn ook complexere gevallen. Soms zijn er bijvoorbeeld meerdere organisaties betrokken bij *dezelfde verwerking*. Je bent dan 'gezamenlijk verantwoordelijk' om de Wbp na te leven. Dat leidt snel tot onduidelijkheid over wie precies wat moet doen. Daarbij zijn partijen snel geneigd om deze lasten op elkaar af te schuiven. Doet zo'n situatie zich voor, laat je dan altijd adviseren door een privacy-deskundige. Je voorkomt daarmee het aangaan van onjuiste verplichtingen. Een deskundige kan meestal eenvoudig vaststellen waartoe je wel of niet verplicht bent.

1.6 De bewerker

Als verantwoordelijke voer je tegenwoordig veel werk uit via externe dienstverleners. Meestal gaat het dan om administratieve of bepaalde IT-diensten. Hierbij worden eigenlijk altijd wel op de een of andere manier persoonsgegevens verwerkt. Jij bepaalt als verantwoordelijke in dat geval weliswaar nog steeds het doel van de verwerking van die persoonsgegevens, maar de dienstverlener verzorgt (een deel van) de feitelijke uitvoering. Deze partij verwerkt dus persoonsgegevens ten behoeve van jou als verantwoordelijke. Zo'n dienstverlener heet in privacy-te*rmen een* bewerker.

Bewerkers hebben op grond van de huidige wetgeving nauwelijks eigen wettelijke plichten. Dit betekent dat je ontzettend goed moet oppassen dat je uitsluitend persoonsgegevens ter beschikking stelt aan betrouwbare dienstverleners. Gaat jouw leverancier op welke manier dan ook de fout in, dan kan jouw organisatie daar als verantwoordelijke uiteindelijk op worden aangesproken. Op dit moment moet je vooral onthouden dat je wettelijk verplicht bent om een bewerkersovereenkomst te sluiten. We komen daar in dit handboek nog regelmatig op **terug.**

Voorbeeld:
Sportbond neemt de persoonsgegevens van Kees op in een online ledenbeheersysteem. Dit systeem wordt aangeboden en gehost door een ICT-dienstverlener. Deze hosting vindt plaats door de ICT-dienstverlener ten behoeve van Sportbond (en niet voor eigen doeleinden van de ICT-dienstverlener). De ICT-dienstverlener is dus bewerker, en Sportbond is verantwoordelijke voor de verwerkingen die plaatsvinden met het ledenbeheersysteem. Sportbond moet een bewerkersovereenkomst sluiten met de ICT-dienstverlener.



© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 2: Basisregels

2.1 Doel en grondslag

2.1.1 Mag ik persoonsgegevens verwerken?

Persoonsgegevens mogen alleen worden verwerkt met een duidelijk omschreven en gerechtvaardigd doel. Die rechtvaardiging bestaat volgens de wet in zes gevallen, en noem je de grondslag van een verwerking.

In de thematische hoofdstukken van dit handboek lichten we nog regelmatig toe op basis van welke grondslag zoal persoonsgegevens mogen worden verwerkt.

2.1.2 Grondslagen

Een verwerking kan op zes manieren gerechtvaardigd zijn:

1. De verwerking is noodzakelijk om een gerechtvaardigd belang te behartigen
2. De betrokkene geeft uitdrukkelijk toestemming voor de verwerking
3. De verwerking is noodzakelijk in verband met een contract met de betrokkene
4. De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht
5. De verwerking is noodzakelijk om een vitaal belang van de betrokkene te beschermen
6. De verwerking is noodzakelijk om een publiekrechtelijke taak te vervullen

Stemt jouw beoogde doel niet overeen met minstens één van deze zes grondslagen, dan is de verwerking niet toegestaan.

Het kan natuurlijk voorkomen dat je dezelfde persoonsgegevens op meerdere manieren verwerkt voor diverse doelen. Zo wordt bijvoorbeeld een e-mailadres dikwijls gebruikt voor zowel facturatiedoeleinden (grondslag: contractuitvoering) als marketingdoeleinden (grondslag: toestemming).

Ook als je beschikt over een geldige grondslag om persoonsgegevens te verwerken, moet je goed blijven opletten dat je uitsluitend gegevens gebruikt die noodzakelijk en voldoende relevant zijn voor het doel waarvoor je verwerkt. Een bekende misser is bijvoorbeeld de verplichting om een digitale inschrijving te weigeren bij opengelaten optionele velden. Vermijd dit soort onhandigheden. Je wekt er namelijk wantrouwen en irritatie mee tegenover je publiek.

In de praktijk baseer je een verwerking meestal op (1) *een gerechtvaardigd belang*, (2) *toestemming*, (3) *contractuitvoering* of (4) een *wettelijke plicht*. We lichten deze grondslagen daarom hierna verder toe.

Let op!
Het is een misvatting dat toestemming altijd de meest veilige en geschikte grondslag is om persoonsgegevens te verwerken. Het tegendeel is waar: toestemming is in de praktijk vaak onhandig, al is het maar omdat een gegeven toestemming altijd (voor de toekomst) kan worden ingetrokken. Bestaat er een *andere* geschikte grondslag om je verwerking op te baseren, dan kun je het vragen van toestemming dus beter vermijden. Twijfel je of toestemming voor een bepaalde verwerking geschikt is? Vraag dan om deskundig advies.

2.1.3 Grondslag: gerechtvaardigd belang

Een ingewikkelde maar nuttige grondslag om persoonsgegevens te mogen verwerken, is die van het 'gerechtvaardigd belang'. Begrijp je eenmaal hoe je de aanwezigheid van een dergelijk belang goed onderbouwt, dan merk je dat deze grondslag geschikt kan zijn voor zeer uiteenlopende situaties waarin je persoonsgegevens verwerkt.

Wanneer heb je een gerechtvaardigd belang?
Het uitvoeren van veel activiteiten is lastig (of zelfs onmogelijk) zonder daarbij persoonsgegevens te verwerken. Slechts een aantal van die activiteiten worden gedekt door een specifieke grondslag (zoals toestemming of een contract, zie hiervoor). Er blijft dus een belangrijke restcategorie over van belangen die weliswaar niet *specifiek* door de wet worden genoemd, maar die de wetgever wél toelaat (vandaar de term 'gerechtvaardigd belang'). Ook in die gevallen mag je dus persoonsgegevens verwerken.

Enkele voorbeelden van een gerechtvaardigd belang

Verstrekking contactgegevens
Een organisatie mag bepaalde contactgegevens van cursisten verstrekken aan een opleider als dat nodig is om cursisten te kunnen contacteren in het kader van de opleiding.

Publicatie persoonlijk e-mailadres
Als een functionaris van een vereniging gebruikmaakt van een persoonlijk e-mailadres (in plaats van adres van de vereniging) en daarmee extern communiceert namens de vereniging, dan mag je dit persoonlijke e-mailadres publiceren voor contactdoeleinden (bijvoorbeeld op de website van de vereniging).

Monitoring ICT-gebruik
Werkgevers kunnen tot op zekere hoogte het ICT-gebruik van hun werknemers volgen om misbruik van het systeem te voorkomen.

Antecedentenonderzoek
Voor sommige functies heeft een werkgever een legitieme reden om een kandidaat te vragen om een Verklaring Omtrent Gedrag.

Gerichte aanbieding
Een webwinkel kan een bezoeker een gerichte aanbieding doen op basis van een eerdere aankoop of het huidige winkelmandje. Zo heeft iemand die ski's koopt wellicht ook interesse in skischoenen. Hij verwerkt dan aankoopinformatie (persoonsgegevens dus) voor een gerechtvaardigd commercieel belang.

© CMS Derks Star Busmann N.V., 2017

Het hoeft overigens niet altijd te gaan om het belang van de verantwoordelijke. Het mag ook gaan om een gerechtvaardigd belang van een *derde* aan wie jij de persoonsgegevens verstrekt.

Voorbeeld: onderzoeksbelang universiteit
Een sportbond kan onder bepaalde omstandigheden persoonsgegevens (zoals medische gegevens) verstrekken aan een universiteit in het kader van wetenschappelijk onderzoek (mits uiteraard is voldaan aan de vuistregels voor het delen van persoonsgegevens).

Is het belang voldoende gerechtvaardigd?
Stellen dat je een belang hebt is nog niet voldoende voor de conclusie dat sprake is van een 'gerechtvaardigd belang'. Tegenover dat belang staat namelijk altijd een privacybelang van de betrokkene. Hoe groter dat privacybelang van die betrokkene is, des te relevanter wordt de vraag of jouw belang daar tegenop weegt. Je bent dus verplicht om een goede *belangenafweging* te maken. Stel bij het maken van die afweging altijd de volgende vragen:

1. Is de verwerking écht nodig om het gestelde belang te behartigen, of bestaat er een alternatief waarbij het gebruik van persoonsgegevens achterwege kan blijven?
2. Op welke manier zou de privacy van de betrokkene aangetast kunnen worden door de verwerking?
3. Zijn er maatregelen mogelijk om de hiervoor genoemde aantasting weg te nemen of te verkleinen?
4. Weegt jouw belang, eventueel na de genoemde maatregelen, in dit specifieke geval voldoende op tegen het privacybelang van de betrokkene?

Luidt het antwoord op de laatste vraag ontkennend, dan is de beoogde verwerking onvoldoende gerechtvaardigd en mag deze dus niet plaatsvinden.

Voorbeeld: publicatie wanbetalers
Het is voor een vereniging belangrijk dat leden hun contributie (tijdig) betalen. Het is dan ook begrijpelijk dat een vereniging wanbetaling wil ontmoedigen. Dat mag echter niet plaatsvinden door een lijst van wanbetalers openbaar te maken (als een soort "wall of shame"). Een betrokkene kan door zo'n publicatie immers onevenredig in zijn reputatie worden aangetast, en daar zal het verenigingsbelang (tijdige betaling) niet tegen opwegen. Een geschikter en minder ingrijpend middel is om de wanbetaler persoonlijk te benaderen.

2.1.4 Grondslag: toestemming

Persoonsgegevens mogen ook worden verwerkt als de betrokkene daar voorafgaand aan de verwerking ondubbelzinnige toestemming voor geeft.

Let op!
Een groot misverstand is dat je veel privacy-regels kunt ontlopen zolang je de betrokkene maar om toestemming vraagt. Die gedachte is onjuist. Ook na het verkrijgen van toestemming moet je gewoon alle privacy-regels naleven.

Denk bijvoorbeeld aan de informatieplicht, beveiliging en bewaartermijnen. Het enige dat je dus via toestemming verkrijgt is het recht (lees: een geldige grondslag) om überhaupt bepaalde persoonsgegevens te mogen verwerken.

Voorbeelden: toestemming vereist
Reclamemails
Voor het gebruik van iemands e-mailadres om reclame te verzenden heb je vrijwel altijd toestemming nodig van de betrokkene. Let hier ook op de regels voor direct marketing.

Profilering
Voor het analyseren van iemands gedrag met behulp van persoonsgegevens (bijvoorbeeld door het gebruik van cookies of locatiegegevens) heb je vrijwel altijd toestemming nodig van de betrokkene. Let hier ook op de cookieregels.

Online publicatie
Voor het online publiceren van persoonsgegevens (bijvoorbeeld deelnemerslijsten of contactgegevens van leden) heb je in veel gevallen toestemming nodig van de betrokkene.

Gezondheidsgegevens
Voor het verwerken van gezondheidsgegevens is in veel gevallen toestemming nodig van de betrokkene.

Op informatie gebaseerd
Als je toestemming als grondslag gebruikt, moet voldoende duidelijk zijn waarvoor je toestemming vraagt. Vertel dus concreet voor welk(e) doel(en) je de persoonsgegevens verwerkt en voorkom vaag taalgebruik. Je hoeft daarbij niet te vervallen in onnodige details: teveel informatie is immers ook verwarrend. Gedetailleerde informatie kan je meestal beter opnemen in een privacyverklaring, die je op grond van de informatieplicht beschikbaar stelt.

Voorbeeld: vaag en algemeen taalgebruik
Wil je de naam van een deelnemer aan een opleidingsprogramma graag publiceren op de website van de opleider, vraag dan niet of hij akkoord gaat met "online publicatie" van "zijn gegevens", maar verzoek uitdrukkelijk om publicatie van zijn voor- en achternaam, en maak duidelijk om welke website het gaat.

Uitdrukkelijk
Je mag als verantwoordelijke niet uitgaan van een stilzwijgende toestemming. Je hebt uitdrukkelijke instemming nodig van de betrokkene. Die verklaring mag zowel mondeling als schriftelijk (papier of digitaal) zijn. Wij bevelen een schriftelijke verklaring (waar mogelijk) wel aan.

Voorbeeld: automatisch ingevulde vinkjes
Vraag je op digitale wijze toestemming waarbij de betrokkene een hokje moet aanvinken voor het geven van zijn toestemming? Zorg dan dat het vakje niet al bij voorbaat is aangevinkt, maar zorg dat de betrokkene dat zélf moet doen.

© CMS Derks Star Busmann N.V., 2017

Betrokkenen jonger dan 16 jaar

Is een betrokkene nog geen 16, dan kan deze formeel gezien niet zelf toestemming geven. Vraag in dat geval toestemming aan zijn wettelijk vertegenwoordiger, zoals een ouder of voogd.

Vrije wil

Toestemming moet zonder aanwezigheid van dwang zijn gegeven, oftewel: de betrokkene moet daadwerkelijk een keuze hebben. Je mag hem dus niet direct of indirect dwingen om gegevens te verstrekken.

Het komt vaak voor dat de betrokkene in een zwakke positie staat ten opzichte van de verantwoordelijke. Zo zijn bedrijven geneigd om in hun algemene voorwaarden te bepalen dat hun klanten met allerlei zaken instemmen, terwijl je op die voorwaarden als consument geen 'nee' kunt zeggen: het is immers slikken of stikken, waarbij de keuze is beperkt tot het niet kopen/afnemen van een dienst of product. Een dergelijke toestemming is in principe ongeldig, zodat op die grond geen persoonsgegevens mogen worden verwerkt.

Voorbeeld: live-registratie sportevenement

Stel dat toeschouwers van een sportevenement sporadisch in beeld komen bij live registraties, dan is het niet verstandig om in je ticketvoorwaarden te stellen dat de toeschouwer daar met de aankoop van een ticket mee instemt. Zou de toeschouwer immers weigeren, dan sneuvelt zijn recht om het evenement bij te wonen en is van een vrije keuze dus geen sprake. Dat betekent overigens niet dat je dergelijke opnamen niet mag maken; je kunt immers een andere grondslag gebruiken, namelijk die van een gerechtvaardigd belang. Het uitzenden van een evenement kan immers dienen om de bekendheid van een organisatie te vergroten, of media en fans in staat te stellen om het evenement te volgen. Zolang het voor een bezoeker maar duidelijk is dat hij kan worden gefilmd, wordt de privacy van een bezoeker daarmee doorgaans niet onevenredig aangetast.

Intrekking

Een betrokkene mag zijn toestemming voor een verwerking op ieder moment intrekken. Na de intrekking ben je niet langer bevoegd om de verstrekte gegevens te gebruiken. Dit kan in de praktijk onhandige gevolgen hebben. Zorg daarom dat verwerkingen, zeker als je daar in de toekomst erg afhankelijk van kan zijn, zoveel mogelijk zijn gebaseerd op een andere grondslag dan toestemming.

Documentatieplicht en bewijslast

Een verkregen toestemming moet je zorgvuldig documenteren. Als er later discussie ontstaat over de vraag of een betrokkene toestemming heeft gegeven, dan rust de bewijslast namelijk op de verantwoordelijke. In een digitale context (denk aan de aanmelding voor een reclamemail/evenement) kun je dit meestal eenvoudig oplossen door het gegeven akkoord te 'loggen' in het systeem.

Toestemming via een derde

Soms verkrijg je gegevens niet direct van een betrokkene, maar via een derde. Ga er in dat geval niet klakkeloos van uit dat deze derde namens jou de vereiste toestemming heeft gekregen van een betrokkene, maar ga na of degene van wie je de gegevens verkrijgt de verkregen toestemming kan aantonen.

2.1.5 Grondslag: overeenkomst

De verantwoordelijke mag persoonsgegevens ook verwerken als dat nodig is voor de uitvoering van een overeenkomst.

Voorbeeld: verzending clubblad

Als een betrokkene op grond van zijn lidmaatschap een clubblad ontvangt, dan mag de vereniging persoonsgegevens (namelijk adresgegevens) van de betrokkene gebruiken om het blad te kunnen toesturen.

De verantwoordelijke mag deze grondslag alleen gebruiken als de betrokkene zelf partij is bij de overeenkomst. De verantwoordelijke hoeft niet zelf partij te zijn bij de overeenkomst.

2.1.6 Grondslag: wettelijke plicht

De verantwoordelijke mag persoonsgegevens verwerken als dat nodig is om te voldoen aan een wettelijke plicht. Denk bijvoorbeeld aan personeels- of verkoopadministratie die plaatsvindt in het kader van inkomsten- en omzetbelasting. Een verantwoordelijke kan deze grondslag alleen gebruiken als de wettelijke plicht op hemzelf rust.

2.1.7 Doelbinding: gebruik voor andere dan oorspronkelijke doeleinden?

Het kan zo zijn dat de verantwoordelijke persoonsgegevens wil gebruiken voor een ander doel dan waarvoor deze oorspronkelijk zijn verzameld. Dat is in principe niet verboden, maar dan moet ook voor dat alternatieve doel wel een geldige grondslag bestaan. Er geldt bovendien nog een tweede eis, en dat is dat het nieuwe doel niet *onverenigbaar* mag zijn met het oorspronkelijke doel. We noemen dit het principe van *doelbinding*. De achtergrond hiervan is dat het hergebruik van op zichzelf rechtmatig verkregen informatie niet alsnog leidt tot onwenselijke aantasting van iemands privacy.

Wil je bepaalde persoonsgegevens op enig moment voor andere doeleinden gaan gebruiken, stel dan altijd de volgende vragen:

1. Bestaat er voldoende samenhang tussen het oorspronkelijke en nieuwe 'doel' waarvoor je de persoonsgegevens wil gebruiken? Onthoud daarbij dat wanneer de verwantschap tussen deze doelen kleiner is, er minder kans bestaat dat je de persoonsgegevens kunt 'hergebruiken'.
2. Zijn de gegevens niet te gevoelig om voor alternatieve doeleinden te gebruiken dan waarvoor ze oorspronkelijk zijn verkregen?
3. Kan worden uitgesloten dat er nadelige gevolgen voor de betrokkene zijn als ik de persoonsgegevens ga gebruiken voor het alternatieve doel?

© CMS Derks Star Busmann N.V., 2017

4. Is er voldoende gelegenheid om de betrokkene te informeren over het nieuwe doel, zodat een onwenselijk verrassingseffect achterwege blijft?

Is het antwoord op deze vragen hoofdzakelijk ontkennend, dan kan je vermoeden dat het alternatieve gebruik niet verenigbaar is met het doel waarvoor je de persoonsgegevens hebt verkregen.

Voorbeeld: sollicitatie oud-deelnemer
Stel je voor dat iemand solliciteert voor een trainersfunctie bij een sportbond. Wellicht ken je deze persoon al, omdat hij het jaar daarvoor toevallig deelnam aan een opleidingsprogramma van diezelfde bond. Het kan in die situatie verleidelijk zijn om voorafgaand aan het sollicitatiegesprek nog even te graven naar informatie die je destijds over de persoon in kwestie hebt verzameld. Toch is hier voorzichtigheid geboden. De sollicitant realiseert zich wellicht niet dat jij als potentiële werkgever al over dergelijke informatie beschikt. Het is bovendien niet ondenkbaar dat bepaalde opleidingsinformatie de kansen van de sollicitant negatief beïnvloedt, terwijl deze informatie wellicht een vertekend beeld schetst van de kandidaat. Je laat het graven naar zulke informatie daarom vaak beter achterwege.

2.2 Bewaren
Apparaten kunnen tegenwoordig grote hoeveelheden informatie opslaan. Dat maakt het soms verleidelijk om informatie eindeloos te bewaren. 'Je weet maar nooit' is daarbij een bekend argument. Toch geldt voor het bewaren van persoonsgegevens juist het tegenovergestelde. De verantwoordelijke mag persoonsgegevens namelijk niet langer bewaren dan noodzakelijk is voor het doel waarvoor je ze hebt verkregen. Bewaar je persoonsgegevens dus (bewust of onbewust) te lang, dan kan dit in strijd zijn met de wet.

2.2.1 Welke bewaartermijn moet ik hanteren?
Dat is volledig situatieafhankelijk en moet je als organisatie per onderwerp en per afdeling goed beoordelen. Dat vereist dus dat je eerst goed in kaart brengt welke persoonsgegevens in de gehele organisatie op welke wijze worden verwerkt. Vervolgens stel je per organisatieonderdeel vast welk doel wordt gediend met het bewaren van deze persoonsgegevens. Zolang dat doel nog actueel en relevant is, heb je meestal een legitieme reden om de gegevens te bewaren. Ontbreekt een geldig doel? Dan wordt het tijd om de gegevens te wissen of vernietigen.

Voorbeeld: dag-lid
Een dag-lid neemt in 2016 deel aan een sportwedstrijd. Ter afhandeling van de inschrijving beschik je wellicht over betaal-, contact- en bepaalde gezondheidsgegevens. Er is dan meestal geen reden om de gezondheidsgegevens na het evenement te bewaren. Voor het e-mailadres geldt eventueel dat je dit mag bewaren voor direct marketing (mits je aan de daarvoor geldende regels voldoet!), zodat je de persoon bijvoorbeeld kan benaderen voor de editie van 2017. Sommige betaalgegevens moet je voor fiscale regels misschien nog enkele jaren geadministreerd houden. Je ziet dus dat er verschillende bewaartermijnen kunnen gelden rondom één deelnemer aan één evenement.

Het is natuurlijk niet praktisch om telkens interne vragen te moeten beantwoorden over de toepasselijke termijn. Stel daarom voor alle vormen van gegevensverwerking een duidelijk bewaarbeleid op en zie vervolgens toe op de naleving daarvan. Je kunt dit trouwens vaak deels automatiseren via software die je nu al binnen de organisatie gebruikt. Bespreek deze mogelijkheden met je ICT-leverancier.

2.2.2 Wettelijke plicht
Soms heb je niet zozeer een eigen belang, maar wel een wettelijke plicht om gegevens te bewaren. Zo zijn bepaalde persoonsgegevens relevant voor de Belastingdienst en moeten deze daarom een aantal jaren worden bewaard op grond van belastingwetgeving. Dat geldt bijvoorbeeld bij verkoop- en personeelsadministratie. Bespreek dus per afdeling welke bewaarplichten mogelijk van toepassing zijn.

2.2.3 Langer bewaren voor historische, statistische of wetenschappelijke doeleinden
De wet schept een belangrijke uitzondering om persoonsgegevens langer te mogen bewaren dan noodzakelijk is voor het doel waarvoor ze oorspronkelijk zijn verkregen of verwerkt. Je mag persoonsgegevens namelijk langer bewaren als daarmee een historisch, statistisch of wetenschappelijk doel is gediend.

© CMS Derks Star Busmann N.V., 2017

Je moet wel zorgen dat de persoonsgegevens niet alsnog zomaar voor andere doeleinden uit het archief kunnen worden gehaald.

De begrippen 'historisch', 'statistisch' en 'wetenschappelijk' zijn nogal algemeen. Het is in de praktijk dan ook niet altijd duidelijk wat hier nu precies wel of niet onder valt. Om je op weg te helpen geven we drie voorbeelden waarin deze uitzonderingsgrond behulpzaam kan zijn.

Voorbeeld: clubhistorie
Verenigingen hechten er meestal waarde aan om een bepaald erfgoed van de club op te bouwen. Denk aan sportprestaties of fotomateriaal. Dat is in principe geen probleem, maar zorg dan wel dat er geen onnodige gegevens in de archieven belanden. Bovendien moet je voorkomen dat persoonsgegevens uit het archief later alsnog voor andere dan historische doeleinden worden gebruikt.

Voorbeeld: statistiek
Het kan voor een organisatie om allerlei redenen prettig zijn om bepaalde persoonsgegevens voor statistische doeleinden langer te bewaren. Dat is doorgaans geen probleem. Stel dan wel duidelijk vast welke persoonsgegevens daarvoor wel en niet noodzakelijk zijn, en voorkom ook hier dat jij of een derde de langer bewaarde gegevens alsnog voor *andere* doeleinden gaat gebruiken. Overweeg ook of het mogelijk is om de gegevens te anonimiseren of pseudonimiseren, zodat je de negatieve invloed op iemands privacy wegneemt of beperkt.

Voorbeeld: wetenschappelijk onderzoek
Het bijhouden van sportgerelateerde data resulteert vaak in bergen informatie die niet alleen interessant zijn voor de sporter en sportorganisaties, maar ook voor de wetenschap. Denk bijvoorbeeld aan medisch-wetenschappelijk onderzoek. Het is in principe toegestaan om dit soort persoonsgegevens om die reden langer te bewaren.

Hier geldt overigens wel dat het vaak om gezondheidsgegevens gaat. Het is daarom extra belangrijk dat je ook overweegt of het mogelijk is om de gegevens te anonimiseren of pseudonimiseren, zodat je de negatieve invloed op iemands privacy wegneemt of beperkt.

Twijfel je of je bepaalde gegevens langer mag bewaren dan noodzakelijk? Vraag dan altijd om deskundig advies.

2.2.4 Vrijstellingsbesluit als hulpmiddel
Op dit moment bepaalt de Wbp nog dat je verwerkingen vooraf (via een formulier) moet aanmelden bij de Autoriteit Persoonsgegevens. Veel soorten verwerkingen zijn echter uitgezonderd van deze plicht. Deze uitzonderingen staan in het zogeheten *Vrijstellingsbesluit*. Daarin staat met zoveel woorden dat je bepaalde verwerkingen niet hoeft aan te melden, mits je de persoonsgegevens niet langer bewaart dan een specifieke periode. Het Vrijstellingsbesluit geeft per onderwerp (bijvoorbeeld leden, personeel, ICT en beveiliging) concrete termijnen.

De aanmeldplicht verdwijnt in 2018 met de inwerkingtreding van de Verordening, en wordt nu al niet meer gehandhaafd door de Autoriteit Persoonsgegevens. Toch biedt het Vrijstellingsbesluit handige inspiratie om te beslissen welke bewaartermijn je gebruikt als uitgangspunt. We adviseren je dan ook om het Vrijstellingsbesluit eens door te nemen. Het besluit bevat bijvoorbeeld indicaties voor termijnen bij:

- Lidmaatschap en begunstiging
  (o.a. verenigingen)
- Arbeid en pensioen
  (o.a. sollicitanten, uitzendkrachten, personeels- en salarisadministratie)
- Goederen en diensten
  (o.a. klantgegevens)

Verzamel enkel noodzakelijke gegevens
Hoe meer informatie je verzamelt over een betrokkene, des te ingewikkelder het is om de juiste bewaartermijnen uit elkaar te houden. Maak het jezelf dus eenvoudig door niet méér persoonsgegevens te verzamelen dan strikt noodzakelijk is om het doel te bereiken.

2.3 Bijzondere persoonsgegevens
De wet maakt een onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens. Bij het verwerken van bijzondere persoonsgegevens ontstaan extra privacy-risico's. Daarom bestaan hiervoor strengere regels.

Het is *verboden* om bijzondere persoonsgegevens te verwerken, tenzij er een wettelijke uitzondering van toepassing is die de verwerking rechtvaardigt. Welke uitzondering van toepassing is, hangt mede af van het soort bijzondere persoonsgegevens dat je verwerkt.

2.3.1 Wat zijn bijzondere persoonsgegevens?
De wet noemt als bijzondere persoonsgegevens de gegevens over iemands:

- godsdienst of levensovertuiging;
- strafrechtelijke gegevens;
- ras;
- politieke gezindheid;
- gezondheid;
- seksuele leven; en
- lidmaatschap van een vakbeweging.

Op een directe of indirecte manier bijzonder
Persoonsgegevens kunnen direct, maar soms ook op een indirecte manier 'bijzonder' zijn. Een direct bijzonder persoonsgegeven is bijvoorbeeld een medisch rapport. Op een *indirecte* manier kunnen een voor- of achternaam op een lijst van personen met diabetes een bijzonder persoonsgegeven zijn. Doordat een naam op zo'n lijst staat, zegt dat namelijk indirect iets over iemands gezondheidstoestand. Hetzelfde geldt voor een ledenlijst van een sportvereniging die zich richt op een bepaalde levensovertuiging, of op personen die een bepaalde applicatie

© CMS Derks Star Busmann N.V., 2017

downloaden die is gericht op mensen met een afwijking of ziekte. Let dus goed op de context van de informatie om te zien of op enige manier sprake kan zijn van bijzondere persoonsgegevens.

Niet bijzonder, maar wel gevoelig

Dat sommige persoonsgegevens niet 'bijzonder' zijn, wil nog niet zeggen dat ze niet alsnog zeer *gevoelig* kunnen zijn. Zo worden als extra gevoelig aangemerkt:

- gegevens over iemands financiële of economische situatie;
- gegevens die kunnen worden misbruikt voor (identiteits-)fraude (bijv. Burger Service Nummer, kopieën van identiteitsbewijzen, etc.);
- gegevens die onder een geheimhoudingsplicht vallen;
- gegevens die tot stigmatisering of afpersing kunnen leiden (denk aan gokverslaving, werk- of relatieproblemen, etc.); en
- inloggegevens (wachtwoorden, gebruikersnamen).

Hoewel voor deze gevoelige gegevens geen algemeen verbod geldt om ze te verwerken (zoals dat wél geldt bij bijzondere persoonsgegevens), moet je met dit soort gegevens heel voorzichtig zijn! Denk bijvoorbeeld aan de manier waarop je de informatie beveiligt, maar ook hoelang je deze bewaart en voor welk doel je deze gebruikt.

Burger Service Nummer

Het verwerken van het Burger Service Nummer (BSN) is in principe verboden, tenzij de wet dit expliciet toestaat of verplicht. Daar is slechts in een beperkt aantal gevallen sprake van. Kijk voor meer informatie in de Richtsnoeren van de Autoriteit Persoonsgegevens.
Het maken van een kopie van iemands paspoort of identiteitskaart (waarop een BSN staat afgebeeld) is een vorm van verwerking, en valt dus ook onder het verbod. Wat wel mag, is verzoeken of iemand zich kan legitimeren door zijn document te *tonen*. In dat geval is namelijk geen sprake van een verwerking.

2.3.2 Wanneer mag ik bijzondere persoonsgegevens verwerken?

Er bestaan veel wettelijke uitzonderingen op het verwerkingsverbod voor bijzondere persoonsgegevens. Daarbij gelden de vuistregels dat bijzondere persoonsgegevens slechts mogen worden verwerkt:

- door degenen die door hun *taak* een erkend belang hebben bij dat soort gegevens (bijvoorbeeld verzekeraar, medisch specialist, hulpverlener, school, werkgever, etc.); of
- als het *doel* vereist dat het betreffende bijzondere persoonsgegeven wordt verwerkt (bijvoorbeeld identificatie, opsporing of verdenking van strafbare feiten (denk aan camera-toezicht), of de screening van een potentiële werknemer of vrijwilliger).

Daarnaast zijn er een paar *algemene* uitzonderingen op grond waarvan je bijzondere persoonsgegevens mag verwerken:

- de betrokkene geeft toestemming voor de verwerking;
- de betrokkene maakt de gegevens zelf duidelijk openbaar;
- de gegevens zijn nodig voor het voeren van een juridische procedure; of
- de verwerking is van vitaal belang voor de betrokkene of een derde, waarbij het vragen van toestemming onmogelijk blijkt.

2.3.3 Gezondheidsgegevens

Een voor de sportwereld belangrijke categorie bijzondere persoonsgegevens is de informatie over iemands gezondheid. Uit een rapport van de Autoriteit Persoonsgegevens over de Nike+ Running App (een hardloop-app) blijkt dat je het begrip 'gezondheidsgegevens' ruim moet opvatten. Volgens de Autoriteit gaat het niet alleen om informatie uit medisch onderzoek, maar om alle gegevens over iemands geestelijke of lichamelijke gezondheid. Ook gegevens over rook- en drinkgedrag, allergieën, lidmaatschap van een patiëntenhulpgroep of dieetclub zijn een gezondheidsgegeven.

Het verwerken van gezondheidsgegevens is (net als andere bijzondere persoonsgegevens) in principe verboden. Een paar uitzonderingen op dit verbod luiden als volgt:

- Hulpverleners, gezondheidszorg-instellingen en maatschappelijke-dienstverleners mogen gezondheidsgegevens verwerken voor zover dat nodig is voor goede behandeling, verzorging, of het beheer van hun praktijk;
- Verzekeraars mogen gezondheidsgegevens verwerken voor risicobeoordeling en voor het uitvoeren van een overeenkomst;
- Scholen mogen gezondheidsgegevens verwerken voor speciale begeleiding van leerlingen;
- Jeugdwet-gerelateerde instellingen mogen gezondheidsgegevens verwerken voor zover dit nodig is voor hun taken;
- Bestuursorganen, pensioenfondsen, werkgevers (of daaraan verwante instellingen) mogen gezondheidsgegevens verwerken voor de uitvoering van wettelijke voorschriften, pensioenregelingen of cao's, en voor de re-integratie van zieke werknemers.

Zoals je ziet kom je als sportbond dus niet een aanmerking voor een specifieke uitzondering om gezondheidsgegevens te mogen verwerken. Dat betekent dat je in de praktijk in veel gevallen toestemming nodig zult hebben om gezondheidsgegevens te verwerken. Sportartsen hebben hier, in hun hoedanigheid van arts, uiteraard een andere positie.

Voorbeelden gezondheidsgegevens

Artsen

Een sportarts of andere medisch specialist verwerkt bij het behandelen of keuren van sporters altijd gezondheidsgegevens. Hij doet dit om zijn taak te kunnen uitoefenen. De arts mag voor dit doel gezondheidsgegevens verwerken, mits hij deskundig en onafhankelijk is. Daarnaast moet hij zich aan speciale regels voor geneeskundige behandelingsovereenkomsten houden. Deze regels laten we in dit boek buiten beschouwing. De arts of medisch specialist mag gezondheidsgegevens niet zonder uitdrukkelijke toestemming van de sporter verstrekken aan de sportbonden. De sportbond voert namelijk niet zelf de behandeling uit en heeft geen noodzaak bij het verwerken van de gegevens.

© CMS Derks Star Busmann N.V., 2017

Apps
Als de sportbond een app laat ontwikkelen waarmee gezondheidsgegevens van sporters worden verwerkt, dan is de sportbond mogelijk verantwoordelijke. Eventuele derden (zoals een IT-dienstverlener) is daarbij bewerker. Allereerst moet de sportbond zorgen voor de juiste grondslag om gezondheidsgegevens te mogen verwerken. Waarschijnlijk is in dit geval uitdrukkelijke toestemming van de app-gebruiker nodig. Die toestemming wordt verkregen door de gebruiker duidelijk te informeren over hoe hij die toestemming geeft (en weer kan intrekken), over hoe de app werkt en over welke persoonsgegevens door welke partijen worden verwerkt. Algemene informatie over het verwerken van persoonsgegevens wordt meestal verstrekt via een privacyverklaring. Daarnaast moet de sportbond met de IT-dienstverlener een bewerkersovereenkomst sluiten, waarin beveiliging (gezien de gevoeligheid van de gegevens) extra aandacht verdient.

Sportbond als werkgever
Ook als de sportbond als werkgever optreedt, dan mag de bond maar in een paar gevallen gezondheidsgegevens van personeel verwerken. Dit zijn echter zeer specifieke gevallen die we in dit handboek buiten beschouwing laten. De werkgever mag echter in principe niet de fitheid van zijn werknemers monitoren door ze wearable devices (zoals stappentellers) te laten dragen. Dit mag zelfs niet als de werknemer toestemming geeft, zo stelt de Autoriteit Persoonsgegevens. Wil je dus zulke gadgets verstrekken, zorg dan dat je als werkgever op geen enkele wijze betrokken raakt bij het gebruik ervan. Bij topsport is sprake van een andere situatie.

2.4 Beveiliging

De verantwoordelijke moet veilig omgaan met persoonsgegevens. Als persoonlijke informatie spoorloos raakt, eindeloos bewaard blijft of zelfs wordt gestolen, dan kan dat zeer vervelende gevolgen hebben voor de privacy van een betrokkene.

Informatiebeveiliging is een complex onderwerp, waarvan privacy slechts één stukje van de puzzel vormt. Wij beperken ons in dit handboek daarom tot de wettelijke beveiligingseis rondom *persoonsgegevens*.

Tip
De Autoriteit Persoonsgegevens heeft in 2013 de *Beleidsregels beveiliging persoonsgegevens* gepubliceerd. Wij bevelen sterk aan om dit document eens rustig te bestuderen, nu het onderwerp informatiebeveiliging daarin helder wordt uitgelegd.

2.4.1 Waar moet ik tegen beveiligen?

Een bekend misverstand is dat informatiebeveiliging enkel ziet op anti-diefstal. Beveiliging gaat namelijk ook over het vermijden van 'ongelukjes'. We verwezen al naar het verliezen van data, maar ook het gebruik van verkeerde persoonsgegevens kan een beveiligingsprobleem vormen. Je moet volgens de wet beveiligen tegen iedere vorm van onrechtmatige verwerking!

2.4.2 Wat zijn 'passende' beveiligingsmaatregelen?

De wet geeft slechts een algemene omschrijving van de beveiligingsplicht, namelijk dat de verantwoordelijke 'passende technische en organisatorische maatregelen' moet nemen om onrechtmatige verwerking te voorkomen.

Om te bepalen welke maatregelen 'passend' zijn, moet je in de eerste plaats weten *waartegen* je beveiligt. Je voert daarom allereerst een risicoanalyse uit, waarbij je in ieder geval let op:
- de gevoeligheid van bepaalde persoonsgegevens;
- de soort onrechtmatige verwerking die zich kan voordoen bij die persoonsgegevens; en
- de feitelijke kans dat het risico daadwerkelijk intreedt.

Privacy Impact Assessment: In de praktijk wordt bij het maken van een risicobeoordeling veel gebruik gemaakt van een zogeheten privacy impact assessment ('PIA'). In deze bijlage behandelen we enkele veelvoorkomende vragen over de PIA. Let op: In 2018 wordt het uitvoeren van een PIA in veel gevallen wettelijk verplicht!

Zijn de risico's eenmaal in beeld, dan moet je overwegen welke maatregelen deze risico's kunnen voorkomen of beperken. Je let daarbij zowel op:
- Effectiviteit: in welke mate neemt het risico door deze maatregel daadwerkelijk af?
- Efficiëntie: hoeveel inspanning en geld kost de maatregel?

Maatregelen zijn zowel technisch als organisatorisch van aard: je moet daarom steeds de juiste combinatie vinden om daadwerkelijk tot een veilige situatie te komen. Zo is een sterk wachtwoord bijvoorbeeld zinloos als dit vervolgens door de gebruiker op een post-it naast zijn computer wordt geplakt.

Voorbeeld: beveiligingsmaatregelen
Technisch:
- o Toegangscodes
- o Encryptie
- o Antivirus
- o Software-updates
- o Aanvalsdetectie

Organisatorisch:
- o Toegangsniveaus
- o Protocollen voor incidenten
- o Geheimhouding

2.4.3 Wat als wij geen kennis in huis hebben?

Het zelfstandig uitvoeren van een PIA is als sportorganisatie nog redelijk te overzien. De informatiebeveiliging vervolgens daadwerkelijk naar een hoger niveau brengen vraagt echter om meer expertise. Heb je die niet in huis? Schakel dan een deskundige in.

© CMS Derks Star Busmann N.V., 2017

Een gebrek aan kennis, uitbesteding van taken bij een derde of simpelweg een gebrek aan incidenten is absoluut geen excuus om informatiebeveiliging links te laten liggen. Je wordt als verantwoordelijke geacht om je zaken goed op orde te hebben.

Informatiebeveiliging bij leveranciers en partners

Beveiligingsmaatregelen in jouw eigen organisatie hebben weinig zin als de persoonsgegevens alsnog worden blootgesteld aan risico's bij doorgifte aan leveranciers en partners. Is jouw leverancier of partner een bewerker, dan ben je wettelijk verplicht om in de bewerkersovereenkomst specifieke afspraken te maken over het niveau van informatiebeveiliging.

Tips

- Informatiebeveiliging vraagt om een proactieve houding. Doet een incident zich eenmaal voor, dan is het kwaad vaak al geschied. Wees daarom bijzonder alert op nonchalance in de organisatie. Bij het horen van de volgende clichés moeten direct alarmbellen gaan rinkelen:
  "Dit regel je maar met de IT-ers"
  "Wij hebben nog nooit issues gehad; er is dus geen risico"
  "Niemand in onze branche trekt zich hier iets van aan"
- Informatiebeveiliging vraagt, net als privacy, om een zekere mate van management. Het raakt de *gehele* organisatie, en heeft daarom recht op rechtstreekse aandacht vanuit het bestuur. Dump het onderwerp informatiebeveiliging dus niet bij 'de IT' (als je daar als sportbond überhaupt al over beschikt) en ga samen aan de slag om tot een integraal beveiligingsplan te komen.
- Evalueer je beveiliging regelmatig. De beveiliging van vandaag dekt lang niet altijd de uitdagingen van morgen.

2.5 Meldplicht datalekken

2.5.1 Wat is een datalek?

De verantwoordelijke is verplicht om passende maatregelen te nemen om persoonsgegevens goed te beveiligen. Sinds begin 2016 kennen we in Nederland de *meldplicht datalekken*. Dat betekent dat je als verantwoordelijke onder bepaalde voorwaarden inbreuken op de beveiliging moet melden aan de Autoriteit Persoonsgegevens, en soms ook aan de betrokkene.

Wanneer de beveiliging (i) niet goed functioneert of (ii) ontoereikend is geweest spreken we van een inbreuk op de beveiliging. Van een inbreuk op de beveiliging is óók sprake als de beveiliging op zich in orde is, maar desondanks wordt omzeild.

Een ***inbreuk op de beveiliging***, oftewel een *beveiligingslek*, is ***niet hetzelfde*** als een ***datalek***.

Je spreekt pas van een datalek wanneer er daadwerkelijk negatieve gevolgen zijn voor de persoonsgegevens die worden verwerkt, of wanneer die gevolgen redelijkerwijs niet uit zijn te sluiten.

2.5.2 Moet ik melden aan de Autoriteit Persoonsgegevens?

Bijna ieder beveiligingsincident waar persoonsgegevens bij zijn betrokken, draagt een zekere mate van risico in zich. Toch hoeft niet ieder incident te worden gemeld. Pas als een inbreuk op de beveiliging een *aanzienlijke* kans geeft op *ernstige nadelige* gevolgen voor de bescherming van persoonsgegevens, moet deze inbreuk worden gemeld aan de Autoriteit Persoonsgegevens. Die melding moet "onverwijld" plaatsvinden, waarmee wordt bedoeld dat dit zonder vertraging moet gebeuren.

Er zijn 3 vragen die je moet stellen als blijkt dat sprake is van een mogelijk incident:

1. Is er een technische of organisatorische inbreuk op getroffen beveiligingsmaatregelen geweest? Zo ja, ga door naar vraag 2.
2. Heeft de inbreuk tot gevolg dat persoonsgegevens zijn blootgesteld aan een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens (lees: een risico op verlies of onrechtmatige verwerking)? Zo ja, ga door naar vraag 3.
3. Zijn de feiten en omstandigheden zodanig dat de aanzienlijke kans op deze nadelige gevolgen redelijkerwijs aanwezig is of moet worden verondersteld? Zo ja, dan moet in principe een melding aan de Autoriteit Persoonsgegevens plaatsvinden.

2.5.3 Moet ik melden aan de betrokkene?

Een datalek dat moet worden gemeld aan de Autoriteit Persoonsgegevens, moet soms ook worden gemeld aan de betrokkenen zelf – de personen van wie data is gelekt. Dat moet wanneer het datalek *waarschijnlijk ongunstige gevolgen* heeft voor de *privacy* van die personen. Ook hier geldt dat de melding "onverwijld" moet gebeuren.

Voor de afweging of betrokkenen moeten worden geïnformeerd, is het aantal betrokkenen niet van doorslaggevend belang. De aard en omvang van het incident zelf zijn echter wel belangrijk. Als gevoelige gegevens zijn gelekt dan moeten de betrokkenen bijna altijd worden geïnformeerd. Er is echter een belangrijke uitzondering: betrokkenen hoeven *niet* te worden geïnformeerd als de gelekte gegevens op een passende manier zijn beveiligd, zodat onbevoegden de gegevens niet kunnen inzien. Denk hierbij aan beveiligingsmaatregelen zoals *encryptie* of *hashing*. De vermoedelijke risico's van het lek moeten wel altijd in kaart worden gebracht. Het is belangrijk om te beseffen dat deels versleutelde gegevens, of versleuteling op een achterhaalde wijze, géén passende beveiligingsmaatregelen zijn.

Enkele voorbeelden

- Het *verlies* van persoonsgegevens kan resulteren in een datalek. Bij verlies zijn persoonsgegevens bijvoorbeeld gewist of verloren gegaan. Als er geen back-up beschikbaar is, dan kan het zijn dat zo'n incident moet worden gemeld aan de Autoriteit Persoonsgegevens. Onder "verwerken" valt namelijk ook het onbedoeld of onrechtmatig vernietigen en uitwissen van gegevens, zodat de meldplicht van toepassing is. Een veelvoorkomend geval is bijvoorbeeld het verlies van een onbeveilig de laptop waarop klantgegevens staan zoals betalingsgegevens, adresgegevens, e-mailadressen en medische gegevens. Een dergelijk datalek zal moeten worden gemeld aan de Autoriteit Persoonsgegevens en aan de betrokkenen.

© CMS Derks Star Busmann N.V., 2017

- Een kliniek stuurt per e-mail een nieuwsbrief naar ernstig zieke patiënten met dezelfde aandoening zonder de lijst van ontvangers onzichtbaar te maken (te "BCC'en"). Dit is een inbreuk op de organisatorische beveiliging. Door de context waarin de e-mail adressen worden gebruikt is er bovendien vaak sprake van gevoelige gegevens. Het datalek moet in dit geval waarschijnlijk worden gemeld aan de Autoriteit Persoonsge gevens en aan betrokkenen, omdat er voor de betrokkenen mogelijk ongunstige privacy-gevolgen zijn.
- Als een organisatie te maken krijgt met *malware*, kunnen computerbestanden worden aangetast. Het kan bijvoorbeeld gebeuren dat bestanden worden 'gegijzeld', zodat ze niet meer beschikbaar zijn. Er is dan sprake van een datalek, omdat de persoonsgegevens onrechtmatig zijn verwerkt of zijn aangetast. Bovendien zijn de bestanden mogelijk aan onbevoegden beschikbaar gesteld. Het incident zal waarschijnlijk aan de Autoriteit Persoonsgegevens moeten worden gemeld. Of ook betrokkenen op de hoogte moeten worden gebracht is afhankelijk van de vraag of een onbevoegde derde de mogelijkheid heeft gehad om de gegevens te raadplegen, en dat een benutting van die mogelijkheid redelijkerwijs niet kan worden uitgesloten.

Tips

- De Autoriteit Persoonsgegevens heeft beleidsregels opgesteld voor de omgang met datalekken. Daarin staan stroomschema's die stapsgewijs ingaan op de beoordeling van beveiligingsincidenten. Voor het gemak zijn twee van deze stroomschema's opgenomen als bijlage.
- Een datalek kan worden gemeld op deze webpagina van de Autoriteit Persoonsgegevens.
- Heb je geen eigen expertise in huis om de omgang met datalekken af te handelen, schakel dan onmiddellijk een deskundige in. Het Data Protection & Privacy Team van CMS staat klaar om alle benodigde hulp te leveren bij het afhandelen van incidenten.
- Het registreren (*loggen*) van informatie over wie op welk moment toegang heeft ge had tot informatie kan je helpen om de omvang van een risico te kunnen inschatten.
- Maak in de bewerkersovereenkomst duidelijke afspraken over de beveiliging tegen en het melden van datalekken. Je wil soms bijvoorbeeld voorkomen dat bewerkers zelfstandig contact opnemen met de Autoriteit Persoonsgegevens en betrokkenen.
- Zorg dat iedereen binnen je organisatie (i) veilig met ICT omgaat en (ii) weet hoe er moet worden gehandeld zodra een vermoeden bestaat van een beveiligingsincident. Menselijke fouten zijn een belangrijke aanleiding voor (de escalatie van) datalekken. Je kunt eventueel het modelprotocol uit dit handboek gebruiken.
- Stel een intern team samen dat wordt opgeroepen zodra zich een incident voordoet. Leg de werkafspraken vast in een protocol. Een model hiervoor is in dit handboek opgenomen als bijlage.
- Onderzoek bij een incident zo snel mogelijk hoe je maatregelen kan treffen die de schade kunnen beperken.

2.6 Bewerkers en de bewerkersovereenkomst

2.6.1 Wat is een bewerker?

Een organisatie die verantwoordelijke is, maakt vaak gebruik van allerlei externe dienstverleners. Denk bijvoorbeeld aan salarisadministratie, het beheer van apps, het hosten van websites of de afhandeling van ticketverkoop. Bij de uitvoering van zulke diensten zijn vrijwel altijd persoons-gegevens betrokken. Jij bepaalt als verantwoordelijke dan weliswaar nog steeds het doel van de verwerking van die persoonsgegevens, maar de dienstverlener verzorgt de feitelijke uitvoering. Deze partij verwerkt dus persoonsgegevens ten behoeve van de verantwoordelijke. Zo'n dienstverlener heet in privacy-termen een bewerker.

Verantwoordelijke of bewerker?

Het is niet altijd duidelijk of je voor een bepaalde verwerking verantwoordelijke of bewerker bent. Zo neemt een dienstverlener een proces soms zodanig over, dat je als verantwoordelij-ke nauwelijks kunt overzien wat een dienstverlener precies uitspookt. Denk bijvoorbeeld aan IT-leveranciers, waarbij je als niet-deskundige al snel geneigd bent om blind te vertrouwen op de leverancier. Dat kan zo ver gaan, dat de dienstverlener in belangrijke mate controle (ver)krijgt over het verwerkingsproces. In dat geval is de leverancier mogelijk een *verantwoordelijke* in plaats van bewerker, waardoor de juridische rollen en verplichtingen anders kunnen liggen dan je wellicht verwacht. Laat je bij twijfel in dit soort scenario's tijdig adviseren door een deskundi-ge! Verkeerde inschattingen over je juridische rol en rechtspositie kunnen leiden tot wetsovertre-dingen en aanzienlijke aansprakelijkheid.

2.6.2 Bewerkersovereenkomst

De meeste privacy-regels uit de Wbp gelden op dit moment (2017) enkel voor de verantwoorde-lijke, óók indien deze een bewerker inschakelt. Het idee hierachter is dat een verantwoordelijke zich nooit mag verschuilen achter eventuele fouten van een bewerker, die in feite 'onderaanne-mer' is. Je moet dus vooraf regelen dat een bewerker nauwkeurig de regels naleeft, waarop jij als verantwoordelijke uiteindelijk wordt aangesproken.

Je bent als verantwoordelijke wettelijk ***verplicht*** om met bewerkers een zogeheten 'bewerker-sovereenkomst' te sluiten. Een goede bewerkersovereenkomst schept een duidelijke taakverde-ling en zorgt vooral dat je als verantwoordelijke voldoende grip houdt op de bewerker.

Let op!

De Verordening stelt ten opzichte van de Wbp meer en hogere eisen aan de inhoud van bewerkersovereenkomsten. Dit heeft voor veel huidige bewerkersovereenkomsten tot gevolg dat ze moeten worden herzien of zelfs geheel vervangen. Je kunt daarover meer lezen in deze brochure van CMS.

Model bewerkersovereenkomst

We hebben voor het gemak een voorbeeld van een bewerkersovereenkomst opgenomen achterin dit boek. Daaruit blijkt waar een bewerkersovereenkomst zoal aan moet voldoen. We hebben de voorbeeldovereenkomst zodanig opgesteld dat deze vooral tegemoet komt aan de

© CMS Derks Star Busmann N.V., 2017

belangen van de verantwoordelijke (en dus niet zozeer de bewerker). Let goed op welke bepalingen in het voorbeeld relevant zijn voor het doel waarvoor je de overeenkomst wilt aangaan. Twijfel je over de benodigde inhoud van een bewerkersovereenkomst, vraag dan om deskundig advies.

2.6.3 Veelvoorkomende vragen over de bewerkersovereenkomst

Het maken van privacy-afspraken met leveranciers leidt vaak tot de nodige misverstanden en frictie. We hebben daarom een aantal veelvoorkomende vragen op een rij gezet.

Wij werken al jaren probleemloos met dezelfde bewerker zonder een bewerkersovereenkomst te hebben gesloten. Is het écht nodig om dit alsnog te doen?

Ja, je overtreedt als verantwoordelijke namelijk de wet indien een bewerkersovereenkomst ontbreekt.

De leverancier hanteert een eigen modelovereenkomst. Kan ik daarin meegaan?

Dat hangt natuurlijk af van de inhoud van het model. Onthoud echter dat een leverancier meestal weinig belang heeft om zichzelf vergaande verplichtingen op te leggen, dus bekijk de modelovereenkomst kritisch. Modellen van leveranciers bieden jou als verantwoordelijke soms onvoldoende waarborgen. Als de leverancier openstaat voor jouw inbreng, maak dan gebruik van het voorbeeld uit dit handboek.

Wat als de leverancier weigert om überhaupt een bewerkersovereenkomst te sluiten?

Vraag aan de leverancier wat de achtergrond is voor deze weigering. Als een leverancier beweert dat via haar diensten geen persoonsgegevens worden verwerkt, onderzoek dan goed of dit wel het geval is en vraag desnoods om deskundig advies. Blijkt dat wel degelijk persoonsgegevens worden verwerkt, heroverweeg dan de beslissing om met deze leverancier in zee te gaan.

Moet ik genoegen nemen met een privacy-bepaling in het dienstverleningscontract?

Nee, in veel gevallen is dit onvoldoende. Veel leveranciers hanteren standaardcontracten voor hun dienstverlening met slechts één privacy-bepaling. Daarin staat meestal dat jouw organisatie verantwoordelijke is en de leverancier uitsluitend optreedt als bewerker, gevolgd door een summier aantal rechten en plichten. Stel in dat geval voor om de voorbeeldovereenkomst als uitgangspunt te nemen.

Wat als een leverancier gebruik maakt van onderaannemers?

Als verantwoordelijke moet je er zorg voor dragen dat ook alle partijen die 'jouw' persoonsgegevens verwerken de privacy-regels naleven. Dit betekent dat je kunt worden aangesproken op privacy-schendingen van onderaannemers van de leverancier, ook al heb je daarop feitelijk geen invloed. Het is daarom belangrijk dat jouw leverancier gelijksoortige rechten heeft ten opzichte van de onderaannemers als de rechten die jij krijgt via de bewerkersovereenkomst. In de voorbeeldovereenkomst is een bepaling opgenomen die de leverancier verplicht om een dergelijke sub-bewerkersovereenkomsten te sluiten.

De leverancier maakt (deels) gebruik van servers die zich buiten Nederland bevinden. Moet de bewerkersovereenkomst daar iets over regelen?

Zolang persoonsgegevens worden verwerkt binnen de Europese Economische Ruimte (EER), is er in principe geen reden tot zorg. Het merendeel van IT-bedrijven maakt echter (ook) gebruik van servers die zich in de Verenigde Staten bevinden. Je mag persoonsgegevens niet doorgeven naar landen buiten de EER, tenzij bijzondere waarborgen zijn getroffen om de persoonsgegevens te beschermen. In de praktijk kan dit meestal goed worden opgelost met 'EU-modelcontracten', en inmiddels ook het zogeheten 'Privacy Shield'. Als de leverancier niet in staat is om een dergelijke oplossing aan te bieden, vraag dan om deskundig juridisch advies.

2.7 Informeren

2.7.1 Wat houdt de informatieplicht in?

Een belangrijke privacy-verplichting is dat je als verantwoordelijke een betrokkene op eigen initiatief goed informeert over *welke* persoonsgegevens je verwerkt, maar ook waarom en hoe je dit doet. Deze transparantie voorkomt dat je een betrokkene onaangenaam verrast, bijvoorbeeld omdat men zich gecontroleerd of gevolgd voelt. Informeren is bij uitstek niet alleen een kwestie van de wet naleven, maar ook een mooie kans om te demonstreren dat jouw organisatie goed omgaat met privacygevoelige informatie.

Voorbeelden:

- Topsporters moeten begrijpen hoe zij door de bond worden gemonitord;
- Medewerkers moeten weten of hun computer- en telefoongebruik kan worden gecontroleerd;
- Arbiters en deelnemers moeten weten of hun persoonlijke e-mail- en telefoongegevens voor anderen zichtbaar zijn;
- Deelnemers aan een winactie moeten weten of ze kunnen worden benaderd met commerciële berichten;
- Bezoekers en deelnemers van evenementen moeten weten of zij kunnen worden gefilmd of gefotografeerd, en hoe deze media achteraf wel/niet wordt gebruikt;
- Vrijwel iedere website en app verzamelt data van gebruikers, zodat je bezoekers en gebruikers moet uitleggen wat je daarmee van plan bent.

2.7.2 Op welk moment moet de betrokkene worden geïnformeerd?

Het moment waarop je de betrokkene informeert hangt af van de wijze waarop je persoonsgegevens hebt verkregen. Verkrijg je de persoonsgegevens *direct* van de betrokkene, dan informeer je de betrokkene *voorafgaand* aan de verwerking. Verkrijg je de persoonsgegevens via een *andere weg* (bijvoorbeeld van een derde), dan informeer je de betrokkene zodra je de gegevens zelf hebt *vastgelegd* in de eigen systemen.

© CMS Derks Star Busmann N.V., 2017

2.7.3 Welke informatie moet worden verstrekt?

Als verantwoordelijke ben je verplicht om de volgende informatie te verstrekken aan de betrokkene:

1. de identiteit van de verantwoordelijke (naam, vestiging, contactgegevens);
2. welke persoonsgegevens worden verwerkt;
3. voor welke doeleinden vindt de verwerking plaats; en
4. alle overige informatie die nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen tegenover de betrokkene.

Het laatste punt ('alle informatie') is een open norm en dus zeer situatieafhankelijk. Het betekent dat naarmate een verwerking ingrijpender is voor de betrokkene, het belang om daarover juist en tijdig te informeren steeds groter wordt.

Wees duidelijk

Een betrokkene heeft er niets aan om te lezen dat jij 'bepaalde informatie' 'mogelijk' voor 'kwaliteitsdoeleinden' gebruikt. Het lijkt misschien aantrekkelijk om jezelf met vage termen veel ruimte te geven, maar je wekt daarmee slechts argwaan.

Gewijzigd privacy-beleid

Wijzigt het privacy-beleid? Communiceer dit duidelijk en vooraf met betrokkenen, vooral als het gaat om ingrijpende veranderingen. Zorg er ook voor dat de privacyverklaring wordt aangepast.

2.7.4 In welke vorm stel ik de informatie beschikbaar?

Daar zijn geen specifieke regels voor. Het advies is om zoveel mogelijk aan te sluiten bij de manier waarop je met de betrokkene in contact staat, en het voor een betrokkene zo eenvoudig mogelijk te maken om tijdig kennis te nemen van de informatie. Hierna geven we daarom een paar voorbeelden uit de dagelijkse praktijk.

Achterin dit handboek tref je een modeldocument voor een privacyverklaring, dat in veel situaties een geschikt middel is om de betrokkene te informeren. Je kunt dit document naar eigen wens aanpassen. Ook vind je hierin terug welke informatie je in ieder geval moet opnemen.

Voorbeelden: hoe informeer je?

Personeel

Informatie over personeelszaken is voor werknemers meestal op een centrale plaats digitaal te vinden, bijvoorbeeld op het intranet van de organisatie. Dat is een geschikte weg om werknemers te informeren over jouw privacy-beleid. Werkt jouw organisatie niet met een intranet? Dan zijn er wellicht fysieke handleidingen/brochures waar je de informatie in kunt opnemen.

Websitebezoekers

Het privacy-beleid voor bezoekers van een website kun je uiteraard eenvoudig op diezelfde website plaatsen met een privacyverklaring. Zorg dat het beleid te bereiken is via een sub-pagina, bijvoorbeeld door het opnemen van een link onderaan de pagina.

Webwinkel

Het privacy-beleid voor klanten in de webshop communiceer je tijdens het bestelproces in de vorm van een privacyverklaring. Maak je gebruik van een digitaal inschrijfformulier, wijs dan op de privacyverklaring en plaats daarheen een duidelijk zichtbare hyperlink, die opent in een apart venster.

Apps

Het privacy-beleid bij apps kun je communiceren door het opnemen van een privacyverklaring in de app. Zorg ervoor dat nieuwe gebruikers bij eerste gebruik een 'pop-up' te zien krijgen. Je verklaart daarin het privacy-beleid van toepassing en verwijst naar de privacyverklaring.

Lidmaatschap/evenementen/winacties/opleidingen

Het privacy-beleid bij dit soort zaken communiceer je op hetzelfde moment als dat waarop iemand zich aanmeldt. Schrijft iemand zich ter plaatse in (bijvoorbeeld bij een balie/stand), leg dan de privacyverklaring klaar ter inzage. Maak je gebruik van een digitaal inschrijfformulier, vermeldt dan dat er een privacy-beleid van toepassing is en plaats een duidelijk zichtbare hyperlink naar de privacyverklaring, die opent in een apart venster. Zorg er bij voorkeur voor dat de betrokkene ergens op het papier/digitaal formulier afvinkt/klikt dat hij kennis heeft genomen van het privacy-beleid, zodat je daarop nog een extra keer de aandacht vestigt. Krijgen deelnemers/leden na hun inschrijving toegang tot een digitale omgeving (zoals een ledenportaal of actiepagina), neem dan ook hier een verwijzing op naar de privacyverklaring.

2.7.5 Moet de betrokkene altijd worden geïnformeerd?

In de praktijk kun je er bijna altijd vanuit gaan dat de informatieplicht van toepassing is. Er gelden echter enkele uitzonderingen, waar we in dit handboek slechts kort naar verwijzen. Raadpleeg bij twijfel een deskundige.

1. **Betrokkene al op de hoogte**
   Als de verantwoordelijke kan vaststellen dat een betrokkene al voldoende op de hoogte is van bepaalde verwerking, dan kan nadere informatieverstrekking daarover achterwege blijven.

   Voorbeeld: gelaagde structuur sportorganisaties
   Als een sportvereniging al concreet en helder heeft gecommuniceerd dat bepaalde persoonsgegevens zullen worden gedeeld met de sportbond/NOC*NSF voor bepaalde doeleinden, dan hoeft de sportbond (eenmaal verkregen) de betrokkene daarover in principe niet opnieuw te informeren.

2. **Onmogelijkheid of onevenredige inspanning**
   Verkrijgt de verantwoordelijke persoonsgegevens niet rechtstreeks van de betrokkene, dan kan het soms onmogelijk blijken of onevenredige inspanning kosten om de betrokkene te informeren. Ook in dat geval mag informatieverstrekking achterwege blijven.

© CMS Derks Star Busmann N.V., 2017

3. **Algemene wettelijke uitzondering**
   De wet erkent een aantal specifieke gevallen waarin de verantwoordelijke het informeren van een betrokkene achterwege mag laten. Een belangrijke uitzondering in de praktijk is het geval waarin de belangen van de verantwoordelijke of een derde geschaad zouden worden door het informeren van een betrokkenen.

Let op!
Voor het informeren van een betrokkene over een datalek gelden bijzondere regels. We bespreken dit in het onderdeel datalekken.

2.8 Rechten van de betrokkene

Een belangrijk uitgangspunt is dat een betrokkene enige macht kan uitoefenen over het verwerken van 'zijn' persoonsgegevens. Hij bezit daarom bepaalde wettelijke rechten, die tegenover jou als verantwoordelijke kunnen worden uitgeoefend. We bespreken hierna kort met welke rechten je zoal te maken krijgt.

2.8.1 Recht op inzage

Ten eerste heeft een betrokkene het recht om de verantwoordelijke te vragen welke persoonsgegevens van hem worden verwerkt. De betrokkene hoeft jou daarbij niet te vertellen waarom hij inzage wil. Je vraagt hier dus niet naar, tenzij je een sterk vermoeden hebt dat iemand zijn recht misbruikt.

Wat moet ik verstrekken?

Zorg dat je op verzoek een overzicht aan de betrokkene verstrekt, dat in ieder geval inzicht geeft in:
- het soort persoonsgegevens waarover je beschikt (bijvoorbeeld 'naam', 'geboortedatum', 'lidnummer', 'wedstrijdhistorie', etc.);
- het doel waarvoor je ze verwerkt ('ledenadministratie', 'marketing', etc.);
- met welke eventuele derden jij deze gegevens hebt gedeeld ('sponsoren', 'NOC*NSF', etc.); en
- de manier waarop je de gegevens hebt verkregen (direct van de betrokkene, via vereniging, etc.).

Uitzonderingen op het inzagerecht

Soms beschik je weliswaar over (gevoelige) informatie over een betrokkene, maar wil of mag je deze niet met hem delen. Je hoeft volgens de wet in bepaalde gevallen geen gehoor te geven aan een inzageverzoek. Denk bijvoorbeeld aan een melding over grensoverschrijdend gedrag. Je hebt daar als organisatie wellicht een intern rapport over opgemaakt, maar wil in verband met een lopend onderzoek misschien niet dat dit bij de betrokkene bekend wordt.
Bovendien zou inzage in dat rapport de belangen van iemand anders (zoals een slachtoffer) kunnen schaden.

Er zijn talloze andere situaties denkbaar waarin het inzagerecht in conflict komt met jouw of andermans rechten en plichten. Het is daarbij belangrijk dat je altijd een zorgvuldige afweging maakt. Twijfel je over medewerking aan iemands inzagerecht, vraag dan om deskundig advies.

Aandachtspunten
- Je moet binnen vier weken op een verzoek van de betrokkene reageren.
- Heb je het vermoeden dat een derde bezwaar kan hebben tegen een verzochte inzage, namelijk doordat bij inzage tevens gegevens van deze derde bekend zouden worden, stel de derde dan vóór de verstrekking in de gelegenheid om zich daarover uit te laten.
- Een betrokkene kan zijn inzagerecht slechts uitoefenen over eigen persoonsgegevens. Inzage in andermans persoonsgegevens is dus niet toegestaan, tenzij het een verzoek door de ouder of voogd van een minderjarige betreft.
- Het inzagerecht betekent niet dat je integraal alle informatie moet verstrekken waarover je als verantwoordelijke beschikt. Meestal kun je volstaan met het overzicht dat hiervoor is geschetst.
- Maak duidelijk dat inzageverzoeken schriftelijk moeten worden ingediend. Probeer het verstrekken van informatie over de telefoon te vermijden. Het kan namelijk lastig zijn om te controleren of je daadwerkelijk met de betrokkene spreekt. Verlang ook dat de verzoeker zich legitimeert. Het onbevoegd verstrekken van persoonsgegevens levert een datalek op. Gaat het om gegevens van een minderjarige, dan kun je deze wel verstrekken aan de ouder of voogd.

2.8.2 Recht op verbetering, aanvulling en verwijdering

Soms beschik je als verantwoordelijke over verouderde, onvolledige of irrelevante persoonsgegevens. Een betrokkene heeft in dat geval het recht om deze persoonsgegevens te laten:
- verbeteren;
- aanvullen; of
- verwijderen.

Bestaat er een gegronde reden om het verzoek te weigeren, dan moet je de betrokkene hiervan schriftelijk op de hoogte stellen.

Aandachtspunten
- Je moet binnen vier weken op een verzoek van de betrokkene reageren. Stel de betrokkene op de hoogte zodra je de aanpassingen hebt doorgevoerd.
- Een betrokkene kan zijn recht slechts uitoefenen over eigen persoonsgegevens. Aanpassing van andermans persoonsgegevens is dus niet toegestaan.
- Maak duidelijk dat verzoeken schriftelijk moeten worden ingediend. Het kan namelijk lastig zijn om te controleren of je daadwerkelijk met de betrokkene spreekt. Verlang ook dat de verzoeker zich legitimeert. Het onbevoegd aanpassen van persoonsgegevens levert mogelijk een datalek op.
  Gaat het om gegevens van een minderjarige, dan kun je wel meewerken aan een verzoek van de bevoegde vertegenwoordiger.

© CMS Derks Star Busmann N.V., 2017

- Als je iemands gegevens hebt gedeeld met een derde partij, regel dan dat eventuele aanpassingen ook bij deze derde worden doorgevoerd.

2.8.3 Recht van verzet

Heb je als verantwoordelijke geen goede reden om persoonsgegevens te verwerken, dan kan een betrokkene altijd verzoeken dat je daarmee stopt. Het is echter ook denkbaar dat je op zich een goede reden hebt om iemands persoonsgegevens te verwerken, maar dat een *zwaarwegender persoonlijk belang* van een betrokkene in een specifiek geval voorrang krijgt. Ook in dat geval moet je de verwerking staken. Dat geldt overigens alleen als je persoonsgegevens verwerkt op basis van de grondslag 'gerechtvaardigd belang'!

Aandachtspunten

- Verzoek de betrokkene om zijn verzet, inclusief argumenten, schriftelijk in te dienen.
- Maak bij het afwegen van jouw belang tegenover dat van de betrokkene gebruik van de criteria zoals omschreven bij het gerechtvaardigd belang.
- Je moet binnen vier weken op een verzoek reageren.
- Een betrokkene kan zijn recht slechts uitoefenen over eigen persoonsgegevens.
- Voor marketingdoeleinden geldt dat je een verzoek tot staking van de verwerking niet mag weigeren.
- Maak duidelijk aan de betrokkene dat verzoeken schriftelijk moeten worden ingediend. Het kan namelijk lastig zijn om te controleren of je daadwerkelijk met de betrokkene spreekt. Gaat het om gegevens van een minderjarige, dan kun je wel meewerken aan een verzoek van de bevoegde vertegenwoordiger.
- Als je iemands gegevens hebt gedeeld met een derde partij, regel dan dat het verzet ook bij deze derde wordt doorgevoerd.

2.9 Doorgifte naar het buitenland

2.9.1 Het doorgifteverbod

Bij het lezen van dit handboek is het je misschien al opgevallen dat in Nederland en in de EU nogal strenge regels gelden voor de omgang met persoonsgegevens. In landen buiten de Europese Economische Ruimte (EER) gelden er vaak andere regels, of kent men geen regels voor de omgang met persoonsgegevens. Om te voorkomen dat de privacy van betrokkenen na doorgifte aan ontvangers in dergelijke landen wordt aangetast, mag je persoonsgegevens niet zomaar doorgeven aan ontvangers in landen waar de betrokkene een risico loopt om onvoldoende te worden beschermd.

Voorbeeld: werken in de cloud

Werkzaamheden binnen organisaties worden steeds vaker uitgevoerd met webapplicaties of apps. Denk bijvoorbeeld aan tools voor administratie en ticketverkoop, maar ook aan webhosting en apps (zoals Dropbox/Whatsapp/WeTransfer). Men spreekt dan vaak over 'de cloud', wat meestal betekent dat data (waaronder persoonsgegevens) terecht komen op servers van externe leveranciers. Die servers staan niet zelden in de VS. In dat geval zijn de regels voor doorgifte van toepassing, zodat je bijzondere maatregelen moet treffen.

Voor Amerikaanse (IT-)organisaties geldt dat zij sinds enige tijd kunnen deelnemen aan het Privacy Shield-programma. Meestal wordt deze deelname duidelijk op de website van de leverancier vermeld. Is dit het geval, dan kun je er in veel gevallen op vertrouwen dat jouw doorgifte aan een dergelijke leverancier in de VS is toegestaan. De huidige verwachting is dat veel leveranciers zich bij Privacy Shield aansluiten. Privacy Shield is de opvolger van het inmiddels ongeldig verklaarde 'Safe Harbor'-programma. Vermeldt een leverancier dus dat wordt voldaan aan Safe Harbor, realiseer je dan dat dit onvoldoende is.

2.9.2 Welke landen maken deel uit van de EER?

Op dit moment bestaat de EER uit de volgende landen:

België;	Bulgarije;
Cyprus;	Denemarken;
Duitsland;	Estland;
Finland;	Frankrijk;
Griekenland;	Hongarije;
Ierland;	IJsland;
Italië;	Kroatië;
Letland;	Liechtenstein;
Litouwen;	Luxemburg;
Malta;	Nederland;
Noorwegen;	Oostenrijk;
Polen;	Portugal;
Roemenië;	Slovenië;
Slowakije;	Spanje;
Tsjechië;	Verenigd Koninkrijk (Engeland, Schotland, Wales en Noord-Ierland);
Zweden.	

2.9.3 Is het doorgifteverbod relevant voor mijn organisatie?

Ja, meestal wel. Het verbod betekent namelijk in de praktijk dat jouw organisatie (als verantwoordelijke of bewerker) persoonsgegevens niet mag doorgeven aan ontvangers in vrijwel alle landen buiten de EER, tenzij je bepaalde maatregelen treft. Zo moet je soms speciale doorgiftecontracten sluiten met de ontvanger (zoals de EU-modelcontracten), of moet je voor een eenmalige doorgifte expliciete toestemming vragen aan een betrokkene.

Voorbeeld: buitenlandse evenementen

Als sportbond vervul je regelmatig een actieve rol bij de deelname van topsporters aan buitenlandse evenementen. Je onderhoudt dan bijvoorbeeld contact met reisorganisaties, hotels, autoriteiten of wellicht de lokale zusterorganisatie. Met deze partijen worden veelal identificatiedocumenten, contactgegevens en wellicht ook gezondheidsgegevens uitgewisseld. Bevinden dergelijke ontvangers zich buiten de EER, besef dan goed dat je ook hier de doorgifteregels in acht moet nemen.

© CMS Derks Star Busmann N.V., 2017

Gaat het om een eenmalige doorgifte aan een beperkt aantal ontvangers, dan kun je meestal volstaan met het vragen van specifieke toestemming tot doorgifte aan de betrokkene. Gaat het echter om langdurigere uitwisseling, dan moet je mogelijk andere maatregelen treffen.

Het doorgifteverbod is een complex onderwerp, dat we in dit handboek niet in detail bespreken. Twijfel je of een bepaalde doorgifte is toegestaan, bespreek de situatie dan tijdig intern en schakel eventueel een privacy-deskundige in. De praktijk leert namelijk dat er voor veel doorgifteproblemen een goede oplossing beschikbaar is.

2.10 Aanmelding bij de Autoriteit Persoonsgegevens

Volgens de Wbp moet je als verantwoordelijke de Autoriteit Persoonsgegevens op de hoogte stellen van het feit dat je persoonsgegevens gaat verwerken. Deze algemene melding wordt vervolgens gepubliceerd in een openbaar register. Het idee hierachter is dat voor het publiek kenbaar is wat jouw organisatie zoal doet met persoonsgegevens.
De aanmeldplicht is sinds 2016 eigenlijk een dode letter geworden. De Autoriteit Persoonsgegevens handhaaft de plicht niet, en bovendien is de boete op het achterwege laten van een melding sinds 2016 afgeschaft. Bovendien vervalt de aanmeldplicht zoals we die nu kennen met de inwerkingtreding van de Verordening in 2018. We besteden er daarom geen verdere aandacht aan in dit handboek.

Wil je meer lezen over de omstandigheden waaronder je verwerkingen wel en niet moet aanmelden, kijk dan op de website van de Autoriteit Persoonsgegevens.

2.11 Functionaris gegevensbescherming

2.11.1 Wat is een Functionaris gegevensbescherming?

Het naleven van privacy-regels in een organisatie vraagt om een duidelijke taakverdeling. De wet schept hier een mogelijkheid voor organisaties om zelf een interne privacy-toezichthouder te benoemen, met de interne bevoegdheid om te controleren of de regels worden nageleefd. Dit is de zogeheten *Functionaris* gegevensbescherming ("Fg"), in de praktijk ook wel "privacy officer" genoemd.

Behalve toezicht kan een Fg ook een geschikt aanspreekpunt zijn voor:
- een betrokkene die zijn rechten wil uitoefenen;
- medewerkers met privacy-vragen; en
- de Autoriteit Persoonsgegevens.

De wet bepaalt dat de Fg geen nadeel mag ondervinden van de uitoefening van zijn taak. Hij/zij moet zich dus kritisch kunnen opstellen, zonder de angst om daardoor te worden ontslagen. Uiteraard moet de Fg wel over de nodige kennis en betrouwbaarheid beschikken.
Een groot voordeel van een Fg is dat privacy permanente aandacht krijgt binnen je organisatie, zodat risico's eerder kunnen worden ontdekt. Bovendien kan diezelfde Fg, vanuit zijn expertise, vaak direct als intern adviseur optreden om problemen op te lossen.

2.11.2 Is een Functionaris gegevensbescherming verplicht?

Nee, op dit moment is het ***niet verplicht*** om een Fg aan te stellen. Om vanaf 2018 te kunnen voldoen aan de veeleisende Verordening kan het aanstellen van een Fg echter een verstandige beslissing zijn. Dat geldt met name voor organisaties met een wat grotere omvang. Wij verwachten dat het belang van een goede Fg en het aantal Fg's de komende jaren flink toeneemt. Op de website van de Autoriteit Persoonsgegevens vind je meer praktische informatie over de Fg.

2.12 Toezicht, sancties en aansprakelijkheid

De kans is groot dat je dit handboek leest vanwege de explosieve aandacht die privacy inmiddels krijgt. Is de boel immers niet op orde, dan kamp je inmiddels daadwerkelijk met een probleem. Dat beperkt zich niet tot de veelbesproken boetes voor datalekken. Je loopt een risico op schadeclaims, vertrouwensverlies, en niet onbelangrijk: negatieve publiciteit.

We bespreken hierna kort wat er op je pad kan komen bij overtreding van de regels. De belangrijkste les is daarbij misschien wel om mogelijke misstanden *altijd* met serieuze aandacht op te pakken. Realiseer je dat privacy-overtredingen vrijwel nooit opzettelijk plaatsvinden, maar het gevolg zijn van onschuldige vergissingen of onwetendheid. Wil je fouten tijdig opsporen en oplossen, dan is interne transparantie dus essentieel. Onthoud dat de kans op escalatie aanmerkelijk toeneemt naarmate een probleem zich langer onder de radar afspeelt.

2.12.1 Handhaving door autoriteiten

Formeel onderzoek

Vermoedt een autoriteit dat jouw organisatie de regels overtreedt, dan kan die een formeel onderzoek starten. De Autoriteit Consument & Markt handhaaft daarbij de regels rondom direct marketing en cookies. De Autoriteit Persoonsgegevens houdt toezicht op alle overige privacy-regels.

Je bent als organisatie *verplicht* om medewerking te verlenen aan het onderzoek. Zo dien je op verzoek alle noodzakelijke informatie te verstrekken en hebben autoriteiten het recht om ter plaatse onderzoek te verrichten. Het contact met de autoriteiten kan bijzonder stressvol zijn. Het eerste contactmoment is vaak onverwacht, en de beschikbare tijd om te handelen is vervolgens kort. Voorkom dat je in dit soort stressvolle situaties fouten maakt en schakel tijdig een deskundig advocaat in. Deze begeleidt je in de juiste opstelling tegenover de autoriteit, en zorgt dat jouw belangen tijdens het onderzoek goed naar voren komen.

Alternatieve interventie

In plaats van een formeel onderzoek probeert men overtredingen soms ook te beëindigen via zogeheten 'alternatieve interventies'. De autoriteit stuurt dan een brief, of belt met een aantal vragen en opmerkingen. Je moet hier vervolgens snel op reageren en op korte termijn eventuele herstelmaatregelen doorvoeren. Ook hier geldt: twijfel je over je rechten en plichten, vraag dan om deskundig advies.

© CMS Derks Star Busmann N.V., 2017

Dwangsommen en boetes

Concludeert een autoriteit na onderzoek dat er sprake is van overtreding, dan kan ten eerste een zogeheten 'last onder dwangsom' worden opgelegd. Je krijgt dan een formeel bevel om de overtreding te staken. Volg je die instructies niet op, dan moet je een dwangsom betalen. Het gaat hierbij vaak om hoge bedragen, waarbij de hoogte afhangt van de overtreden regel.
In plaats van een dwangsom kan een autoriteit ook forse boetes opleggen. Ook hier hangt de hoogte af van de overtreden regel. De maximale boete per overtreding die de Autoriteit Persoonsgegevens kan opleggen bedraagt maar liefst € 820 000. Bij de Autoriteit Consument & Markt is dat zelfs € 900 000.

Voordat een boete wordt opgelegd, geven autoriteiten meestal een 'bindende aanwijzing'. In die bindende aanwijzing staat dan op welke wijze je de overtreding moet beëindigen. Negeer je die aanwijzing, dan komt alsnog een boete in beeld. Is overigens sprake van opzettelijke overtreding of ernstige nalatigheid, dan mag direct een boete worden opgelegd en blijft een bindende aanwijzing achterwege. In de Boetebeleidsregels van de ACM en Autoriteit Persoonsgegevens vind je meer informatie over boetehoogtes en de wijze waarop deze worden opgelegd.

Let op!
De meest beruchte boete ziet weliswaar op het niet-melden van een datalek, maar ook voor vele andere overtredingen gelden hoge boetes. Denk bijvoorbeeld aan het onvoldoende informeren van een betrokkene, het onrechtmatig verwerken van BSN-nummers of het slecht beveiligen van persoonsgegevens.

Betrokkenheid van bewerkers

Soms is niet jouw eigen organisatie, maar een ingeschakelde bewerker in overtreding. Hoewel je daar misschien weinig grip op hebt, kun je daarvoor als verantwoordelijke meestal wél worden aangesproken. Dat geldt zowel richting de autoriteiten als richting de betrokkene. Een goede bewerkersovereenkomst is daarom onmisbaar. Je kunt daarin namelijk een boetebepaling opnemen voor het geval jouw leverancier in de fout gaat. Ook kun je daarin een 'vrijwaring' opnemen: daarmee verplicht je de bewerker tot vergoeding van eventuele claims die jij (als verantwoordelijke) ontvangt van de autoriteiten of betrokkenen.

2.12.2 Civiele aansprakelijkheid

Handel je als organisatie in strijd met privacy-verplichtingen en ondervindt een betrokkene daardoor schade, dan ben je mogelijk verplicht tot het betalen van een schadevergoeding. Schade is hier een breed begrip. Zo kan het gaan om ernstige reputatieschade, maar ook om schade door identiteitsfraude, bijvoorbeeld door een datalek.

2.12.3 Strafrecht

Bij opzettelijke en ernstige overtreding van bepaalde privacy-regels kan het Openbaar Ministerie overgaan tot strafrechtelijke vervolging. De straffen rondom het schenden van privacywetgeving zijn aanzienlijk. In de context van dit handboek laten we dit verder buiten beschouwing.

2.12.4 Verzekeren

Het is deels mogelijk om je als organisatie te verzekeren tegen bepaalde vormen van cyber- en privacy-gerelateerde kosten, schade en aansprakelijkheid. Overweeg daarom als (adviseur van het) bestuur, aan de hand van het gewenste risicoprofiel binnen de organisatie, het eventuele voordeel van een dergelijke verzekering.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 3: Het delen van persoonsgegevens

In 't kort:

- Deel je persoonsgegevens met een derde, neem dan de 5 vuistregels in acht:
  Regel 1: Bepaal of er een geldige grondslag is
  Regel 2: Verstrek uitsluitend noodzakelijke gegevens
  Regel 3: Zorg voor een geschikte en veilige overdracht
  Regel 4: Stel vast of je de betrokkene moet informeren
  Regel 5: Documenteer de verstrekking
- Ook binnen de eigen organisatie gelden beperkingen voor het delen van persoonsgegevens. Let er daarom op dat toegang tot interne informatie voldoende wordt beperkt.
- Werken met vrijwilligers? Maak duidelijke afspraken over de omgang met persoonsgegevens en houd voldoende toezicht.

Als sportbond of koepelorganisatie beschik je over veel persoonsgegevens van individuele sporters, zowel op amateur- als op topsportniveau. Dat maakt de organisatie erg aantrekkelijk voor allerlei partijen die interesse hebben in dit soort informatie. Toch mogen persoonsgegevens niet zomaar worden gedeeld met derden.

Een reden om bij het delen van persoonsgegevens extra goed op te letten, is dat na een verstrekking vaak moeilijk valt te controleren wat de ontvanger met de gegevens doet. Heb je de gegevens eenmaal gedeeld en blijkt dit achteraf onrechtmatig, dan is het kwaad al geschied.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

In dit hoofdstuk geven we 5 vuistregels voor het delen van persoonsgegevens met derden. Ook lees je waar je op moet letten bij gegevensuitwisseling *binnen* de organisatie, en behandelen we enkele aandachtspunten voor de omgang met vrijwilligers.

3.1 Delen met derden: 5 vuistregels

Is de organisatie om welke reden dan ook van plan om persoonsgegevens te delen met een derde, dan zijn er steeds 5 algemene vuistregels die je minimaal in acht moet nemen:

Regel 1: Bepaal of er een geldige grondslag is om de persoonsgegevens te delen
Regel 2: Verstrek uitsluitend noodzakelijke persoonsgegevens
Regel 3: Zorg voor een veilige overdracht
Regel 4: Stel vast of je de betrokkene moet informeren
Regel 5: Documenteer de verstrekking

In deze paragraaf hebben we het steeds over 'delen' en 'derde'. Delen is daarbij een breed begrip. Het gaat niet alleen om een rechtstreekse verzending per e-mail van gegevens, maar bijvoorbeeld ook om de publicatie op een server waartoe derden toegang krijgen. Met 'derde' bedoelen we iedere persoon of organisatie die niet onder rechtstreeks gezag staat van de verantwoordelijke, maar ook geen betrokkene of bewerker is.

Let op!
Sportbonden, verenigingen en koepelorganisaties moeten elkaar meestal ook als 'derde' behandelen. Dat er in de sport traditioneel veel informatie wordt uitgewisseld en gezamenlijke doelen worden nagestreefd, doet daar niets aan af. Neem dus ook bij de uitwisseling met samenwerkende organisaties de hierna besproken vuistregels in acht.

3.1.1 Regel 1: Bepaal of er een geldige grondslag is

Persoonsgegevens mogen uitsluitend aan een derde worden verstrekt wanneer daar een geldige grondslag voor is. In het hoofdstuk Doel en grondslag hebben we uitgelegd hoe je bepaalt of dat het geval is. Past het doel waarvoor je wil verstrekken niet bij minimaal één van de zes wettelijke grondslagen, ga er dan in principe van uit dat de verstrekking niet is toegestaan. Raadpleeg bij twijfel een deskundige.

Voorbeelden: verstrekking aan derden

- De verstrekking van lidgegevens aan sponsoren voor marketingdoeleinden (grondslag: toestemming);
- De beschikbaarstelling van wedstrijdinformatie (inclusief persoonsgegevens van deel nemers en arbiters) door sportbonden aan aangesloten verenigingen (grondslag: ge rechtvaardigd belang);
- De verstrekking van persoonsgegevens van topsporters aan bijvoorbeeld reisbureaus of autoriteiten bij deelname aan evenementen (meerdere grondslagen mogelijk);
- De doorgifte van adresgegevens van leden aan de uitgever van het clubblad, zodat deze rechtstreeks via de uitgever kunnen worden verzonden (grondslag: uitvoering overeenkomst/gerechtvaardigd belang).

© CMS Derks Star Busmann N.V., 2017

Is het delen echt nodig?
Je bent verplicht om te overwegen of het doel dat je nastreeft voldoende aanleiding geeft om gegevens te delen met een derde. Kun je hetzelfde doel dus net zo eenvoudig bereiken door het delen achterwege te laten, deel de gegevens dan niet.

Verenigbaarheid
Controleer altijd of de verstrekking aan een derde verenigbaar is met het doel waarvoor je de persoonsgegevens als verantwoordelijke hebt verkregen, óók als voor die verstrekking op zichzelf een geldige grondslag aanwezig is. Soms kan een verstrekking namelijk toch onaanvaardbare gevolgen hebben.

Voorbeeld: doorgifte contactgegevens aan media
Sportbonden beschikken meestal voor interne doeleinden over de contactgegevens van topsporters. Op het moment dat een sporter de aandacht trekt van de media, is het niet ongebruikelijk dat de sportorganisatie bijvoorbeeld wordt gevraagd om verstrekking van het mobiele (privé)nummer. Denk aan een verzoek om een interview of felicitatie. Wij adviseren echter om daar niet aan mee te werken zonder dat de persoon in kwestie daarmee heeft ingestemd. Een praktische oplossing is hier om de persoon vooraf om een algemene toestemming te vragen (bijvoorbeeld in het contract dat jij als sportbond met de persoon sluit).

3.1.2 Regel 2: Verstrek uitsluitend noodzakelijke gegevens
De persoonsgegevens van een betrokkene bevinden zich meestal niet geïsoleerd in je systemen, maar zijn ze onderdeel van bijvoorbeeld een spreadsheet, een profiel, een databank etc. Meestal hoef je maar een fractie van die informatie te delen om je doel te bereiken. Je bent dan ook verplicht om alléén die informatie te delen die voor het doel noodzakelijk is.

Voorbeeld: beperkte informatieverstrekking sponsor
Als je e-mailadressen van leden voor de verzending van marketingmails deelt met een sponsor, voorkom dan dus dat de sponsor toegang krijgt tot overige lid-gegevens. Die informatie is namelijk onnodig om de marketingmail te kunnen verzenden. De sponsor zal wellicht ook interesse hebben in aanvullende kolommen met voor- en achternamen, geboortedata en woonplaatsen, maar daar zal je doorgaans niet bevoegd toe zijn zonder daarvoor uitdrukkelijke toestemming te hebben verkregen van de betrokkene.

3.1.3 Regel 3: Zorg voor een veilige overdracht
Je bent als verantwoordelijke verplicht om bij het verwerken van persoonsgegevens passende beveiligingsmaatregelen treffen. Dat geldt dus ook voor de manier waarop je persoonsgegevens deelt met derden.

Er zijn tegenwoordig eindeloos veel manieren om informatie te delen. Denk niet alleen aan intranet of e-mail, maar ook aan platforms waarmee gegevens kunnen worden gedeeld (Dropbox, WeTransfer) en chatservices (Whatsapp, Facebook Messenger). Het gebruik van dergelijke platforms en diensten is soms echter in strijd met de wet, omdat met dit soort dienstverleners nauwelijks goede afspraken mogelijk zijn. Zo is vaak niet te achterhalen hoe deze aanbieders omgaan met data, en worden daadwerkelijke garanties op veiligheid vrijwel nooit afgegeven. Houd er bovendien rekening mee dat het gebruik van deze diensten vaak leidt tot doorgifte buiten de EER, iets dat niet zomaar is toegestaan. Overleg dus met je eigen IT-afdeling of –leverancier welke maatregelen eventueel nodig zijn om dit soort diensten alsnog veilig te gebruiken.

Behalve het treffen van technische maatregelen moet je natuurlijk ook zorgen dat de gegevens uitsluitend belanden bij de ontvanger die je voor ogen hebt. Voorkom dus dat data kan worden geraadpleegd door onbevoegden, want daarmee veroorzaak je een datalek.

Structurele uitwisseling
Het komt ook voor dat je met verenigingen, koepelorganisaties of sponsors doorlopend persoonsgegevens deelt. Dat gebeurt vooral bij informatie die continu wordt geactualiseerd, zoals ledengegevens of wedstrijdregistraties. Er wordt dan vaak een digitale koppeling gelegd tussen informatiesystemen (overleg dit met je IT-afdeling of -leverancier), of het gehele informatiesysteem wordt gedeeld. In dat geval is het zeer verstandig om schriftelijke afspraken met elkaar te maken over onder andere het toegestane gebruik en de beveiliging. Bovendien moet het duidelijk zijn wie voor welke verwerkingen als verantwoordelijke optreedt. Let op: dit is niet hetzelfde als de bewerkersovereenkomst, die sluit je namelijk alleen met bewerkers.

3.1.4 Regel 4: Stel vast of je de betrokkene moet informeren
Zoals uitgelegd in paragraaf 2.7 moet je de betrokkene in principe vooraf informeren over een verwerking. Dat geldt ook voor het verstrekken van persoonsgegevens aan een derde.

Voorbeeld: lid is al op de hoogte
Je kunt er regelmatig op vertrouwen dat een lid al op de hoogte is van bepaalde uitwisselingen. Heb je een lid bijvoorbeeld ten tijde van zijn aanmelding al op de hoogte gesteld dat je voor bepaalde doeleinden bepaalde gegevens zal delen met sponsors of een koepelorganisatie, dan hoef je hem dat niet opnieuw te vertellen op het moment dat die verstrekking inderdaad plaatsvindt.

Voorbeeld: bewust niet informeren
Het komt ook voor dat je weliswaar persoonsgegevens van de betrokkene hebt verstrekt aan een derde, maar de betrokkene daar op dat moment niet wil of mag informeren. Denk bijvoorbeeld aan vertrouwelijke meldingen rondom grensoverschrijdend gedrag of bepaalde communicatie met dopingautoriteiten. In dat geval blijft het informeren van de betrokkene mogelijk achterwege.

3.1.5 Regel 5: Documenteer de verstrekking
Zorg dat je in een later stadium nog kunt achterhalen (en aantonen) of en hoe je bepaalde persoonsgegevens hebt verstrekt aan een derde. Deze informatie kan bijvoorbeeld van belang zijn om te reageren op een verzoek van de betrokkene of om je te verweren tegen eventuele claims.

© CMS Derks Star Busmann N.V., 2017

Gaat het om een incidentele verstrekking, administreer dan:
- de datum van de verstrekking;
- de wijze van verstrekking;
- welk soort persoonsgegevens zijn verstrekt;
- het doel van de verstrekking;
- wie er heeft verstrekt; en
- aan wie de verstrekking is gericht.

Wissel je op structurele basis persoonsgegevens uit via een digitale koppeling (zie regel 3), zorg dan dat deze digitale activiteit wordt vastgelegd ('gelogd').

3.2 Delen binnen de organisatie

Het uitwisselen van persoonsgegevens *binnen* de organisatie is geen vorm van 'delen' zoals besproken in paragraaf 3.1. Zolang de uitwisseling namelijk intern plaatsvindt tussen (bijvoorbeeld) werknemers van de verantwoordelijke, is er geen sprake van verstrekking aan een derde. Toch is het belangrijk om kort stil te staan bij interne gegevensuitwisseling, omdat ook hier beperkingen gelden.

Voorbeelden:
- De personeelsadministratie bevat uiteraard veel vertrouwelijke gegevens en moet alleen toegankelijk zijn voor HR-medewerkers.
- Gevoelige informatie over topsporters is vatbaar voor publieke aandacht en moet daarom beschermd worden tegen onbevoegde inzage door personeel.

Let op!
Als de ontvangende persoon niet in dienst is ('op de pay-roll staat') van dezelfde werkgever als jij (ook al zit hij aan het bureau tegenover je), kan al sprake zijn van delen met een derde!

Toegangsbeperking
De organisatie is verplicht om persoonsgegevens intern voldoende af te schermen vanwege de eisen van beveiliging en geheimhouding.

Tips
- Stel duidelijke regels op voor het intern delen van informatie, en communiceer met personeel dat dit beleid van kracht is en hoe zij hier gebruik van moeten maken.
- Zorg dat werknemers bij eventuele vragen of twijfel over het beleid terecht kunnen bij een vaste contactpersoon.
- Veel computerprogramma's bieden tegenwoordig de mogelijkheid om toegangsrechten per gebruiker in te stellen. Overweeg of dit binnen jouw organisatie uitkomst kan bieden.

3.3 Beschikbaarstelling aan vrijwilligers

Veel sportorganisaties maken als verantwoordelijke gebruik van vrijwilligers. Deze vrijwilligers krijgen regelmatig toegang tot persoonsgegevens. Denk bijvoorbeeld aan deelnemerslijsten of de registratie van wedstrijduitslagen. Je gaat met die vrijwilligers mogelijk soepeler om dan met betaald personeel. Zo wordt er over vrijwilligers vaak minder uitdrukkelijk gezag uitgeoefend, en zijn werkafspraken minder strikt of zelfs geheel afwezig.

Een gebrek aan controle op vrijwilligers is vanuit privacy-opzicht erg riskant. De organisatie is in de rol van verantwoordelijke namelijk verplicht om ervoor te zorgen dat vrijwilligers (net als werknemers) persoonsgegevens slechts gebruiken zoals ze door de organisatie wordt opgedragen. Schiet de verantwoordelijke daarin tekort, dan kan dit leiden tot sancties en aansprakelijkheid.

Tips
- Sluit de sportorganisatie met vrijwilligers (digitaal of op papier) een vrijwilligersovereenkomst? Zo ja, neem daarin dan een specifieke geheimhoudingsclausule op. Zo nee, sluit dan een aparte geheimhoudingsovereenkomst. Let op: dit is niet hetzelfde als een bewerkersovereenkomst.
- Beperk de toegang tot persoonsgegevens zodat vrijwilligers alleen toegang hebben tot die gegevens die strikt noodzakelijk zijn voor de uitvoering van hun taak.
- Stel beleid op waarin je vrijwilligers duidelijk vertelt wat zij wel en niet mogen doen met persoonsgegevens. Je kunt daarbij waar mogelijk vaak aansluiten bij het beleid dat je oplegt aan werknemers. Denk bijvoorbeeld aan de regels rondom Bring Your Own Device. Controleer bovendien of het beleid wordt nageleefd.
- Vrijwilligers kunnen soms (sneller dan werknemers) plots uit beeld raken nadat zij hun taak neerleggen. Vergeet nooit om de toegang tot informatie direct te beëindigen. Zorg ook dat alle persoonsgegevens worden teruggegeven, en waar nodig worden gewist van privéapparatuur van de vrijwilliger.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 4: Wedstrijdadministratie

In 't kort:
- Stel op amateurniveau persoonsgegevens uit de wedstrijdinformatie (uitslagen, standen, inschrijfgegevens etc.) uitsluitend beschikbaar voor degenen die daarbij een redelijk belang hebben.
- Stel persoonsgegevens van arbiters enkel beschikbaar voor zover dat redelijkerwijs nodig is en aan degenen die daar daarbij een redelijk belang hebben.
- Zorg dat je voldoende grip hebt op vrijwilligers die beschikking krijgen over wedstrijdadministratie.

4.1 Wedstrijduitslagen en standen

Het is tegenwoordig steeds eenvoudiger om informatie over uitslagen, standen en ranglijsten in real-time online te publiceren. Er bestaat daarom al snel een neiging om zulke informatie beschikbaar te stellen voor het publiek. Toch moet ook hier rekening worden gehouden met privacywetgeving. Wedstrijduitslagen en standen bevatten immers dikwijls persoonsgegevens, zoals een naam en identificatienummer. Zorg dus dat je als organisatie altijd bewust blijft van de (mogelijk negatieve) privacy-gevolgen van de online publicatie daarvan voor de betrokkene.

Let op!
Het is ook mogelijk dat wedstrijdinformatie van een team bijvoorbeeld geen informatie over individuele personen bevat, maar uitsluitend informatie op teamniveau (zoals "Heren 2"). In dat geval zal geen sprake zijn van een verwerking van persoonsgegevens.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

Maak bij het publiceren van uitslagen en standen op amateurniveau (met daarin persoonsgegevens), zeker bij minderjarigen, altijd een zorgvuldige belangenafweging als je bepaalde informatie wil publiceren. Dit geldt zeker wanneer je publiceert zonder toesteming van de betrokkene.

Voorbeeld:
Het is niet ongebruikelijk dat verenigingen de prestaties van lokale teams online plaatsen. Daarbij worden soms ook de voor- en achternaam van de betreffende sporters genoemd. Als de vereniging daarvoor geen toestemming vraagt aan de betrokken sporters, dan zal de vereniging moeten kunnen aantonen dat een dergelijke publicatie een gerechtvaardigd belang dient.

Tip
Zorg bij voorkeur dat je dergelijke informatie uitsluitend beschikbaar stelt voor leden of personen die een legitiem belang hebben bij toegang tot dergelijke informatie. Zij moeten daarbij bijvoorbeeld inloggen op de website.

Op het niveau van *topsport* is de openbare publicatie van uitslagen en standen geen probleem. Toch geldt ook hier dat niet méér persoonsgegevens mogen worden gepubliceerd dan noodzakelijk is. Zo lijkt het vermelden van de bloeddruk of de hartslag (wat bijzondere persoonsgegevens zijn) tijdens een sportwedstrijd naar onze mening nog geen geaccepteerde verwerking, tenzij een sporter daarvoor uitdrukkelijke toestemming verleent.

4.2 (Inschrijf)gegevens van deelnemers en arbiters

Voor organisatorische doeleinden (zeker op amateurniveau) gebeurt het weleens dat van zowel deelnemers als arbiters naam- en contactgegevens online beschikbaar worden gesteld.

Voor deelnemers van wedstrijden op amateurniveau geldt dat je in principe een gerechtvaardigd belang nodig hebt om iemands voor- en achternaam te publiceren, tenzij iemand al uitdrukkelijke toestemming heeft gegeven. Ben je niet in staat om goed te onderbouwen dat de publicatie noodzakelijk is vanuit een belang van de sportorganisatie of een derde (bijvoorbeeld andere verenigingen), overweeg dan om zulke publicaties achterwege te laten.

Bij arbiters ligt het mogelijk in de rede dat je zijn naam om organisatorische doeleinden wel vermeldt, maar ontbreekt dikwijls de noodzaak om daar contactgegevens aan toe te voegen (zoals zijn mobiele telefoonnummer). Dit ligt wederom anders als de publicatie echt noodzakelijk is vanuit een gerechtvaardigd belang. Blijkt het noodzakelijk om een individu op een lijst te vermelden (soms ontkom je daar niet aan), overweeg dan of het mogelijk is om een lidnummer te gebruiken in plaats van een achternaam. Dat is weliswaar nog steeds een (gepseudeonimiseerd) persoonsgegeven, maar de publicatie ervan is doorgaans minder bezwaarlijk dan die van een voor- of achternaam.

© CMS Derks Star Busmann N.V., 2017

4.3 Werken met vrijwilligers

Bij de organisatie van wedstrijden zijn vaak vrijwilligers betrokken. Zij handelen in veel gevallen in de naam van de sportorganisatie. Dat betekent dat de organisatie ook verantwoordelijke is voor de wijze waarop vrijwilligers met persoonsgegevens omgaan. Je kunt hier lezen waar je in dat kader extra goed bij moet opletten.

4.4 Bewaartermijn

Hoelang je persoonsgegevens uit de wedstrijdadministratie bewaart, hangt af van het doel waarvoor je deze verzameld. Het is daarom lastig om algemene uitspraken te doen over een geschikte bewaartermijn.

Het uitgangspunt is dat je de persoonsgegevens niet langer bewaart dan noodzakelijk is voor het doel waarvoor je ze hebt verzameld. Sommige persoonsgegevens uit de wedstrijdinformatie zal je wellicht voor statistische, wetenschappelijke of historische doeleinden nog langer willen bewaren. Dat is mogelijk, maar zorg dan wel dat deze langer bewaarde gegevens niet alsnog voor *andere* doeleinden worden gebruikt. Kijk bovendien of er eventueel persoonsgegevens zijn die niet relevant zijn voor deze statistische (etc.) doeleinden, zodat je alleen de relevante informatie behoudt.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 5: Ledenadministratie

In 't kort:
- Het lidmaatschap van een sporter is voor de bond geen vrijbrief voor het verrichten van verwerkingen waar geen geldige grondslag voor bestaat.
- Ledenlijsten mogen door een vereniging in principe niet geheel openbaar worden gepubliceerd, maar wel op afgeschermde wijze aan leden beschikbaar worden gesteld.
- Doorgifte van e-mailadressen aan sponsoren is in principe mogelijk, maar let op de regels die daarvoor gelden.

Sportbonden met (tevens) individuele leden beschikken uiteraard over een ledenadministratie. Die administratie bestaat hoofdzakelijk uit persoonsgegevens. Denk bijvoorbeeld aan namen en bondsnummers, maar ook aan contact- en betaalgegevens. Het verwerken van die gegevens is de verantwoordelijkheid van de betreffende sportbond. Of je de ledenadministratie nu gebruikt om de organisatie draaiende te houden of voor een andere reden, je dient bij elk gebruik de algemene regels in acht te nemen zoals besproken in hoofdstuk 2. Hierna lichten we toe waar je in de omgang met de ledenadministratie voornamelijk op moet letten.

5.1 Welke gegevens neem je op in de ledenadministratie?

In de ledenadministratie mogen uitsluitend persoonsgegevens worden opgenomen waarvoor een geldige grondslag bestaat om ze te verwerken. Bovendien mogen niet meer (soorten) persoonsgegevens worden opgenomen dan noodzakelijk is voor de vervulling van de doeleinden waarvoor je de gegevens verwerkt.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

5.2 Gelaagde structuur: wat zijn 'leden'?

De sportwereld kent een 'gelaagde structuur'. Zo heeft een sporter meestal een lidmaatschap bij een sportvereniging die is aangesloten bij een sportbond, en de sportbond is aangesloten bij NOC*NSF. Daarbij wordt vaak gesproken over 'indirecte leden'. Dat kan verwarring veroorzaken. Zolang een sportbond formeel gezien geen lidmaatschap is overeengekomen met een persoon, is die persoon namelijk juridisch gezien *geen lid* van die sportbond. Andersom geldt dat de vereniging de sportbond en NOC*NSF in principe als 'derden' moet beschouwen. Dat betekent bijvoorbeeld dat, indien de vereniging persoonsgegevens van leden wil delen met de sportbond of NOC*NSF, de vereniging daar steeds een geldige grondslag voor nodig heeft. Het uitwisselen van persoonsgegevens met een 'derde' zonder geldige grondslag is absoluut niet toegestaan!

Let op!
In de praktijk kunnen sportbonden en verenigingen dit probleem grotendeels oplossen door bijvoorbeeld het opnemen van bepaalde constructies in de statuten en/of reglementen van de vereniging of sportbond. Dat kan per sporttak in Nederland echter behoorlijk verschillen, zodat we dergelijke constructies in dit handboek niet nader bespreken.

5.3 Ledenlijst beschikbaar stellen aan leden

Bij sportbonden met individuele leden is het een vereniging in principe toegestaan om *aan leden* een ledenlijst beschikbaar de stellen. Wij bevelen wel aan om de ledenvergadering eenmalig te verzoeken om daarmee in algemene zin in te stemmen.

Let op!
We gebruiken hier begrip 'ledenlijst'. Daarmee bedoelen we *niet* het integrale ledenbestand/de ledenadministratie waarin zich méér gegevens bevinden (contactgegevens, financiële gegevens etc.). Met ledenlijst bedoelen we slechts een lijst met namen van personen die lid zijn van de vereniging.

5.4 Online publicatie van de ledenlijst

Sportorganisaties mogen een ledenlijst niet zomaar online beschikbaar stellen aan het publiek. De Autoriteit Persoonsgegevens is van oordeel dat het online publiceren van een ledenlijst slechts is toegestaan op een voor leden afgeschermde webpagina.

Voorbeeld: online databank
Als je als sportbond mogelijk wilt maken dat sporters elkaar kunnen zoeken in een databank via een door jou aangeboden app of website, zorg dan dat je die informatie uitsluitend aan ingelogde bondsleden beschikbaar stelt.

© CMS Derks Star Busmann N.V., 2017

5.5 Toegestaan gebruik binnen de organisatie

De ledenadministratie wordt door de vereniging op allerlei manieren gebruikt om de organisatie draaiende te houden. Zo zijn bankrekeningnummers nodig om de contributie te innen, en heb je misschien adresgegevens nodig om het maandelijkse tijdschrift te kunnen verzenden. Een dergelijk gebruik kan meestal worden gebaseerd op het gerechtvaardigd belang van de verantwoordelijke vereniging, of de contractuitvoering tegenover de betrokkene.

Zorg dat je de ledenadministratie binnen de sportorganisatie uitsluitend gebruikt op een manier die verenigbaar is met het doel waarvoor je de gegevens uit de administratie hebt verkregen.

5.6 Delen met sponsoren voor marketingdoeleinden

In hoofdstuk 3 hebben we uitgelegd dat je bij het delen van persoonsgegevens met een derde steeds 5 vuistregels in acht moet nemen. Dit geldt ook wanneer persoonsgegevens van leden voor marketingdoeleinden worden gedeeld met sponsoren.

Tip: als het doorgeven aan sponsoren in algemene zin is goedgekeurd door de ledenvergadering, dan heeft de sportbond voor die verstrekking geen individuele toestemming meer nodig van de betrokkene. De sportbond kan deze doorgifte in dat geval namelijk baseren op een gerechtvaardigd belang. Heeft een ledenvergadering een dergelijk besluit niet genomen, dan zal voor de verstrekking aan de sponsor uitdrukkelijke toestemming van de betrokkene nodig zijn.

Let op!
De sponsor is op zijn beurt zélf verantwoordelijke voor wat hij met de persoonsgegevens doet. Dat is dus niet de zorg van de sportorganisatie die de gegevens heeft verstrekt.

Let op!
Bij een verstrekking van persoonsgegevens aan een sponsor moet je de betrokkene informeren dat hem een kosteloos recht van verzet toekomt tegen de verstrekking. Dit betekent dat hij gedurende een bepaalde periode eenvoudig bezwaar moet kunnen maken tegen de verstrekking. Je moet dit recht van verzet aanbieden voordat de verwerking plaatsvindt! De sportorganisatie kan leden daarover informeren via bijvoorbeeld mail, het clubblad of de eigen website.

5.7 Bewaartermijn

Als een lid zich uitschrijft of slechts een daglid is, dan hoeven zijn gegevens niet direct na het einde van het lidmaatschap te worden verwijderd. Voor een geschikte bewaartermijn kan worden aangesloten bij het Vrijstellingsbesluit, wat in dit geval betekent dat je persoonsgegevens van een lid uit de ledenadministratie in principe niet langer bewaart dan twee jaar na einde van het lidmaatschap. Voor informatie die valt onder de fiscale bewaarplicht geldt een langere bewaartermijn, namelijk zeven jaar. Overleg dit met de financiële afdeling binnen de organisatie.

Sommige informatie zal je wellicht voor statistische, wetenschappelijke of historische doeleinden langer willen bewaren. Dat is mogelijk, maar zorg dan wel dat deze langer bewaarde gegevens niet alsnog voor andere doeleinden worden gebruikt. Kijk bovendien of er eventueel persoonsgegevens zijn die niet relevant zijn voor deze statistische (etc.) doeleinden, zodat je alleen de relevante informatie behoudt.

Tips
- Bevat de ledenadministratie behalve contact- en betaalgegevens ook verdergaande informatie zoals gezondheidsgegevens, let dan op de strengere regels die daarbij gelden.
- Niet iedereen binnen de organisatie heeft voldoende belang bij toegang tot (alle delen van) de ledenadministratie. Beperk iemands toegangsrechten dus op basis van zijn taken en verantwoordelijkheden.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 6: Talent en topsport

In 't kort:

- Sportorganisaties verwerken met trainings- en begeleidingsprogramma's vaak gezondheidsgegevens van topsporters. Daarvoor is doorgaans toestemming van de sporter nodig.
- Vraag bij het gebruik van gezondheidsgegevens via talentvolgsystemen en wearables toestemming aan de betreffende sporter, en sluit waar nodig bewerkersovereenkomsten met IT-leveranciers van dergelijke systemen.
- Let op dat bij talent van jonger dan 16 jaar toestemming dient te worden verleend door de ouder of voogd.
- Neem bij de organisatie van reizen de 5 vuistregels voor delen met derden in acht, en let goed op dat geen onrechtmatige verwerking van het Burger Service Nummer plaatsvindt.

Op het niveau van topsport verwerkt een sportorganisatie vaak meer en extra gevoelige persoonsgegevens. We bespreken hierna kort welke implicaties dit heeft voor een aantal veelvoorkomende processen in de organisatie.

6.1 Gezondheidsgegevens

De persoonsgegevens van sporters die in trainings- en begeleidingsprogramma's worden verwerkt door sportorganisaties zijn vaak deels gezondheidsgegevens. In paragraaf 2.3 hebben we uitgelegd dat gezondheidsgegevens bijzondere persoonsgegevens zijn. Het verwerken van bijzondere persoonsgegevens (zoals gezondheidsgegevens) is niet zomaar toegestaan.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

Voor sportorganisaties (als verantwoordelijke) betekent dit in de praktijk dat zij slechts gezondheidsgegevens van de sporter mogen verwerken als de sporter daar (als betrokkene) toestemming voor geeft. Die toestemming regel je bijvoorbeeld in een contract.
De gezondheidsgegevens mogen door de sportorganisatie ook worden gebruikt voor juridische procedures zoals sportarbitrage. In dat geval is geen toestemming nodig van de betrokkene.

6.2 Monitoring

Topsporters worden doorgaans nauwkeurig gemonitord. Daarvoor worden allerlei systemen gebruikt die (bijvoorbeeld via mobiele applicaties en *wearables*) allerlei aspecten van de carrière in kaart brengen, bijvoorbeeld trainingsschema's, prestatiemeting, communicatie met trainers en blessureoverzichten. Personeel en andere personen rondom de sportorganisatie krijgen meestal inzicht in dergelijke data, die vaak gezondheidsgegevens bevatten. Dat betekent dat de sporter uitdrukkelijke toestemming moet geven voor dergelijke monitoring en toegang tot zulke data.

Realiseer je dat gegevens van topsporters kunnen rekenen op extra aandacht van de buitenwereld, waaronder zich ook kwaadwillende partijen kunnen bevinden. Een goede beveiliging is dan ook van belang ter voorkoming van datalekken. Als er IT-leveranciers betrokken zijn bij de verwerking van persoonsgegevens (bijvoorbeeld door het hosten van webapplicaties of apps), dan zijn deze partijen bewerker en moet een bewerkersovereenkomst worden gesloten.

6.3 Wearables

We verwezen hiervoor al kort naar het gebruik van wearables. Dat zijn draagbare apparaatjes die allerlei lichaamsfuncties kunnen meten. Denk aan stappentellers, bloeddrukmeters en hartslagmeters die je op je lichaam of kleding draagt. De gegevens die met wearables worden gegenereerd zijn ook aan te merken als gezondheidsgegevens. De verwerking van dit soort gegevens moet dus voldoen aan de eisen die we hebben toegelicht in paragraaf 2.3. Dit betekent voornamelijk dat sporters meestal uitdrukkelijke toestemming zullen moeten geven aan de verantwoordelijke voor het gebruik maken van wearable-data.

Let op!
Sporters zijn soms als werknemer in dienst bij een sportorganisatie. Als deze sportorganisatie als verantwoordelijke tevens een werkgever/werknemer-relatie heeft met de sporter, dan wordt het geven van 'vrije' toestemming al gauw problematisch, zie daarover paragraaf 2.1.4. Probeer topsporters daarom (voor zover dit mogelijk is) daadwerkelijk keuzevrijheid te geven bij het gebruik van wearable-data door de sportorganisatie.

6.4 Minderjarig talent

Het verwerken van persoonsgegevens van een talent jonger dan 16 jaar vereist extra aandacht. Zoals we hebben uitgelegd in paragraaf 2.1.4 kan deze namelijk niet zelfstandig toestemming verlenen voor de verwerking van zijn of haar persoonsgegevens. Nu voor het verwerken van gezondheidsgegevens in het kader van talentbegeleiding veelal toestemming nodig zal zijn (zie paragraaf 6.2), zal die toestemming dus telkens door een ouder of voogd moeten worden verleend. Houd daar rekening mee bij het contracteren met minderjarig talent.

© CMS Derks Star Busmann N.V., 2017

6.5 Reizen

Sport (en vooral topsport!) is een internationale aangelegenheid. Sporters, vrijwilligers en medewerkers van sportorganisaties zijn daarom vaak op reis. Bij het boeken van reizen worden behoorlijk wat persoonsgegevens verwerkt van deelnemers aan het reisgezelschap. Denk aan namen, geboortedata, *frequent flyer numbers*, en (wellicht) ook betaalgegevens. De sportbond die de boeking doet is verantwoordelijke voor de verstrekking aan bijvoorbeeld reisbureaus, en moet daarbij de 5 vuistregels voor het delen met derden naleven. Deze derden (zoals het reisbureau of een luchtvaartmaatschappij) zijn vervolgens verantwoordelijke voor de verwerkingen die zij op hun beurt verrichten.

De verstrekking van persoonsgegevens door de sportorganisatie is, voor zover dat nodig is om de reis te boeken, toegestaan op grond van de uitvoering van een overeenkomst, toestemming van de betrokkene of een gerechtvaardigd belang. Ook is het mogelijk dat de sportbond van een andere organisatie opdracht krijgt om een reis te boeken.

Let op!

In aanloop naar en tijdens de reis wordt hier en daar nog wel eens gevraagd om een kopie van een paspoort. Onder de Nederlandse wetgeving is dat echter niet zomaar toegestaan. Het paspoort bevat namelijk het Burgerservicenummer (BSN). Dit nummer mag slechts worden gebruikt als de wet dit expliciet verplicht, en daar is slechts in een beperkt aantal gevallen sprake van. Dat de betrokken persoon eventueel toestemming verleent voor zo'n kopie is daarbij irrelevant.

Vindt de verstrekking overigens plaats in het buitenland, dan is de Wet bescherming persoonsgegevens mogelijk niet van toepassing. Je wordt dan mogelijk wel geconfronteerd met buitenlandse wetgeving. Vraag bij twijfel om deskundig advies.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 7: Marketing

In 't kort:
- Denk bij het versturen van nieuwsbrieven en reclame aan de regels rondom direct marketing.
- Ook voor het versturen van persoonlijke berichten op sociale media gelden de direct marketing-regels.
- Denk bij het plaatsen van cookies aan de 'cookieregels'.
- Prijsvragen en winacties zijn toegestaan, maar zorg voor een deugdelijke privacy-bepaling in de actievoorwaarden en let op de minimumleeftijd van 18 jaar voor deelname.

Het verwerken van persoonsgegevens speelt tegenwoordig een rol in vrijwel alle vormen van marketing. Als de sportorganisatie zelf bepaalt of en hoe een actie wordt georganiseerd, dan is de organisatie verantwoordelijke. De grondslag voor promotionele acties is doorgaans het gerechtvaardigd belang of de toestemming van de betrokkene.
We bespreken hierna de belangrijkste regels bij:
1. Elektronische direct marketing
2. Social media
3. Winacties
4. Cookies

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

7.1 Elektronische direct marketing (o.a. mailings)

7.1.1 Wat is direct marketing?

Het sturen van commerciële berichten naar iemands e-mailadres is een vorm van direct marketing. Direct marketing is het individueel benaderen van een persoon of rechtspersoon ter promotie van een organisatie, product of dienst. Voor direct marketing via elektronische berichten (zoals e-mail of persoonlijk bericht via social media) gelden bijzondere regels, ook wel de "SPAM-regels" genoemd. We behandelen hierna de kern van deze regels voor sportbonden.

7.1.2 Wanneer is het SPAM-verbod wel/niet van toepassing?

Het SPAM-verbod geldt voor het versturen van "ongevraagde" elektronische berichten. Daarbij hoeft het niet perse te gaan om pure reclameboodschappen: ook een nieuwsbrief wordt in veel gevallen beschouwd als een ongevraagd bericht. Een bekend voorbeeld is de tussenvariant: een mailing waarin zowel nieuws als sponsorboodschappen zijn opgenomen. Ook zulke berichten kunnen kwalificeren als "ongevraagd", zodat het SPAM-verbod van toepassing is (zie ook 7.1.5).

Let op!
Bij het versturen van nieuwsbrieven door een *vereniging* aan *leden* is sprake van een bijzondere situatie. Een vereniging moet haar leden immers kunnen informeren over het reilen en zeilen binnen de vereniging. Zolang een nieuwsbrief uitsluitend dergelijke berichten bevat, is het SPAM-verbod dus niet van toepassing. Een dergelijke nieuwsbrief mag dus door een vereniging worden verstuurd. Er moet dan wel daadwerkelijk sprake zijn van een lidmaatschap. Zie 7.1.5 over het versturen van gemengde berichten (een mix van reclame en nieuws).

Voorbeelden: SPAM-verbod niet van toepassing, geen toestemming nodig
- Algemene mededelingen van de vereniging (zoals de uitnodiging voor een ledenvergadering of de verenigingsagenda, wedstrijduitslagen, evenementagenda);
- Het versturen van een antwoord aan iemand die een verzoek heeft ingediend via het contactformulier;
- Het versturen van een ontvangstbevestiging ("wij hebben uw verzoek/bestelling ontvangen");
- Het versturen van een betalingsherinnering;

7.1.3 Heb je toestemming nodig voor het versturen van mailings?

Ja, voor het versturen van ongevraagde elektronische berichten (zie 7.1.2) heb je voorafgaande toestemming nodig van de ontvanger. In de praktijk gaat het daarbij meestal om nieuwsbrieven of reclame.

Lees hier hoe je op de juiste wijze toestemming verkrijgt.

© CMS Derks Star Busmann N.V., 2017

Let op!
Bij de SPAM-regels geldt het zogeheten opt-in-systeem. Dat betekent dat iemand uitdrukkelijk en vooraf met de ontvangst van dergelijke berichten moet hebben ingestemd. Opt-out (je vraagt niet vooraf toestemming maar biedt wel gelegenheid om uit te schrijven) is dus onvoldoende!

Let op!
Probeer geen toestemming te verkrijgen door het opnemen/verstoppen van een bepaling in algemene voorwaarden of privacyverklaring. De heersende opvatting is dat een toestemming daarmee onvoldoende uitdrukkelijk wordt verkregen. Wil je dus toestemming vragen voor dergelijke mailingen terwijl iemand zich bijvoorbeeld aanmeldt voor een evenement of een aankoop doet, vraag daar dan apart en expliciet toestemming voor.

Let op!
Is het bericht vrijwel geheel een commerciële boodschap van een sponsor die door de sportbond wordt verstuurd, dan heb je zeker toestemming nodig van de ontvanger.

7.1.4 Zijn er ook situaties waarin je geen toestemming nodig hebt?

Ja, maar slechts in uitzonderlijke gevallen (of als het SPAM-verbod niet van toepassing is, zie 7.1.2). Als je het mailadres bijvoorbeeld van de ontvanger hebt verkregen doordat je iemand eerder een product of dienst hebt verkocht, dan mag je deze persoon commerciële berichten sturen over eigen, soortgelijke producten of diensten.

Voorbeelden: eigen soortgelijke producten of diensten
- Je mag een betalende deelnemer aan een evenement/wedstrijd/opleiding benaderen voor eigen soortgelijke activiteiten.
- Je mag een klant van een webshop die een product bestelt benaderen met aanbiedingen voor producten uit dezelfde webshop.

Je mag een klant van een webshop dus bijvoorbeeld niet benaderen met reclame voor een evenement of opleiding (tenzij je daar uiteraard aparte toestemming voor hebt verkregen).

Toestemming is evenmin nodig als je een bericht verstuurt aan een adres dat bestemd en bekend isvoor zulke ongevraagde berichten. Een fictief voorbeeld is het e-mailadres aanbiedingen@sportbond.nl. Let op dat een algemeen ‘info@’-e-mailadres niet voldoet aan de eisen voor deze uitzondering, zodat je hier niet zomaar berichten aan kan versturen.

7.1.5 Hoe zit het met gemengde nieuwsbrieven aan leden?

Het is in de sportwereld gebruikelijk dat sportbonden aan leden allerlei berichten sturen die zowel nieuws/mededelingen als commerciële elementen bevatten. Denk bijvoorbeeld aan een sponsoritem of de vermelding van kortingsacties voor leden. In dit soort situaties is sprake van een juridisch grijs gebied, en kan slechts per geval worden beoordeeld of het SPAM-verbod wel/niet van toepassing is.

Daardoor is soms onduidelijk of je voor dergelijke berichten wel of geen expliciete toestemming nodig hebt van de ontvanger.

Een verstandige oplossing is hier wat ons betreft om ook voor dit soort gemengde berichten iedere geadresseerde vooraf toestemming te vragen. Je ondervangt hiermee het probleem dat per bericht discussie kan ontstaan over de aard (commercieel/niet-commercieel) ervan. Het kan zo zijn dat je over adresbestanden beschikt waarbij je tot op heden geen expliciete toestemming hebt verkregen voor het verzenden van dergelijke berichten. Mocht je aan die adressen dus gemengde berichten sturen, zorg dan minstens dat je een deugdelijke opt-out biedt aan de ontvangers (zie 7.1.6).

Let op!
Voor het versturen van gemengde berichten aan niet-leden heb je toestemming nodig, omdat je met dergelijke ontvangers in feite geen relatie hebt (tenzij het klanten zijn, zie daarover 7.1.4).

Let op!
De enkele vermelding van een sponsor (bijvoorbeeld door het plaatsen van een logo onderin de nieuwsbrief aan leden (met uitsluitend nieuws/updates) leidt er nog niet toe dat sprake is van een commercieel bericht.

7.1.6 Informeren en opt-out

Of je nu toestemming nodig hebt of niet, je moet de ontvanger altijd vooraf informeren over het feit dat zijn contactgegevens (persoonsgegevens dus) gebruikt kunnen worden voor reclame of nieuwsbrieven. Bovendien moet je, voorafgaand en in elk bericht dat wordt verstuurd, de betrokkene de mogelijkheid bieden om zich uit te schrijven (de zogeheten “opt-out”).

7.1.7 Targeted advertising

Soms wil je niet je gehele adressenbestand aanschrijven, maar slechts een bepaalde doelgroep binnen dat bestand. Als reclame of marketingcampagnes worden toegespitst op bepaalde categorieën personen die geselecteerd zijn op basis van voorkeur en/of gedrag, spreekt men doorgaans van ‘targeted advertising’ of ‘behavioural targeting’. Dat mag, maar zorg dat je de ontvanger voorafgaand (betrokkene) goed informeert dat je dergelijke analyses uitvoert en waarom je dit doet. Daarmee voorkom je dat een betrokkene onaangenaam verrast (bijvoorbeeld omdat hij zich onaangekondigd ‘gevolgd’ voelt).

7.1.8 Externe partij als bewerker

Voor het versturen van direct-marketing-berichten mag je een externe partij inschakelen. Meestal zijn dit online dienstverleners (denk bijvoorbeeld aan MailChimp). Deze derde wordt doorgaans aangemerkt als bewerker en mag uitsluitend berichten versturen in naam en in opdracht van jouw organisatie. Zorg dat je als organisatie met zulke dienstverleners een bewerkersovereenkomst sluit.

© CMS Derks Star Busmann N.V., 2017

7.1.9 Telemarketing

Voor *telefonische* direct marketing zijn de regels iets soepeler. Het bellen voor commerciële, ideële of charitatieve doeleinden mag in beginsel altijd, tenzij anders blijkt uit het Bel-me-niet-register. Deze *opt-out* geldt alleen voor *natuurlijke personen*. 'Cold calling' in het kader van business-to-business is onder deze regels dus wel toegestaan.

7.2 Sociale media

Een sportorganisatie die een sociale-media-account beheert is verantwoordelijke voor de persoonsgegevens die de organisatie via dat platform verwerkt. In die zin verschilt sociale media niet van een clubblad of een website. Als gebruikers van het platform op eigen initiatief persoonsgegevens delen, dan zijn zij daarvoor ook *zelf* verantwoordelijke. Sociale media bieden vaak de mogelijkheid om gebruikers gericht te benaderen met aanbiedingen of reclame. Als dit via persoonlijke berichten gebeurt, dan valt dit meestal onder de strenge regels voor direct marketing, en heb je dus meestal toestemming nodig.

Gericht adverteren

In plaats van het direct benaderen van personen kan de doelgroep ook worden bereikt via advertentietools die het sociale platform (zoals Facebook en Twitter) zelf aanbiedt. Je levert dan persoonsgegevens of publiekscriteria aan, welke door het platform worden gelinkt aan informatie die zij zelf al bezitten over hun gebruikers. Wanneer een (potentieel) lid bijvoorbeeld een account heeft op het platform, dan kunnen aan die persoon bepaalde advertenties van de sportorganisatie getoond worden. Het delen van persoonsgegevens met het platform is voor deze doeleinden meestal toegestaan op grond van het gerechtvaardigd belang van de sportorganisatie. Neem echter wel de 5 vuistregels in acht voor de verstrekking van dergelijke persoonsgegevens aan sociale media.

Let op!

Het platform is na de verstrekking door de sportorganisatie zelf verantwoordelijke voor de verwerkingen die met die gegevens plaatsvinden bij de uiteindelijke communicatie aan de eindgebruiker. Je sluit in dat geval dus geen bewerkersovereenkomst.

7.3 Winacties

Het is niet toegestaan om kansspelen aan te bieden zonder vergunning. Op dit verbod bestaat één belangrijke uitzondering: de promotie van eigen producten of diensten, of (de naamsbekendheid van) de organisatie. Dat noemen we een *promotioneel kansspel*. Bij een promotioneel kansspel wordt een prijs of premie vergeven aan een winnaar die grotendeels door kansberekening wordt bepaald. Denk bijvoorbeeld aan prijsvragen waarbij uit de lijst van juiste antwoorden een winnaar wordt geloot, of het loten van een winnaar uit een aantal mensen dat een bepaalde boodschap 'liket' op Facebook. Promotionele kansspelen zijn toegestaan als wordt voldaan aan de Gedragscode promotionele kansspelen 2014.

Deze gedragscode bevat ook een paar bijzondere regels voor het verwerken van persoonsgegevens:

- Een promotioneel kansspel voldoet niet aan de gedragscode als het enige doel is om persoonsgegevens te verzamelen. Als de actie de naamsbekendheid van de sportbond echter daadwerkelijk kan vergroten, zal al snel aan de definitie van 'promotie' zijn voldaan;
- Van minderjarigen mogen persoonsgegevens worden verwerkt, *tenzij* de ouder of wettelijk vertegenwoordiger geen toestemming heeft gegeven. Let op: de grens is hier 18 jaar in plaats van de gebruikelijke 16 jaar.

Uiteraard moet de verantwoordelijke organisator alle algemene regels voor het verwerken van persoonsgegevens in acht nemen, zie daarover hoofdstuk 2. Een belangrijke verplichting daarbij is dat je de betrokkene voldoende informeert, bijvoorbeeld over:

- de doeleinden waarvoor de persoonsgegevens worden gebruikt;
- de partijen aan wie gegevens eventueel worden doorgegeven;
- de toepasselijke bewaartermijn van persoonsgegevens; en
- de rechten van de betrokkene als deelnemer.

Het is in de praktijk vaak handig om dergelijke informatie op te nemen in de toepasselijke actievoorwaarden.

7.4 Cookies

Voor het *uitlezen* en *plaatsen* van informatie op 'randapparatuur', zoals een mobiele telefoon, tablet of computer, zijn specifieke regels opgenomen in de Telecommunicatiewet. Deze regels staan bekend als de 'cookiewet', omdat een cookie het bekendste voorbeeld is van het digitaal uitlezen en plaatsen van informatie. Maar let op: de regels gelden ook voor andere technieken waarbij informatie wordt uitgelezen of geplaatst.

7.4.1 Wat zijn cookies?

Cookies zijn kleine tekstbestanden die worden opgeslagen op de apparatuur van de bezoeker van een website. Ze worden veelvuldig gebruikt. Cookies kunnen gebruikers 'volgen' langs verschillende websites en maken daarmee bijvoorbeeld gericht adverteren mogelijk. Ook kunnen cookies ervoor zorgen dat je blijft ingelogd op een website nadat je een andere internetpagina bezoekt. Het gebruik van cookies kan gevolgen hebben voor de privacy van degene die het betreffende apparaat gebruikt. Daarom bestaan er aanvullende regels voor het plaatsen van cookies. De eindgebruiker kan volgens deze regels zowel een natuurlijk persoon als een rechtspersoon zijn, zoals een B.V. of een stichting. Hierin verschillen de cookieregels van de Wbp: die beschermt enkel natuurlijke personen.

© CMS Derks Star Busmann N.V., 2017

Soorten cookies

Cookies komen grofweg voor in drie vormen:

- Technisch noodzakelijke cookies, ook wel functionele cookies genoemd. Denk bijvoorbeeld aan cookies die een 'winkelwagentje' van een webwinkel mogelijk maken. Zou een order immers spontaan worden vergeten, dan zou het plaatsen van een bestelling al snel onwerkbaar worden.
- Kwaliteits- of effectiviteitscookies: Hiermee kunnen de kwaliteit en de effectiviteit van de website worden verbeterd (voor IT-ers: denk aan A/B-testing). Ook affiliate-cookies vallen onder deze categorie: op die manier kan een adverteerder bijvoorbeeld bijhouden welke advertentie daadwerkelijk tot de aankoop van een product heeft geleid.
- Tracking cookies: deze cookies volgen het internetgedrag van de gebruiker. Daarmee kunnen ze het interesse-profiel van de gebruiker in kaart brengen. Deze vorm wordt veel gebruikt bij online adverteren.

7.4.2 Toestemming, informatieplicht en uitzonderingen

Volgens de hoofdregel moet de eindgebruiker toestemming geven voordat cookies mogen worden geplaatst. Dat betekent dat je de eindgebruiker vooraf duidelijk moet informeren over de doeleinden en werking van de cookies. Je geeft bijvoorbeeld de volgende informatie:

- De naam van de website die de cookies plaatst;
- Het doel waarvoor de cookies worden gebruikt. Denk bijvoorbeeld aan tracking, advertenties tonen en het verbeteren van de website;
- Het type cookie dat door of via de website wordt geplaatst. Denk bijvoorbeeld aan analytisch, tracking, functioneel;
- Het gebruik van eventuele andere technieken. Denk bijvoorbeeld aan Javascript en web beacons;
- De actie waardoor de gebruiker toestemming geeft. Toestemming kan bijvoorbeeld gegeven worden door op 'akkoord' te klikken;
- De eventuele impact die de cookies kunnen hebben op de privacy van de gebruiker.

De eigenaar van de website is het eerste aanspreekpunt voor toezichthouder ACM. Via deze website worden immers alle cookies geplaatst. Meestal vraagt de website-eigenaar ook toestemming voor cookies die door derden worden gebruikt op dezelfde website.

Uitzonderingen op de toestemmings- en informatieplicht

Er zijn drie gevallen waarin je voor het plaatsen van cookies geen toestemming nodig hebt en de betrokkene daarover niet hoeft te informeren:

1. De cookies zijn technisch noodzakelijk om elektronische communicatie mogelijk te maken;
2. De cookies zijn nodig om een door de gebruiker gevraagde dienst te leveren; of
3. De cookies zijn bedoeld om informatie te verkrijgen over de kwaliteit of effectiviteit van de website, en hebben bovendien geen of slechts geringe gevolgen voor de privacy van de gebruiker. In de praktijk betekent dit dat je vrijwel alle technisch noodzakelijke cookies en kwaliteits- of effectiviteitscookies mag plaatsen.

Let op!
Voor tracking cookies vraag je altijd toestemming!

Tip
De ACM (Autoriteit Consument & Markt) heeft enkele veelvoorkomende vragen beantwoord over de toepassing van cookieregels. Het document biedt een zeer nuttig inzicht over het gebruik van cookies in allerlei praktijksituaties. Wij bevelen het raadplegen van dit document dan ook sterk aan.

7.4.3 Verwerken van persoonsgegevens

Het kan zo zijn dat er met behulp van cookies persoonsgegevens worden verwerkt. Dat is het geval wanneer je middels de cookies informatie verkrijgt die herleidbaar is tot een individu.

In het geval van tracking cookies bestaat daarbij een zogenaamd *rechtsvermoeden*: er wordt verondersteld dat je met deze cookies persoonsgegevens verwerkt (tenzij je kunt bewijzen dat dit niet zo is), zodat bij zulke cookies vrijwel altijd ook de *overige* regels van toepassing zijn (zie hoofdstuk 2).

Als er derde partijen betrokken zijn, dat is deze derde mogelijk een bewerker. In dat geval moet er dus een bewerkersovereenkomst worden gesloten. Dit is onder meer het geval bij het gebruik van Google Analytics.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 8: Beeldmateriaal

In 't kort:

- Het maken van foto- en videobeelden met herkenbaar in beeld gebrachte personen is een verwerking van persoonsgegevens. Dat betekent dat daarop alle in hoofdstuk 2 besproken privacy-regels van toepassing zijn.
- Naast privacy-regels geldt ook het zogeheten portretrecht. Daarmee kan de geportretteerde zich verzetten tegen publicatie van beeldmateriaal waarop hij of zij herkenbaar in beeld wordt gebracht.
- Voor in opdracht gemaakte portretten geldt dat voor publicatie altijd toestemming van de geportretteerde of zijn volmachtgever nodig is.
- Voor niet in opdracht gemaakte portretten geldt dat de geportretteerde zich daartegen kan verzetten op grond van een redelijk belang. Dit kan zowel een privacybelang als een commercieel belang zijn. In dat laatste geval moet mogelijk een vergoeding worden betaald.

8.1 Publicatie van beeldmateriaal: privacy-regels

Foto's en video-opnamen van herkenbaar in beeld gebrachte personen zijn meestal persoonsgegevens, en soms zelfs bijzondere persoonsgegevens. Een sportorganisatie die dergelijk beeldmateriaal publiceert is daarvoor verantwoordelijke.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

Let op!
Het is belangrijk om voorafgaand aan de publicatie vast te stellen of het materiaal bijzondere persoonsgegevens bevat, omdat in dat geval strengere regels (zoals toestemming) gelden. De Autoriteit Persoonsgegevens is echter van mening dat beeldmateriaal meestal geen bijzonder persoonsgegeven is zolang de verantwoordelijke niet het *uitdrukkelijke doel* heeft om onderscheid te maken naar ras of geloof. Meestal zal dit uitdrukkelijke doel bij een publicatie door een sportbond niet aanwezig zijn, zodat de striktere regels voor bijzondere persoonsgegevens niet van toepassing zijn.

Voor het maken en publiceren van beeldmateriaal moet de sportorganisatie toestemming verkrijgen van herkenbaar in beeld gebrachte betrokkenen, óf een gerechtvaardigd belang hebben. Denk bij een gerechtvaardigd belang bijvoorbeeld aan persvrijheid, direct marketing, promotie van de organisatie of beveiliging. Ook wedstrijdverslaggeving zal vaak onder het gerechtvaardigd belang vallen. Een sportorganisatie mag dus in principe foto's en beelden van wedstrijden publiceren of uitzenden, ook als daarbij bijvoorbeeld toeschouwers herkenbaar in beeld komen.

Zorg ervoor dat personen (als dat redelijkerwijs mogelijk is) vooraf worden geïnformeerd over eventuele beeldopnamen. Dat kan bijvoorbeeld in wedstrijdreglementen, ticketvoorwaarden of met behulp van een bordje bij de ingang van een evenementlocatie.

8.2 Publicatie van beeldmateriaal: portretrecht

Het publiceren van beeldmateriaal is iets ingewikkelder dan het gebruiken van 'normale' persoonsgegevens. Personen die *herkenbaar* in beeld worden gebracht kunnen zich soms namelijk ook beroepen op het *portretrecht* uit de *Auteurswet*. Volgens deze wet is een portret een afbeelding van het gelaat van een persoon. De geportretteerde kan zich in sommige gevallen verzetten tegen publicatie van een beeldopname
Kort gezegd bestaan er twee soorten portretrecht, die voor *in opdracht* gemaakte portretten en die voor *niet in opdracht* gemaakte portretten. Hieronder leggen we uit wat daarbij de regels zijn.

8.2.1 Portretten in opdracht gemaakt

Teamfoto's en individuele spelersfoto's die op aanvraag door een fotograaf zijn gemaakt, zijn voorbeelden van portretten die in opdracht gemaakt zijn. Voor het *publiceren* van zulke portretten is altijd toestemming nodig van de geportretteerde(n) of gevolmachtigde (bijvoorbeeld een ouder of manager). Vaak blijkt impliciet of iemand toestemming geeft, maar het is niet altijd raadzaam om daarop te vertrouwen.

Let op!
Iemand die toestemming geeft voor het *maken* van een foto geeft daarmee niet per definitie toestemming voor de *publicatie* ervan. Voor dat laatste is schriftelijke instemming vaak het meest wenselijk, voor zover dat in de praktijk uitvoerbaar is. Vaak kun je dit op voorhand oplossen door het opnemen van een toestemmingsbepaling in de lidmaatschapsvoorwaarden, arbeidscontracten, inschrijfvoorwaarden, etc.

© CMS Derks Star Busmann N.V., 2017

8.2.2 Portretten niet in opdracht gemaakt

Voor portretten die *niet* in opdracht zijn gemaakt is de wet iets soepeler. Denk hier bijvoorbeeld aan wedstrijdfoto's of foto's die worden genomen tijdens opleidingen. Tegen publicatie van dergelijke foto's kan de geportretteerde slechts optreden op grond van een *redelijk belang*. Een redelijk belang kan zowel een privacybelang als een *commercieel belang* zijn.

Let op!
Verwar een 'redelijk belang' van de geportretteerde niet met het gerechtvaardigd belang van de verantwoordelijke zoals we die kennen uit privacywetgeving.

Het kan voorkomen dat het belang van de geportretteerde botst met het belang van degene die een beeldopname wil publiceren. Denk bijvoorbeeld aan de vrijheid van meningsuiting van de geportretteerde tegenover het maatschappelijk belang van een goede nieuwsvoorziening. De partij die tot publicatie wil overgaan, moet in dat geval een belangenafweging maken.

Let op!
Ga voorzichtig om met herkenbaar in beeld gebrachte minderjarige amateursporters. Bij kinderen weegt het privacybelang extra zwaar ten opzichte van jouw eventuele nieuws- of promotiebelang. Het is daarom raadzaam om uitdrukkelijk toestemming te vragen aan de ouders of voogd voordat je overgaat tot publicatie. Informeer degene aan wie je toestemming vraagt bovendien waarvoor je het materiaal wel/niet voor wenst te gebruiken. Wordt achteraf bezwaar gemaakt tegen publicatie, dan moet je dit respecteren en (voor zover mogelijk) de publicatie verwijderen.

Een beroep op het *commercieel* belang is alleen mogelijk voor personen die een zogenaamde verzilverbare populariteit hebben. Sporters kunnen zich in de praktijk vaak met succes op het commerciële belang beroepen om publicatie tegen te gaan of daarvoor een redelijke vergoeding te eisen, ook als de afbeelding niet privacygevoelig is. De sporter moet dan wel aantonen dat zijn belang zwaarder weegt dan het belang van degene die het materiaal wil publiceren. Let dus op met het publiceren van afbeeldingen van sporters met een aanzienlijke populariteit.

Voorbeeld: profvoetballers
In 2013 is door de rechter beslist dat voor profvoetballers in Nederland geen absoluut recht bestaat op basis waarvan zij kunnen verhinderen dat hun portretten in wedstrijdverslagen worden afgebeeld (of daarvoor een fikse vergoeding kunnen vragen).
De informatievrijheid en de vrijheid van meningsuiting weegt in sommige gevallen dus zwaarder dan het portretrecht van professionele voetballers.

Onthoud dus dat je in de praktijk altijd een belangenafweging moet maken. Ontstaat er op enig moment discussie met een geportretteerde, vraag dan om deskundig juridisch advies.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 9: Webwinkels

In 't kort:

- Worden verkoopactiviteiten uitbesteed aan een externe leverancier, onderzoek dan goed wie verantwoordelijke en wie eventueel bewerker is. Sluit met eventuele bewerkers een bewerkersovereenkomst.
- Neem de regels rondom cookies en direct marketing in acht.
- Voorkom dat klanten worden verplicht om een account aan te maken.
- Informeer klanten over het privacy-beleid met een privacyverklaring.
- Zorg voor een passend beveiligingsniveau, met name bij het verwerken van betalingen.

9.1 Inleiding

Sommige sportorganisaties verkopen tickets en producten. Bij die verkoopprocessen worden persoonsgegevens verwerkt. Deze verwerkingen moeten uiteraard voldoen aan *alle* regels die we bespraken in hoofdstuk 2. We bespreken hierna enkele specifieke aandachtspunten rondom het verkoopproces.

Vooral bij online verkoopkanalen laten veel sportorganisaties hun verkoopactiviteiten geheel of gedeeltelijk uitvoeren door een derde. De webshop draagt dan vaak een naam die sterk is gerelateerd aan de sportorganisatie, maar in feite is het de leverancier die het proces zowel organiseert als uitvoert.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

De vraag of verkoopactiviteiten geheel of deels zijn uitbesteed is belangrijk om te bepalen wie verantwoordelijke is. Bij *volledige* uitbesteding (waarbij de leverancier handelt op eigen naam en rekening) is de leverancier meestal zelf verantwoordelijke. Beperkt de bemoeienis van de leverancier zich echter tot het technisch beheer van de webshop en regelt de sportorganisatie zelf de overige processen (verzending, incasseren betalingen etc.), dan is de sportorganisatie waarschijnlijk zelf verantwoordelijke. De leverancier is in dat laatste geval bewerker, zodat daarmee een bewerkersovereenkomst moet worden gesloten.

9.2 Doel en grondslag

Voor het afhandelen van bestellingen verwerkt de verkoper voornamelijk informatie in de volgende categorieën:

- Voor- en achternaam
- Contactgegevens
- Adresgegevens
- Ordergegevens
- Betalingsgegevens

De verkopende organisatie mag deze gegevens verwerken op grond van de uitvoering van een overeenkomst. Voor de verwerking van deze gegevens hoeft dus geen toestemming aan de betrokkenen te worden gevraagd, zolang deze slechts worden gebruikt voor het afhandelen van de bestelling.

Wil je de contactgegevens van bestaande klanten in de toekomst gebruiken om een commerciële aanbieding te sturen aan die klant, let dan goed op de regels voor direct marketing.

Let op!
Voorkom dat websitebezoekers zich moeten registreren met een account voordat ze een bestelling kunnen plaatsen. Als een klant namelijk enkel een ticket of product wil bestellen, zal de eis om te registreren meestal onredelijk zijn. Wil je desondanks dat klanten een account aanmaken, vraag dan in ieder geval uitdrukkelijk om toestemming van de betrokkene.

9.3 Direct marketing en cookies

Bij online verkoop heb je vrijwel altijd te maken met specifieke regelgeving voor cookies en direct marketing. Daarover kun je meer lezen in de paragrafen over cookies en direct marketing. We leggen daarin bijvoorbeeld uit of je klanten via e-mail aanbiedingen mag doen, en of je het gedrag van klanten via cookies mag analyseren.

9.4 Informatieplicht

Als verantwoordelijke moet je de betrokkene goed informeren over de wijze waarop je persoonsgegevens verwerkt. Voor bezoekers van webwinkels kun je daarvoor een privacyverklaring gebruiken, die je duidelijk zichtbaar op de website plaatst. Een modelverklaring is achterin dit handboek opgenomen. Het is verstandig om bezoekers die daadwerkelijk een bestelling

© CMS Derks Star Busmann N.V., 2017

plaatsen nog eens expliciet te wijzen op de privacyverklaring, nu juist van deze groep de meeste gegevens worden verwerkt. Verwijs tijdens het bestelproces dus uitdrukkelijk naar de privacyverklaring met een hyperlink.

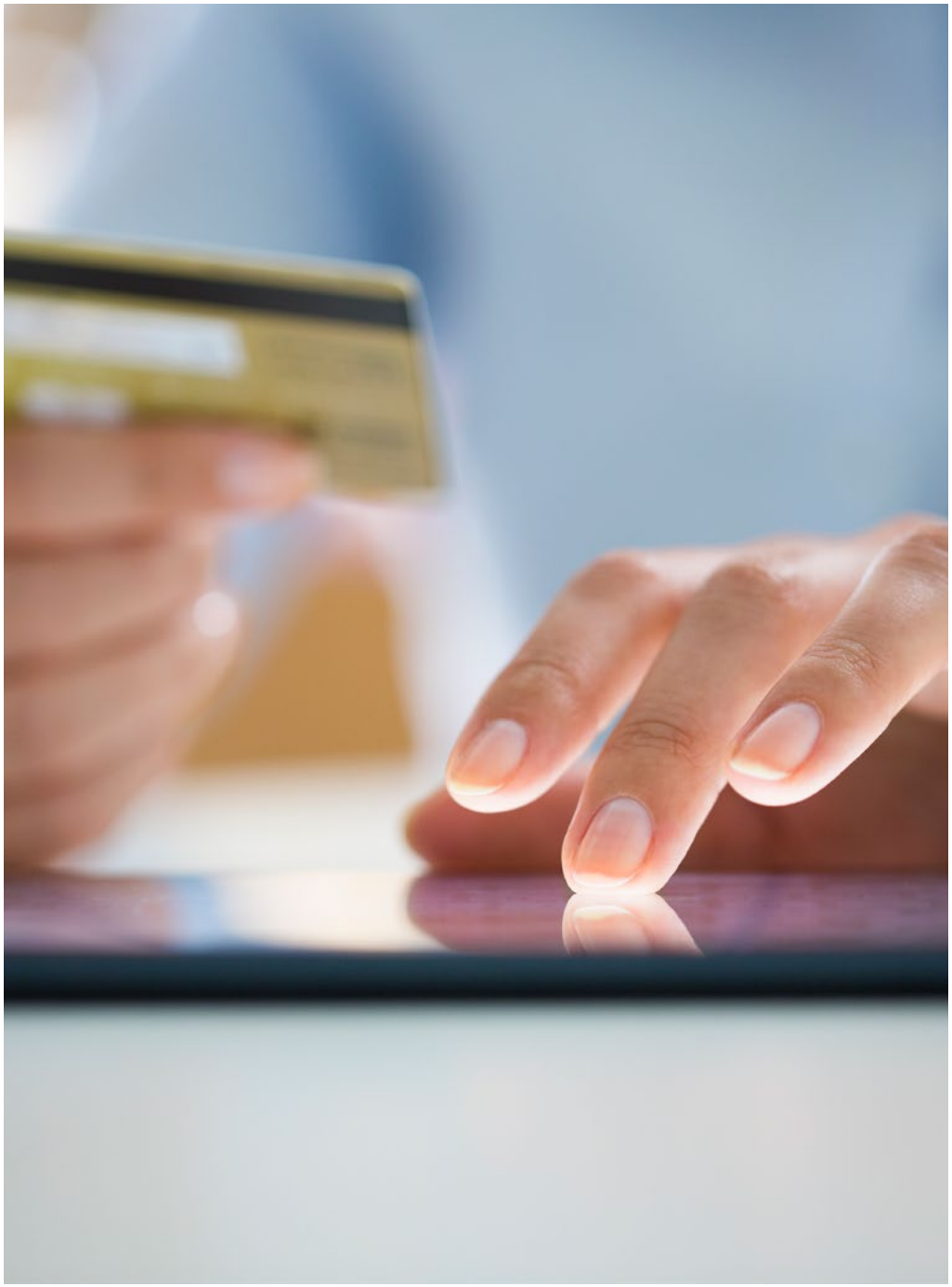
Let op!
Voor het informeren over cookies gelden bijzondere regels.

9.5 Bewaartermijn
Voor een geschikte bewaartermijn bij klant- en verkoopgegevens kun je deels aansluiten bij het Vrijstellingsbesluit. In principe bewaar je de persoonsgegevens niet langer dan twee jaar na afhandeling van de transactie. Sommige gegevens moeten op gerond van fiscale wetgeving worden bewaard voor een langere periode. Overleg dit met de financiële afdeling binnen de organisatie.

Sommige informatie zal je wellicht voor statistische, wetenschappelijke of historische doeleinden langer willen bewaren. Dat is toegestaan, maar zorg dan wel dat deze langer bewaarde gegevens niet alsnog voor andere doeleinden worden gebruikt. Kijk bovendien of er eventueel persoonsgegevens zijn die niet relevant zijn voor deze statistische (etc.) doeleinden, zodat je alleen de relevante informatie behoudt.

9.6 Delen met derden
Worden in het kader van de verkoopactiviteiten persoonsgegevens verstrekt aan derden, let dan goed op de 5 vuistregels voor het delen met derden.

9.7 Beveiliging
Bij online verkoopactiviteiten is het heel erg belangrijk dat persoonsgegevens passend worden beveiligd tegen datalekken. Betaalgegevens van klanten zijn immers extra interessant voor kwaadwillenden. Als je voor het technisch beheer van de webwinkel een externe IT-leverancier inschakelt, controleer dan goed of de contracten met deze leverancier voldoende recht geven op een up-to-date beveiliging. Deze afspraken kun je ook vastleggen in een bewerkersovereenkomst.



© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 10: Opleiding

In 't kort:
- Gebruik persoonsgegevens die je in het kader van de opleiding verkrijgt niet voor doeleinden die daarmee onverenigbaar zijn.
- Informeer deelnemers tijdens het aanmeldproces over het toepasselijke privacy-beleid.
- Publiceer persoonsgegevens van een deelnemer niet zomaar online, tenzij de deelnemer daar uitdrukkelijke toestemming voor geeft.
- Bewaar persoonsgegevens die gerelateerd zijn aan de opleiding niet langer dan noodzakelijk of pas eventueel anonimisering toe.

Bij het opleiden van sporters, arbiters en trainers verwerk je als verantwoordelijke sportorganisatie op allerlei manieren persoonsgegevens. Deze verwerkingen moeten uiteraard voldoen aan alle algemene regels uit de Wbp, waarover je uitgebreid kunt lezen in hoofdstuk 2. We geven hierna een paar specifieke aandachtspunten rondom opleidingen.

10.1 Doel en grondslag

De meeste verwerkingen in het kader van een opleidingsprogramma kun je relatief eenvoudig baseren op een gerechtvaardigd belang of de uitvoering van een overeenkomst, zolang je de informatie maar uitsluitend gebruikt voor de noodzakelijke processen rondom de opleiding.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

Daarbij gebruik je persoonsgegevens in categorieën zoals:
- deelnemerslijsten
- contactgegevens cursisten
- dieetwensen
- financiële administratie (debiteurs)
- contactgegevens docenten
- opleidingsresultaten
- ingeleverd huiswerk

Let op!
Ben je van plan om persoonsgerelateerde opleidingsinformatie openbaar te publiceren (denk aan deelnemerslijsten, uitslagen etc.), dan is het verstandig om daar specifiek toestemming voor te vragen aan de betrokkene. Je kunt meestal namelijk moeilijk volhouden dat een dergelijke publicatie strikt noodzakelijk is voor de opleiding. Je kunt deze toestemming bijvoorbeeld al vragen tijdens aanmelding.

Zorg dat je de persoonsgegevens niet gebruikt voor doeleinden die onverenigbaar zijn met het opleidingsdoel.

10.2 Verstrekking aan derden

Verstrek je persoonsgegevens van cursisten of docenten aan derden, neem dan altijd de daarbij geldende vuistregels in acht.

10.3 Informatieplicht

Zorg dat je cursisten (en eventueel docenten) vooraf informeert hoe je met hun gegevens omgaat. Een geschikte methode hiervoor is het opstellen van een privacyverklaring. Bij cursisten kun je dit doen op het moment van aanmelding. Verwijs op het aanmeldformulier naar de privacyverklaring, en zorg dat de verklaring eenvoudig kan worden geraadpleegd. Verwijs bij een digitaal formulier bijvoorbeeld met behulp van een hyperlink.

10.4 Bewaartermijn

Bewaar opleidingsgerelateerde persoonsgegevens niet langer dan noodzakelijk. Sommige informatie zal je wellicht voor statistische, wetenschappelijke of historische doeleinden langer willen bewaren. Denk bijvoorbeeld aan slagingspercentages, het aantal inschrijvingen of de leeftijd van de cursisten. Dat is mogelijk, maar zorg dan wel dat deze langer bewaarde gegevens niet alsnog voor *andere* doeleinden worden gebruikt. Kijk bovendien of er eventueel persoonsgegevens zijn die niet relevant zijn voor deze statistische (etc.) doeleinden, zodat je alleen de relevante informatie behoudt.

© CMS Derks Star Busmann N.V., 2017

Hoofdstuk 11: Personeel

In 't kort:

- Pas in sollicitatieprocedures geen verdergaande verwerkingen van persoonsgegevens toe dan strikt noodzakelijk is om een kandidaat op geschiktheid te beoordelen.
- Bij (gedeeltelijke) uitbesteding van de personeelsadministratie moet doorgaans een bewerkersovereenkomst worden gesloten met de leverancier.
- Houd er rekening mee dat voor het verwerken van informatie over zieke werknemers zeer strikte regels gelden.
- Wees transparant naar werknemers over de wijze waarop je toezicht uitoefent.
- Ga zorgvuldig om met het werken via Bring Your Own Device-programma's, en vraag bij de uitrol daarvan om deskundig advies.
- Let op de bijzondere regels die gelden voor de omgang met klokkenluiders.

In de dagelijkse praktijk verwerk je als werkgever allerlei persoonsgegevens van werknemers. Voldoende reden dus om een aantal specifieke verwerkingen uit te lichten.

11.1 Sollicitanten

Het doel van de sollicitatieprocedure is het vaststellen van de geschiktheid van een sollicitant voor de vacature. Bij het nemen van die beslissing wil je natuurlijk zoveel mogelijk informatie over de achtergrond en het opleidings- en arbeidsverleden van de kandidaat hebben.

Nooit vergeten: de privacy-principes

1. **Stel vast of je persoonsgegevens verwerkt**
   Een persoonsgegeven is elk gegeven over een levende en identificeerbare persoon. Vrijwel iedere handeling met een persoonsgegeven is een verwerking. Wees extra voorzichtig met gevoelige en bijzondere persoonsgegevens.
2. **Stel vast of je verantwoordelijke bent voor de verwerking**
   De verantwoordelijke is degene die beslist over het doel van en de middelen voor een verwerking.
3. **Stel vast of er een geldige grondslag bestaat voor de verwerking**
   Er zijn slechts zes grondslagen waarop een verwerking mag plaatsvinden. De voornaamste zijn (i) een gerechtvaardigd belang, (ii) uitvoering van een contract en (iii) toestemming van de betrokkene.
4. **Verlies de basisverplichtingen nooit uit het oog:**
   - Informeer waar nodig de betrokkene
   - Beveilig tegen onrechtmatig verwerking
   - Bewaar niet langer dan noodzakelijk
   - Sluit met bewerkers een bewerkersovereenkomst

Ook wil je kunnen toetsen of een kandidaat betrouwbaar is en of de door hem verstrekte informatie waarheidsgetrouw is. Het verzamelen van zulke informatie is een verwerking van persoonsgegevens. Je mag slechts persoonsgegevens verwerken als daar een geschikte grondslag voor is. Bij sollicitanten betekent dit dat je uitsluitend persoonsgegevens mag verwerken om aan een wettelijke verplichting te voldoen of (op grond van een gerechtvaardigd belang) om te beoordelen of de sollicitant geschikt en betrouwbaar is. Deze gegevens moet je zodanig verzamelen dat de inbreuk op de privacy van de sollicitant zo klein mogelijk is.

Let op!
Als je aan een sollicitant toestemming zou vragen om bepaalde informatie te (laten) verzamelen, dan is het voor hem vrijwel onmogelijk om die toestemming te weigeren. Toestemming van de sollicitant is daarom meestal geen geldige grondslag voor het verwerken van persoonsgegevens.

Het spreekt voor zich dat je contactgegevens van de sollicitant nodig hebt om hem te kunnen uitnodigen voor een sollicitatiegesprek. Die persoonsgegevens mag je dus verwerken. Maar mag je ook van iedere sollicitant verlangen dat hij meewerkt aan een medische keuring of pre-employment screening? Wat mag je wel/niet vragen en naar welke informatie mag je zelf op zoek gaan?

Internetzoekopdracht

Veel werkgevers voeren een internetzoekopdracht uit bij de beoordeling wie wordt uitgenodigd voor een sollicitatiegesprek of ter voorbereiding van dat gesprek. Wanneer je dat doet, bijvoorbeeld op sociale media, beperk je dan tot zakelijke en relevante bronnen. Print ook geen informatie die niet relevant is voor de beoordeling van de geschiktheid en de betrouwbaarheid van de kandidaat en sla die informatie ook niet op.

Geen vragen over gezondheid, zwangerschap of kinderwens

Het is verboden om een sollicitant vragen te stellen over zijn gezondheid, zijn ziekteverzuim bij ex-werkgevers of om daarover bij anderen inlichtingen in te winnen. Ook vragen over eventuele zwangerschap of kinderwens zijn verboden. Een medische keuring kan slechts onderdeel uitmaken van de sollicitatieprocedure als de functie bijzondere eisen op het punt van de medische geschiktheid stelt. Denk bijvoorbeeld aan topsporters en trainers met wie een arbeidsovereenkomst wordt gesloten.

Screening

Screening komt als onderdeel van sollicitatieprocedures steeds vaker voor. Denk bijvoorbeeld aan het natrekken van een C.V., het verzoeken om een verklaring omtrent gedrag of het verzamelen van financiële informatie.

In welke mate screening is toegestaan, hangt af van de aard van de functie waarvoor iemand solliciteert en de risico's die met die functie samenhangen. Voor de meeste functies zal echter gelden dat je niet zomaar zelf onderzoek mag doen naar een eventueel strafrechtelijk

© CMS Derks Star Busmann N.V., 2017

verleden van de sollicitant. Dat is vaak ook niet nodig. Je kunt immers om een verklaring omtrent gedrag vragen waaruit blijkt dat de sollicitant geen relevant strafbaar feit heeft gepleegd. Soms rechtvaardigt de aard van de functie specifiek onderzoek juist wel. Financiële functies, waarbij een werknemer toegang heeft tot aanzienlijke geldbedragen, kennen bijvoorbeeld een groter risico op fraude of diefstal dan andere functies. Bij dergelijke risico's mag je daarom onder omstandigheden bijvoorbeeld verzoeken om informatie over de (actuele) financiële positie van de sollicitant.

Tips

- Zorg ervoor dat je (potentiële) sollicitanten vooraf (bijvoorbeeld in de vacature) informeert over de verschillende onderdelen van de sollicitatieprocedure, zoals een assessment, een medische keuring of een verplicht antecedentenonderzoek.
- Zet aanvullende selectiemiddelen (zoals assessments, screening of antecedentenonderzoeken) pas in een zo laat mogelijk stadium van de procedure in. Je voorkomt daarmee dat onnodig inbreuk wordt gemaakt op privacy van sollicitanten die al in een vroeg stadium afvallen.
- Controle van de identiteit van de sollicitant vindt (waar nodig) plaats aan de hand van het originele identiteitsbewijs. Je mag daarvan geen kopie maken!

Bewaartermijn

Gegevens van afgewezen sollicitanten bewaar je in principe niet langer dan vier weken na het einde van de sollicitatieprocedure. Als de sollicitant daarom vraagt moet je de gegevens eerder verwijderen. Als het voor jouw organisatie noodzakelijk is om bij te houden dat iemand eerder gesolliciteerd heeft, bijvoorbeeld met het oog op toekomstige sollicitatieprocedures, dan kun je een langere bewaartermijn toepassen. Het is belangrijk dat je alleen gegevens bewaart die voor dát doel noodzakelijk zijn (zoals de naam van de sollicitant, de namen van personen die gesprekken hebben gevoerd en een korte omschrijving (reden van afwijzing). Bewaar dus niet het volledige dossier van de sollicitatieprocedure. Bepaal zelf een passende maximale bewaartermijn voor deze gegevens.

11.2 Personeelsadministratie

De salaris- en personeelsadministratie van werkgevers bevatten persoonsgegevens van hun werknemers. Het gaat daarbij vooral om gegevens die de werkgever moet verwerken om aan een wettelijke verplichting te voldoen (zoals het bewaren van een kopie van een identiteitsbewijs), gegevens die nodig zijn om de arbeidsovereenkomst uit te voeren (zoals het bankrekeningnummer van de werknemer en verslagen van functioneringsgesprekken) en gegevens die nodig zijn om een gerechtvaardigd belang van de werkgever te behartigen.

De personeelsadministratie moet allereerst voldoen aan alle algemene eisen die besproken zijn in Hoofdstuk 2. Daarnaast wordt de werknemer beschermd door de verplichting van de werkgever om zich als een goed werkgever te gedragen. Je moet er in ieder geval voor zorgen dat de gegevens die je opslaat correct zijn, dat je alleen noodzakelijke gegevens verwerkt, dat werknemers weten waarom je bepaalde gegevens aanhoudt, dat de gegevens goed beveiligd zijn en dat werknemers hun inzage- en correctierecht kunnen uitoefenen. We bespreken hierna de belangrijkste aandachtspunten.

Digitale administratie

Steeds meer werkgevers gebruiken alleen nog maar een digitale personeelsadministratie en digitale personeelsdossiers. Dit is toegestaan. Houd er wel rekening mee dat de Belastingdienst voorwaarden stelt aan het omzetten van een papieren administratie naar een digitale administratie. Het is mogelijk om vooraf overleg te voeren met de Belastingdienst of aan alle voorwaarden voor omzetting is voldaan. Dit voorkomt onaangename verrassingen achteraf. Onthoud dat ook het beheer van je papieren administratie als het verwerken van persoonsgegevens wordt gezien en dus moet voldoen aan dezelfde eisen als een digitale personeelsadministratie.

Uitbesteden administratie aan bewerkers

Als je voor de uitvoering van de arbeidsovereenkomst een derde inschakelt (zoals een salarisadministratiekantoor), sluit met die partij dan een bewerkersovereenkomst. Zorg dat je goed begrijpt hoe dienstverleners met jouw data omgaan. Zo worden persoonsgegevens van werknemers wellicht opgeslagen op buitenlandse servers: je moet als verantwoordelijke dan rekening houden met het doorgifteverbod. Maak ook afspraken met bewerkers over de protocollen die gelden bij eventuele datalekken.

Bewaartermijn

De richtlijn uit het Vrijstellingsbesluit is dat gegevens uit de salaris- en personeelsadministratie uiterlijk twee jaar na einde dienstverband worden verwijderd, tenzij het langer bewaren van de persoonsgegevens noodzakelijk is om te voldoen aan een wettelijke bewaarplicht. Een voorbeeld van een relevante wettelijke bewaarplicht is de fiscale bewaarplicht van zeven jaar voor gegevens uit de salarisadministratie. Ook als er geen wettelijke bewaarplicht van toepassing is, kan het noodzakelijk zijn om gegevens langer dan twee jaar na einde dienstverband te bewaren. Daarvan kan bijvoorbeeld sprake zijn als je als werkgever bepaalde informatie nodig hebt om je te verweren in een juridische procedure.

11.3 Zieke werknemers

Als werkgever mag je in principe geen gezondheidsgegevens opvragen of opslaan. Je mag die informatie wel opvragen als dat noodzakelijk is om te voldoen aan een wettelijke verplichting, een pensioenregeling of een CAO. Informatie die nodig is voor de re-integratie van een zieke werknemer mag je als werkgever ook gebruiken.

Ziekmelding

Bij een ziekmelding mag je *uitsluitend* de volgende gegevens registeren: het telefoonnummer en (verpleeg)adres van de werknemer, de verwachte duur van verzuim, informatie die nodig is voor de werkoverdracht en of de werknemer ziek is door een arbeidsongeval of een verkeersongeval. Je mag ook registreren dat de werknemer een 'vangnetter' is. Dit zijn werknemers met een hoog ziekterisico, zoals orgaandonoren en zwangere werkneemsters.

© CMS Derks Star Busmann N.V., 2017

Volgens de huidige beleidsregels van de Autoriteit Persoonsgegevens mag je *niet* registreren in *welke categorie* vangnetbepalingen de werknemer valt.

Overige informatie mag je in principe niet registreren, ook niet met toestemming van de werknemer. Zelfs wanneer de werknemer uit zichzelf aan zijn leidinggevende vertelt wat zijn diagnose is, mag de werkgever die informatie niet verwerken.

Uitzondering

Soms is het noodzakelijk dat collega's weten dat een werknemer ziek is of dat zij eerste hulp kunnen verlenen. Denk bijvoorbeeld aan een werknemer met een ernstige allergie of epilepsie. In die bijzondere gevallen mag je, met toestemming van de werknemer, de medische aandoening van de werknemer wel registreren en directe collega's van de werknemer daarover informeren.

Re-integratiedossier

Om aan zijn re-integratieverplichtingen te voldoen, moet de werkgever de maatregelen treffen en aanwijzingen geven die redelijkerwijs nodig zijn om de werknemer zijn eigen of andere passende arbeid te laten verrichten. De afspraken over en de inzet van de werkgever en werknemer in het re-integratietraject moeten worden vastgelegd in een re-integratiedossier.
In het re-integratiedossier mag je géén informatie opnemen over de *aard en de oorzaak* van de ziekte van de werknemer. De werkgever mag wel registreren wat de werknemer wel en niet kan doen, oftewel wat zijn functionele mogelijkheden en beperkingen zijn.

Bewaartermijn bij verzuim en re-integratie

De werkgever mag informatie over een ziekmelding in principe maximaal twee jaar na het einde van een dienstverband bewaren. Het re-integratiedossier moet in principe binnen twee jaar na de afronding van de re-integratie worden verwijderd. Is de sportorganisatie een eigenrisicodrager Ziektewet of WGA? Dan gelden langere bewaartermijnen. De wet bepaalt dat, als je eigenrisicodrager bent voor de Ziektewet, het medisch dossier tien jaar en overige gegevens vijf jaar moeten worden bewaard. Nota bene: het medisch dossier wordt opgesteld en bewaard door de bedrijfsarts. Als je eigenrisicodrager WGA bent, dan is het noodzakelijk om gegevens over de medische keuring van de werknemers tien jaar te bewaren, namelijk voor de duur dat je als werkgever zelf de WGA-uitkering aan de werknemer moet betalen.
Het kan soms noodzakelijk zijn om informatie over verzuim en re-integratie van de werknemer langer te bewaren, bijvoorbeeld omdat partijen in juridische procedures verwikkeld zijn waarin de werkgever de stukken nodig heeft als bewijs.

Veranderen van arbodienst/bedrijfsarts

Als de werkgever van arbodienst/bedrijfsarts wisselt, dan zal ook sprake zijn van het overdragen van persoonsgegevens (dossieroverdracht). De oude arbodienst/bedrijfsarts mag op verzoek van de werkgever alle gegevens over de gezondheid van werknemers waarop geen medisch beroepsgeheim rust (zoals administratieve verzuimgegevens) overdragen aan de nieuwe arbodienst/bedrijfsarts.

Andere gegevens waarop wel medisch beroepsgeheim rust, mag de bedrijfsarts alleen aan een andere bedrijfsarts overdragen voor zover het gaat om lopende ziektegevallen of om werknemers die binnen vier weken na betermelding opnieuw uitvallen. Zorg ervoor dat de betrokken werknemers vooraf worden geïnformeerd en stel ze in de gelegenheid om bezwaar te maken.

Tips

- Beperk de groep personen die toegang heeft tot verzuim- en re-integratiegegevens van werknemers zoveel mogelijk;
- Zorg dat personen die toegang hebben tot verzuim- en re-integratiegegevens aan een geheimhoudingsbeding gebonden zijn. Zorg dat het technisch onmogelijk is dat onbevoegde personen deze gegevens kunnen inzien. Gebruik minimaal afgeschermde en beveiligde (digitale) dossiers;
- Ontmoedig het onrechtmatig verwerken van medische gegevens van werknemers door geen open invulvelden in (ziekte)verzuimregistratieformulieren op te nemen;
- Meer informatie vind je in de Beleidsregels zieke werknemer van de Autoriteit Persoonsgegevens

11.4 Toezicht

Controle e-mail, internet en telefoon

E-mail-, internet- en telefoonverkeer wordt beschermd door het recht op privacy. De werknemer heeft ook recht op bescherming van zijn privéleven op de werkplek. Zo mag een werknemer onder werktijd privécontacten onderhouden zolang dat geen nadelige invloed heeft op de uitvoering van zijn taken of op de werksfeer. Als werkgever moet je de privacy van die contacten waarborgen.

Controleer je het e-mail-, internet- of telefoongebruik van werknemers in je organisatie, dan verwerk je persoonsgegevens. De grondslag voor deze verwerking is een gerechtvaardigd belang, zoals het kunnen vaststellen dat een werknemer communicatiemiddelen van jouw organisatie misbruikt (bovenmatig privégebruik), communicatiemiddelen gebruikt voor berichten met een onaanvaardbare inhoud (zoals discriminatie) of het verzamelen van bewijs. Denk in dat laatste geval bijvoorbeeld aan de werknemer die via zijn zakelijke emailadres correspondeert over verboden nevenactiviteiten, of vertrouwelijke informatie doorspeelt aan derden.

Het heeft de voorkeur om verboden gedrag, zoals het bezoeken van bepaalde websites, zoveel mogelijk technisch onmogelijk te maken. Om een werknemer te kunnen aanspreken op (verboden) gedrag moet voor hem duidelijk (kunnen) zijn wat wel en niet mag. We raden aan om een gedragscode op te stellen waarin je uitlegt:

- welk gedrag wel en niet is toegestaan;
- wat de sancties zijn bij overtreding;
- dat sprake kan zijn van toezicht, en
- dat daarbij in specifiek te benoemen gevallen ook gecontroleerd kan worden op inhoud van berichten, gesprekken en/of internetgebruik.

© CMS Derks Star Busmann N.V., 2017

Denk bij het opstellen van een beleid ook aan situaties, zoals vakantie of ziekte, waarbij eveneens een gerechtvaardigd belang kan bestaan voor toegang tot de zakelijke e-mailaccount van de werknemer.

Als er een legitieme grondslag bestaat om het e-mail-, internet- of telefoongebruik van werknemers te controleren, dan moet je dit zorgvuldig aanpakken. De volgende vuistregels kunnen daarbij helpen:

- Definieer het doel van het onderzoek, en stem de onderzoeksmethode en omvang van het onderzoek hierop af. Is sprake van een serieus vermoeden van een ernstige misstand (zoals fraude of diefstal), dan is een grotere inbreuk op de privacy van de werknemer toegestaan dan bij een vermoeden van een relatief onschuldig vergrijp. Onderzoek niet meer of langer dan strikt noodzakelijk is voor het geformuleerde doel.
- Ontzie waar mogelijk (de inhoud van) e-mails die duidelijk privé zijn.
- Gebruik waar mogelijk software om de inhoud van communicatie gericht te doorzoeken (content-filtering). Hiermee beperk je het risico dat je kennisneemt van zaken die irrelevant zijn voor het onderzoek.
- Houd de groep van personen die toegang heeft tot de gegevens zo klein mogelijk en zorg dat ze gebonden zijn aan een geheimhoudingsbeding.
- Laat correspondentie en telefoongesprekken van leden van de ondernemingsraad, met de bedrijfsarts of met een vertrouwenspersoon altijd buiten het onderzoek.
- Informeer de werknemer dat een onderzoek heeft plaatsgevonden zodra het onderzoek dit toelaat.

Bewaartermijn

Het Vrijstellingsbesluit geeft als richtlijn dat persoonsgegevens die worden verwerkt bij ICT-gebruik door werknemers uiterlijk 6 maanden nadat ze zijn verkregen of twee jaar na einde dienstverband worden verwijderd. Het kan onder omstandigheden noodzakelijk zijn dat je gegevens langer bewaard, bijvoorbeeld in verband met een lopende procedure.

Cameratoezicht

Maak je gebruik van cameratoezicht, dan verwerk je persoonsgegevens. We bespreken kort waar je daarbij zoal op moet letten.

Let op!
De aandachtspunten die we hier bespreken zijn van toepassing op het gebruik van zichtbare camera's. Heimelijk cameratoezicht mag je alleen in hele specifieke uitzonderingsgevallen inzetten. Zorg er voor dat werknemers er van op de hoogte zijn dat heimelijk cameratoezicht kan worden toegepast (bijvoorbeeld door dit in het personeelsreglement op te nemen).

Toegangsbeveiliging

De meest voorkomende vorm van cameratoezicht vindt plaats door middel van zichtbare camera's en heeft als doel om personen, gebouwen, terreinen en eigendommen te beschermen (wat doorgaans een gerechtvaardigd belang is). Denk daarbij aan de inzet van camera's bij de ingang van het kantoorpand of een parkeergarage. Als jij niet degene bent die de beslissingen neemt over (de inzet van) het cameratoezicht, maar de verhuurder van het kantoorpand die beslissing neemt, overweeg dan eerst of je wel verantwoordelijke bent voor de verwerking. Ben je geen verantwoordelijke, vraag dan wel (als goed werkgever) na hoe de verhuurder ervoor zorgt dat het cameratoezicht zorgvuldig plaatsvindt.

Cameratoezicht moet proportioneel zijn. Dit betekent dat je niet meer opneemt dan noodzakelijk is. Gebruik je een camera bijvoorbeeld voor toegangscontrole, dan zal het meestal voldoende zijn om beelden te maken van de toegangsdeuren. De hele receptie, inclusief de werkplek van de receptiemedewerker, hoeft dus niet in beeld te worden gebracht. In ruimtes waarin privacy mag worden verwacht, zoals toiletten of kleedkamers, is cameratoezicht uiteraard niet toegestaan. Houd er verder rekening mee dat als je camera's inzet voor toegangsbeveiliging, deze beelden niet bruikbaar zijn voor de beoordeling van het functioneren van werknemers. Dat doel vindt de Autoriteit Persoonsgegevens onverenigbaar met het doel (beveiliging) waarvoor de beelden zijn verzameld.

Camerabeelden mogen niet langer worden bewaard dan noodzakelijk is. Het Vrijstellingsbesluit geeft een bewaartermijn van vier weken als richtlijn.

Tips

- Camerabeelden moeten uiteraard goed worden beveiligd. Zorg er bijvoorbeeld voor dat de groep mensen die toegang heeft tot de beelden zo klein mogelijk is. Log ook wat er met beelden is gedaan, bijvoorbeeld pogingen om toegang tot de beelden te verkrijgen.
- De betrokkene moet worden geïnformeerd over het cameratoezicht vóórdat hij daadwerkelijk worden gefilmd. Die informatie kun je onder meer verstrekken door een bordje bij de ingang.
- Meer informatie vind je in de Beleidsregels Cameratoezicht van de Autoriteit Persoonsgegevens.

Verzoek om gegevens van politie of toezichthouder

Er kan zich een situatie voordoen dat de politie, een overheidsinstantie of een toezichthouder verzoekt om informatie over een werknemer. Een werkgever mag persoonsgegevens van werknemers (of andere natuurlijke personen) slechts doorgeven aan derden wanneer aan de voorwaarden voor doorgifte van die gegevens is voldaan. Die regels gelden ook voor doorgifte van persoonsgegevens aan de hiervoor genoemde instanties. Ben je wettelijk verplicht om de opgevraagde informatie te verstrekken, dan mag je deze doorgeven. De politie kan bijvoorbeeld bepaalde informatie vorderen als een werknemer wordt verdacht van een misdrijf.

© CMS Derks Star Busmann N.V., 2017

Beoordeel in gevallen waarin je informatie aan instanties verstrekt ook zorgvuldig of je de betrokken werknemer(s) daarover mag of moet informeren. Je hoeft de werknemer bijvoorbeeld niet te informeren wanneer dat in het belang is van de voorkoming, opsporing of vervolging van strafbare feiten. In bepaalde gevallen is dit zelfs verboden.

11.5 Bring Your Own Device

Bring Your Own Device ("BYOD") betekent dat werknemers bij hun werkzaamheden een eigen telefoon of laptop gebruiken. Dit kan praktisch zijn, maar kan ook tot gevolg hebben dat de werknemer zakelijke gegevens verwerkt op zijn apparaat. Ook voor deze verwerkingen ben je verantwoordelijke. Bij BYOD moet je dus zorgen dat persoonsgegevens volledig in overeenstemming met de Wbp (zie Hoofdstuk 2) worden verwerkt en niet in verkeerde handen vallen.

Tips

- Vraag om deskundig IT-advies vóórdat je BYOD toestaat. Je moet nauwkeurig in kaart brengen welke gegevens de werknemer wel en niet via de eigen telefoon of computer van de werknemer mag versturen. Je moet ook specifieke BYOD-beveiligingsmaatregelen treffen. Er zijn veel dienstverleners die je daarbij kunnen assisteren.
- Stel een duidelijk intern personeelsbeleid op en maak dit beschikbaar voor het personeel. Leg precies uit wat wel en niet mag en eis dat werknemers hun software up-to-date houden.
- Zorg dat bedrijfs- en privégegevens duidelijk gescheiden blijven, bijvoorbeeld door het gebruik van een zakelijke applicatie.
- Bedenk hoe bedrijfsinformatie door de werknemer bij uitdiensttreding weer veilig aan de werkgever kan worden overgedragen.

11.6 De ondernemingsraad

Organisaties waarin in de regel 50 of meer personen werkzaam zijn, zijn verplicht om een ondernemingsraad in te stellen. Als organisatie met een ondernemingsraad kun je bepaalde besluiten slechts nemen na instemming van de ondernemingsraad. Daarbij gaat het onder meer om het vaststellen, wijzigen of intrekken van privacy-beleid bij werknemers, zoals het beleid over de controle van internet- en e-mailgebruik of over cameratoezicht.

11.7 Klokkenluiders

De klokkenluidersregeling

Sinds 1 juli 2016 bestaat het Huis voor klokkenluiders (het "Huis"). Een werknemer die (op redelijke gronden) vermoedt dat sprake is van een misstand in de organisatie van zijn werkgever, kan bij het Huis terecht voor informatie, advies en ondersteuning. Hij kan het Huis ook verzoeken om een onderzoek in te stellen naar de vermeende misstand en de manier waarop de werkgever zich tegen de werknemer heeft gedragen na de melding.

Werkgever en werknemer zijn hier ruime begrippen. Iedereen die arbeid laat verrichten of heeft laten verrichten kwalificeert als werkgever. Iedereen die op enige manier arbeid verricht of heeft verricht, is een 'werknemer'. Zzp'ers en vrijwilligers zijn dus ook werknemer.

Ook als je uitsluitend werkt met vrijwilligers kun je dus met klokkenluiders te maken krijgen.

Ben je verplicht om een ondernemingsraad in te stellen, dan ben je verplicht om een klokkenluidersregeling op te stellen die voldoet aan de eisen van de wet. Je kunt ook vrijwillig een klokkenluidersregeling implementeren. Kleinere organisaties kunnen overwegen om, individueel of met verschillende bonden gezamenlijk, een externe vertrouwenspersoon aan te wijzen om de onpartijdige en snelle beoordeling en afwikkeling van meldingen mogelijk te maken.

Heeft jouw onderneming een ondernemingsraad, denk er dan aan dat de ondernemingsraad een instemmingsrecht heeft bij het vaststellen, wijzigen of intrekken van een klokkenluidersregeling.

Privacy & klokkenluiders

Via de meldingsprocedure zullen persoonsgegevens worden verwerkt. Daarvoor ben je verantwoordelijke, ook als je gebruikmaakt van een externe vertrouwenspersoon. Houd bij het opstellen van de klokkenluidersregeling dus rekening met alle algemene regels voor het verwerken van persoonsgegevens (zie Hoofdstuk 2).

Welke misstanden?

De wet kwalificeert een misstand als een schending van een wettelijk voorschrift, een gevaar voor de volksgezondheid, een gevaar voor de veiligheid van personen, een gevaar voor de aantasting van het milieu, een gevaar voor het goed functioneren van de openbare dienst of een onderneming als gevolg van een onbehoorlijke wijze van handelen of nalaten waarbij het maatschappelijk belang in het geding is. Een interne klokkenluidersprocedure kan ook worden opengesteld voor andere meldingen waarbij het maatschappelijk belang niet in het geding is maar die wel – binnen de organisatie – van groot belang zijn.

Houd er rekening mee dat een klokkenluidersprocedure niet de plaats moet innemen van de normale procedures via de bestaande kanalen (leidinggevenden, HRM, ondernemingsraad, etc.): stel de procedure dus alleen open voor *substantiële* misstanden.

Informeren van betrokkenen

Het is belangrijk om werknemers en vrijwilligers actief te informeren over het bestaan van de klokkenluidersregeling. Daarmee voorkom je zoveel mogelijk dat de procedure een dode letter wordt. Leg daarbij uit waarvoor de procedure is bedoeld (melden van substantiële misstanden die niet anders kunnen worden gemeld) en hoe de procedure in zijn werk gaat. Leg ook uit hoe de belangen van de betrokkene die onderwerp is van de melding worden beschermd.

Behandel de gegevens van de melder vertrouwelijk en maak zijn gegevens slechts kenbaar aan de personen die met het onderzoek zijn belast. Deze gegevens dienen niet met de in de melding genoemde betrokkene te worden gedeeld, tenzij de melder een valse of lasterlijke melding heeft gedaan. Dan geldt deze bescherming niet.

© CMS Derks Star Busmann N.V., 2017

Beveiliging

Persoonsgegevens die verband houden met de melding moeten worden opgeslagen in een aparte afgeschermde omgeving, die niet toegankelijk is voor andere personen dan die met de afwikkeling van de melding zijn belast.

Andere beveiligingsmaatregelen zijn het versleutelen van correspondentie en het beveiligd opslaan van eventuele fysieke dossiers (waaronder een clean desk policy). Daarnaast dienen de personen die belast zijn met het onderzoek een geheimhoudingsbeding te tekenen.

Tips

- Gebruikt de organisatie een externe vertrouwenspersoon? Zorg dan voor een goede bewerkersovereenkomst en bepaal daarin o.a. dat de externe partij zich committeert aan de (privacy-waarborgen uit de) toepasselijke klokkenluidersregeling en de vertrouwelijkheid en beveiliging van dossiers.
- Anoniem melden moet mogelijk zijn, maar ontmoedig dit zoveel mogelijk om ongegronde meldingen te voorkomen. Informeer werknemers bovendien dat misbruik van de regeling kan leiden tot disciplinaire maatregelen.
- De groep personen die met het onderzoek is belast moet zo klein mogelijk zijn en losstaan van de afdeling personeelszaken.

© CMS Derks Star Busmann N.V., 2017

Bijlage: FAQ Privacy Impact Assessment

VRAAG 1 - Wat is een PIA en waarom voer je deze uit?
Een term die bij privacy regelmatig opduikt is Privacy Impact Assessment (PIA). Een PIA is een onderzoek naar de privacy-risico's van een nieuwe of gewijzigde verwerking van persoonsgegevens. Die vernieuwing of wijziging kan bijvoorbeeld een nieuw product of een nieuwe dienst zijn, maar ook de organisatie van een evenement of een nieuw samenwerkingsverband.

Een PIA voer je uit bij het vermoeden dat de (nieuwe/gewijzigde) verwerking een hoog privacy-risico kan veroorzaken voor de betrokkene. Wat 'hoog' is, is hier moeilijk te duiden. Verwerkingen die ogenschijnlijk onschuldig zijn, kunnen soms namelijk wel degelijk een behoorlijk negatieve impact hebben. Twijfel je of een PIA noodzakelijk is, vraag dan om deskundig advies.

Voorbeeld: verplaatsing administratie naar 'de cloud'
Als je als sportbond besluit om een deel van de administratie te verplaatsen naar een online applicatie, dan heeft dit onmiddellijk allerlei gevolgen voor de persoonsgegevens die zich in die administratie bevinden. Denk bijvoorbeeld aan de betrokkenheid van de hostingprovider, beveiliging, eventuele hosting buiten de EER, etc. Bij de ingebruikname van cloud-applicaties ontstaan dus allerlei nieuwe risico's waarmee je als verantwoordelijke rekening moet houden.

Een PIA kan een belangrijke invloed hebben op de manier waarop je processen in de organisatie vormgeeft. Blijkt uit de PIA bijvoorbeeld dat er negatieve risico's ontstaan door de beoogde verwerking, dan moeten maatregelen worden getroffen om deze te vermijden of beperken. Soms blijkt uit de PIA zelfs dat een verwerking dermate risicovol is, dat deze niet (in de bedachte vorm) mag plaatsvinden. Dat wil je natuurlijk op tijd weten. Zorg daarom dat je de PIA tijdig opstart (zie vraag 6).

Bij goed gebruik is een PIA niet alleen een prima middel voor risicobeheersing, maar ook een middel om te bewaken dat je handelt volgens de wettelijke privacy-regels (zie hoofdstuk 2).

Let op!
Het uitvoeren van PIA's is vanaf mei 2018 (zodra de Verordening in werking treedt) in een aantal scenario's gevallen **wettelijk verplicht**. Zorg dus dat je als organisatie voor die tijd al enige ervaring opdoet.

Een PIA is overigens niet alleen nuttig voor de situaties die de Verordening voorschrijft. De Verordening gaat namelijk uit van een *voorafgaande* risicotoets. Het is ook mogelijk om een PIA toe te passen op *bestaande* processen, hoewel het treffen van maatregelen dan natuurlijk soms lastiger is.

VRAAG 2 - Hoe verloopt een PIA?
Een PIA beantwoordt doorgaans de volgende vragen:

1. Hoe worden persoonsgegevens verwerkt in het onderzochte proces?
2. Welke risico's zijn aan de verwerking verbonden?
3. Welke maatregelen zijn mogelijk om die risico's te vermijden of te beheersen?

De volgorde van deze vragen stuurt de manier waarop de PIA meestal wordt uitgevoerd. Je doorloopt een PIA over het algemeen in de volgende stappen.

Stap 1: Stel vast of een PIA is vereist
Zie het antwoord op vraag 2.

Stap 2: Bepaal wie de PIA gaat uitvoeren
Zie het antwoord op vraag 3.

Stap 3: Breng het object van onderzoek en de verwerkingen in kaart
De PIA begint met het vaststellen welk soort verwerkingen plaatsvinden door welke partijen binnen de onderzochte processen. Meestal doe je dit aan de hand van een vragenlijst, waarbij je de resultaten vastlegt in tabellen. Let op dat je álle relevante verwerkingen in kaart brengt. Je gebruikt dezelfde gegevens immers vaak voor meerdere doelstellingen tegelijkertijd.

Stap 4: Stel vast wat de risico's zijn
Het vaststellen van de relevante risico's kun je doen aan de hand van het invullen van vragenlijsten. Wij bevelen aan om gebruik te maken van de NOREA-vragenlijst.

Stap 5: Bepaal hoe je risico's kan beperken of vermijden
De uitdaging in deze stap is vooral het kiezen van de juiste maatregel. Voor veel scenario's bestaat echter 'good practice', oftewel een algemeen geaccepteerde oplossing. Welke maatregel je moet treffen hangt natuurlijk volledig af van (de omvang van) het risico. Raadpleeg bij twijfel een deskundige.

Een PIA is nutteloos als het niet leidt tot concrete acties en taakverdelingen. Gebruik dus niet vage beschrijvingen ("de betrokkene moet goed worden geïnformeerd bij dit traject"), maar geef concreet aan wie binnen welke deadline verantwoordelijk is voor de uitvoering van bepaalde acties. Dat klinkt logisch, maar het vertalen van een tekst uit de PIA naar een uitvoerbare actie kan best lastig zijn. Je vergroot de kans op succesvolle doorvoering door de risico's en maatregelen zo helder mogelijk in de PIA te duiden. Stuur een IT-er bijvoorbeeld niet het bos in met de actie "zorg dat de beveiliging op orde is". Tegen welk soort beveiligingsinbreuken moet immer worden beschermd? En wanneer is een maatregel goed genoeg?

© CMS Derks Star Busmann N.V., 2017

Stap 6: Rapporteer de bevindingen
Meestal zal je gedurende het onderzoek allerlei bevindingen opschrijven (al dan niet in de vorm van antwoorden op vragenlijsten), die vaak nog worden aangepast zolang de PIA nog wordt uitgevoerd. Zorg ervoor dat de definitieve uitkomst van de PIA goed wordt gedocumenteerd. Voor het opstellen van de rapportage kun je gebruikmaken van het model van NOREA (zie vraag 4).

VRAAG 3 - Wie betrek je bij een PIA?
Bij PIA's geldt dat je niet zozeer bent aangewezen op personen met kennis van het privacy-recht, maar vooral sterk afhankelijk bent van mensen die in detail begrijpen hoe een project/verwerking is vormgegeven. Deze personen weten namelijk vaak het beste welke persoonsgegevens op welke manier voor welk doel worden verwerkt. Denk bijvoorbeeld aan de IT'ers die nieuwe software implementeren, of de coördinator van een evenement. Bovendien zijn zij meestal degene die maatregelen kunnen voorstellen om bepaalde risico's te beheersen. Zorg wel dat je één persoon aanwijst die de uitvoering van de PIA coördineert en verantwoordelijk wordt is voor wat in het PIA-rapport wordt vastgelegd. Kom je er niet uit, schakel dan een privacy-deskundige in.

VRAAG 4 - Is er een model beschikbaar om de PIA uit te voeren?
Ja, er is online veel materiaal te vinden dat je kunt gebruiken om een PIA uit te voeren. Deze modellen bestaan bijvoorbeeld uit templates en vragenlijsten. Wij bevelen sterk aan om gebruik te maken van het kosteloos beschikbare model van NOREA, de beroepsorganisatie van IT-auditors. Je kunt versie 1.2 van dit model downloaden op de website van NOREA. Dit document van NOREA wordt in Nederland veel toegepast, en is een uitgebreid en begrijpelijk instrument om vorm te geven aan de PIA. Zo bevat het document een vragenlijst dat je helpt om stapsgewijs privacy-risico's in kaart te brengen.

VRAAG 5 - Op welk moment start je de PIA?
Het is van groot belang om privacyaspecten zo vroeg mogelijk te betrekken bij nieuwe initiatieven waarbij (mogelijk) persoonsgegevens worden verwerkt. Privacy-regels hebben bijna altijd een effect op hoe je een proces organiseert (denk bijvoorbeeld aan wie op welk moment voor welk doel over welke informatie mag beschikken). Dat zijn dus zaken die je al in de ontwerpfase aan de orde moet stellen. Kom je er dus pas net voor de lancering van een evenement, website, product of dienst achter dat er allerlei privacy-vraagtekens aan het initiatief kleven, dan ben je in feite te laat.

Let op!
Er bestaat soms een neiging om projecten (eenmaal in hun finale stadium) ongewijzigd door te drukken, bijvoorbeeld met het excuus dat er gezien de beschikbare hoeveelheid geld/tijd geen ruimte meer is voor een PIA. Wees uiterst waakzaam voor dit soort signalen: de kans is groot dat juist in dit scenario onaanvaardbare risico's worden genomen.

Bijlage: model bewerkersovereenkomst

Toelichting op het model
Deze modelovereenkomst biedt een uitgangspunt voor de verantwoordelijke die een bewerkersovereenkomst moet sluiten met een bewerker. Instructies voor de gebruiker van het model zijn in **blauw** opgenomen.

Let op: het betreft slechts een model. Afhankelijk van de aard van de relatie met de bewerker dienen afwijkende of aanvullende afspraken te worden gemaakt om te voldoen aan de wettelijke verplichtingen van de verantwoordelijke.

Dit model bevat verwijzingen naar drie bijlagen. De gebruiker moet zorgen dat deze onderdeel vormen van de bewerkersovereenkomst. De bijlagen dienen tezamen met de bewerkersovereenkomst door beide partijen te worden ondertekend.
Het gebruik van dit model is geheel voor eigen risico van de gebruiker.

© CMS Derks Star Busmann N.V., 2017

BEWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. [naam]., gevestigd te [adres], [postcode] [plaats], te dezen rechtsgeldig vertegenwoordigd door [naam persoon], [functie]; hierna: "Opdrachtgever", en
2. [naam], gevestigd te [adres], [postcode] [plaats], te dezen rechtsgeldig vertegenwoordigd door [naam persoon], [functie]; hierna: "Bewerker";

hierna gezamenlijk te noemen: Partijen,

OVERWEGENDE DAT:

a) Partijen op [DATUM] een overeenkomst [SPECIFICEER REIKWIJDTE EN WERKZAAMHEDEN] zijn aangegaan ("Overeenkomst") in het kader waarvan persoonsgegevens door Bewerker (kunnen) worden verwerkt;
b) te dien aanzien Opdrachtgever als "verantwoordelijke", en Bewerker als "bewerker" moet worden aangemerkt in de zin van Artikel 1 Wet bescherming persoonsgegevens ("Wbp");
c) Partijen in deze overeenkomst ("Bewerkersovereenkomst") de gemaakte afspraken neerleggen die gelden voor het verwerken van Persoonsgegevens (zoals nader omschreven in Artikel 1) door Bewerker ten behoeve van Opdrachtgever;

KOMEN ALS VOLGT OVEREEN:

1. REIKWIJDTE VAN DEZE OVEREENKOMST

1.1 Bewerker zal de categorieën persoonsgegevens die omschreven zijn in Bijlage 1 ("Persoonsgegevens") uitsluitend [geautomatiseerd / langs niet-geautomatiseerde weg] verwerken ten behoeve en in opdracht van Opdrachtgever in overeenstemming met de bepalingen van deze Bewerkersovereenkomst, in het bijzonder de verwerkingsdoeleinden die eveneens zijn omschreven in Bijlage 1.

1.2 Bewerker heeft geen zelfstandige zeggenschap over de doeleinden van verwerking van de Persoonsgegevens en de daartoe gebruikte middelen.

2. ALGEMENE VERPLICHTINGEN BEWERKER

2.1 Bewerker verplicht zich om alle instructies van Opdrachtgever op te volgen ten aanzien van de verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst.

2.2 Bewerker zal zich houden aan alle toepasselijke wet- en regelgeving en gedragscodes betreffende de bescherming en beveiliging van persoonsgegevens. Bewerker verklaart met deze regelgeving bekend te zijn.

2.3 Het is Bewerker niet toegestaan om de Persoonsgegevens voor eigen doeleinden of enig ander doel dan de in deze Bewerkersovereenkomst genoemde doelen te verwerken en/of aan derden te verstrekken.

2.4 Bewerker zal op eerste verzoek van Opdrachtgever toegang verlenen aan Opdrachtgever tot de Persoonsgegevens, dan wel de Persoonsgegevens aan Opdrachtgever ter beschikking stellen op een wijze die Opdrachtgever wenselijk acht.

3. SUB-BEWERKERS EN DOORGIFTE

3.1 Bewerker mag voor de verwerking van Persoonsgegevens binnen het kader van de Bewerkersovereenkomst uitsluitend derden inschakelen indien die zijn goedgekeurd door Opdrachtgever en opgenomen in Bijlage 2 ("Sub-bewerker(s)").

3.2 Indien (een deel van) de verwerking van de Persoonsgegevens wordt uitbesteed aan een Sub-bewerker, is Bewerker jegens Opdrachtgever volledig aansprakelijk voor de uitvoering door Sub-bewerker conform de plichten die uit hoofde van deze Bewerkersovereenkomst op Bewerker rusten. Bewerker staat er jegens Opdrachtgever voor in dat de verwerking van de Persoonsgegevens door een Sub-bewerker slechts plaatsvindt binnen de reikwijdte van deze Overeenkomst.

3.3 Bewerker en eventuele Sub-bewerkers mogen Persoonsgegevens uitsluitend (laten) verwerken binnen de Europees Economische Ruimte.

3.4 Bewerker zorgt ervoor dat aan Sub-bewerkers, voor zover het door hen uitgevoerde verwerking(en) van Persoonsgegevens betreft, middels een schriftelijke bewerkersovereenkomst ("Sub-bewerkersovereenkomst") dezelfde verantwoordelijkheden en verplichtingen worden opgelegd als de bepalingen uit deze overeenkomst. Op eerste verzoek van Opdrachtgever verstrekt Bewerker aan Opdrachtgever een kopie van deze Sub-bewerkersovereenkomst(en).

4. GEHEIMHOUDING

4.1 Bewerker mag geen Persoonsgegevens aan derden kenbaar maken of derden daartoe toegang geven, tenzij Opdrachtgever daar vooraf uitdrukkelijk schriftelijk toestemming voor heeft gegeven. Onder derden wordt ook personeel van Bewerker begrepen voor zover het niet noodzakelijk is dat dergelijk personeel voor het uitvoeren van de Overeenkomst kennisneemt van de Persoonsgegevens. Deze geheimhoudingsplicht blijft onverminderd van kracht na het einde van deze Bewerkersovereenkomst.

4.2 Bewerker verplicht zich om medewerkers die werkzaamheden verrichten in het kader van de uitvoering van de Overeenkomst, dezelfde verplichtingen op te leggen ten aanzien van het geheimhouden en vertrouwelijk behandelen van Persoonsgegevens als bedoeld in dit artikel.

5. BEVEILIGING

5.1 Bewerker zal uit eigen beweging zodanige technische en organisatorische beveiligingsmaatregelen treffen dat de Persoonsgegevens adequaat beveiligd zijn tegen verlies of enige vorm van onzorgvuldige, ondeskundige of onrechtmatige verwerking en dat ten aanzien van de Persoonsgegevens steeds sprake is van een adequate bescherming die, gelet op de stand van de techniek, passend is. Daarnaast treft Bewerker in ieder geval de in Bijlage 3 opgenomen beveiligingsmaatregelen.

5.2 Bewerker zorgt ervoor dat het bij de verwerking van Persoonsgegevens betrokken medewerkers de in deze overeenkomst opgenomen verplichtingen van Bewerker kennen en dit deze zich aan die verplichtingen houden.

5.3 Partijen evalueren periodiek de in Artikel 5.1 genoemde maatregelen. Zodra Opdrachtgever ten aanzien van de beveiliging van de Persoonsgegevens nieuwe of gewijzigde afspraken

© CMS Derks Star Busmann N.V., 2017

wenselijk acht, dan zal Bewerker de beveiligingsnormen aanpassen overeenkomstig de wensen van Opdrachtgever.

6. CONTROLE

6.1 Bewerker stelt Opdrachtgever in staat om op verzoek van Opdrachtgever, onder aanzegging van een redelijke termijn, de naleving door Bewerker van deze Bewerkersovereenkomst door Opdrachtgever te laten controleren. Daartoe zal Bewerker aan een onafhankelijke auditor, ingehuurd door Opdrachtgever, toegang verschaffen tot (relevante delen van) de ruimtes, systemen en/of servers waarin/waarmee de verwerking van de Persoonsgegevens op enig moment plaatsvindt. Bewerker zal aan de auditor alle informatie verstrekken die redelijkerwijs nodig is voor het uitvoeren van de controle.

6.2 Bewerker verstrekt op eerste verzoek van Opdrachtgever een rapportage aan Opdrachtgever waarin Bewerker informatie verstrekt over de stand van de beveiligingsmaatregelen zoals omschreven in artikel 5en Bijlage 3, beveiligingsincidenten en mogelijke beveiligingsrisico's ten aanzien van de Persoonsgegevens.

7. INFORMEERPLICHT BEWERKER

7.1 Zodra Bewerker kennisneemt van een incident of dreigend incident inzake diefstal, verlies of ontoegankelijkheid van gegevens of enige inbreuk of dreigende inbreuk op de beveiliging in de zin van art. 34a Wbp (hierna: "Beveiligingsincident"), stelt Bewerker Opdrachtgever hiervan onverwijld, doch uiterlijk op de eerstvolgende werkdag, op de hoogte en zal Bewerker daarbij in ieder geval informatie verstrekken over:

(i) de aard van het Beveiligingsincident en de feitelijke toedracht voor zover bekend of vermoed;

(ii) de (mogelijk) getroffen Persoonsgegevens;

(iii) de vastgestelde en verwachte gevolgen van het Beveiligingsincident voor de verwerking van de Persoonsgegevens en de daarbij betrokken personen; en

(iv) de maatregelen die Bewerker heeft getroffen en zal treffen om de negatieve gevolgen van het Beveiligingsincident te verhelpen of beperken.

7.2 Bewerker verleent op verzoek van Opdrachtgever de gevraagde medewerking die Opdrachtgever nodig acht om een inbreuk op de beveiliging te melden bij de Autoriteit Persoonsgegevens en/of de betrokkenen. Bewerker mag een dergelijke melding niet doen zonder uitdrukkelijke voorafgaande toestemming van Opdrachtgever.

7.3 Bewerker zal Opdrachtgever van eventuele nieuwe ontwikkelingen inzake een Beveiligingsincident in de zin van artikel 7.1 steeds op de hoogte stellen en informeren over de in art. 7.1 genoemde aspecten alsmede getroffen maatregelen om in de toekomst herhaling te voorkomen.

7.4 Eventuele kosten die gepaard gaan met de uitvoering van verplichtingen voor Bewerker zoals genoemd in artikel 7.1, 7.2 en 7.3 komen voor rekening van Bewerker.

7.5 Bewerker zal Opdrachtgever onverwijld informeren over enig verzoek of onderzoek van enige overheids- of vergelijkbare instantie met betrekking tot de verstrekking of verwerking van de Persoonsgegevens.

8. AANSPRAKELIJKHEID EN VRIJWARING

8.1 Onverminderd het bepaalde in art. 3.1, is Bewerker aansprakelijk voor alle schade die voor Opdrachtgever voortvloeit uit een aan Bewerker en/of Sub-bewerker toerekenbare schending van de wet- en regelgeving betreffende de verwerking van Persoonsgegevens of niet-nakoming van verplichtingen ingevolge deze Bewerkersovereenkomst.

8.2 Bewerker zal Opdrachtgever vrijwaren van enigerlei boete of schade die door Opdrachtgever verschuldigd c.q. geleden wordt als gevolg van toerekenbare niet-nakoming door Bewerker van deze Bewerkersovereenkomst.

9. OMGANG MET RECHTEN VAN BETROKKENEN

9.1 Bewerker zal desverzocht aan Opdrachtgever alle benodigde medewerking verlenen om uitvoering te geven aan inzageverzoeken van betrokkenen of het verzoek om verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Indien dergelijke verzoeken binnenkomen bij Bewerker leidt hij deze door naar Opdrachtgever en geeft hij daaraan niet zelfstandig uitvoering.

10. OMGANG MET PERSOONSGEGEVENS BIJ BEËINDIGING

10.1 Bij het eindigen van de Overeenkomst op welke grond en op welke wijze dan ook – moet Bewerker kosteloos op eerste verzoek van Opdrachtgever:

(i) aan Opdrachtgever alle Persoonsgegevens ter beschikking stellen op de wijze en in het format zoals door Opdrachtgever gewenst;

(ii) onmiddellijk de verwerking van Persoonsgegevens staken en zorgen dat eventuele Sub-bewerkers hetzelfde doen;

(iii) alle documenten waarin Persoonsgegevens zijn vastgelegd aan Opdrachtgever ter beschikking stellen, en

(iv) nadat Opdrachtgever daartoe uitdrukkelijk opdracht heeft gegeven, alle Persoonsgegevens die elektronisch zijn opgeslagen permanent verwijderen of, voor zover permanente verwijdering van de gegevensdrager niet mogelijk is, de gegevensdrager vernietigen, en desgevraagd schriftelijk aan Opdrachtgever bevestigen dat aan alle verplichtingen uit hoofde van dit artikel 10.1 is voldaan.

11. INWERKINGTREDING EN DUUR VAN DE OVEREENKOMST

11.1 Deze Bewerkersovereenkomst treedt in werking op de datum dat Partijen de Bewerkersovereenkomst hebben ondertekend.

11.2 Deze Bewerkersovereenkomst geldt voor de duur dat Bewerker Persoonsgegevens verwerkt in het kader van de uitvoering van de Overeenkomst.

11.3 Bewerker kan deze Bewerkersovereenkomst niet tussentijds opzeggen.

11.4 De bepalingen in deze Bewerkersovereenkomst blijven ook na het einde van de Overeenkomst onverminderd van kracht zolang Bewerker Persoonsgegevens onder zich heeft.

© CMS Derks Star Busmann N.V., 2017

12. TOEPASSELIJK RECHT EN BEVOEGDE RECHTER

12.1 Deze Bewerkersovereenkomst en de uitvoering ervan worden uitsluitend beheerst door Nederlands recht.

12.2 Alle geschillen in verband met deze Bewerkersovereenkomst of de uitvoering ervan worden uitsluitend voorgelegd aan de bevoegde rechter te Amsterdam.

Aldus overeengekomen en ondertekend te [plaats] op [datum].

[VERANTWOORDELIJKE]	[BEWERKER]
_____	_____
naam: [naam vertegenwoordiger]	naam: [naam vertegenwoordiger]
functie: [functie vertegenwoordiger]	functie: [functie vertegenwoordiger]

BIJLAGE 1 BIJ MODEL BEWERKERSOVEREENKOMST: PERSOONSGEGEVENS EN DOELEINDEN

1. PERSOONSGEGEVENS

Bewerker zal de volgende (categorieën) Persoonsgegevens verwerken:

(1) [Benoem hier de soort te verwerken persoonsgegevens]
(2) […]
(3) […]

2. VERWERKINGSDOELEINDEN

De doeleinden waarvoor bovengenoemde Persoonsgegevens worden verwerkt zijn:

(1) [Benoem hier de doeleinden waarvoor de verwerking plaatsvindt]
(2) […]
(3) […]

Aldus overeengekomen en ondertekend te [plaats] op [datum].

[VERANTWOORDELIJKE]	[BEWERKER]
_____	_____
naam: [naam vertegenwoordiger]	naam: [naam vertegenwoordiger]
functie: [functie vertegenwoordiger]	functie: [functie vertegenwoordiger]

© CMS Derks Star Busmann N.V., 2017

BIJLAGE 2 BIJ MODEL BEWERKERSOVEREENKOMST: SUB-BEWERKERS

1. VERLENING TOESTEMMING INSCHAKELING SUB-BEWERKERS

Opdrachtgever verleent hierbij toestemming aan Bewerker om de besloten vennootschap [naam] gevestigd te [adres], [postcode en plaats], in te schakelen als Sub-bewerker ten behoeve van:

(a) [naam sub-bewerker]
(b) […]
(c) […]

Aldus overeengekomen en ondertekend te [plaats] op [datum].

[VERANTWOORDELIJKE]	[BEWERKER]
_____	_____
naam: [naam vertegenwoordiger]	naam: [naam vertegenwoordiger]
functie: [functie vertegenwoordiger]	functie: [functie vertegenwoordiger]

BIJLAGE 3 BIJ MODEL BEWERKERSOVEREEKOMST: TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

1. OVERZICHT VAN TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

[Neem in deze bijlage een lijst op met de technische en organisatorische beveiligingsmaatregelen die de bewerker zal treffen.]

Aldus overeengekomen en ondertekend te [plaats] op [datum].

[VERANTWOORDELIJKE]	[BEWERKER]
_____	_____
naam: [naam vertegenwoordiger]	naam: [naam vertegenwoordiger]
functie: [functie vertegenwoordiger]	functie: [functie vertegenwoordiger]

© CMS Derks Star Busmann N.V., 2017

Bijlage: model privacyverklaring

Toelichting op het model
Deze modelverklaring biedt een uitgangspunt voor de verantwoordelijke die de betrokkene moet informeren over een verwerking van persoonsgegevens. Instructies voor de gebruiker van het model zijn in **blauw** opgenomen.

Zorg altijd dat de verklaring eenvoudig kan worden geraadpleegd door de betrokkene.

Let op: het betreft slechts een model. Afhankelijk van de aard van de verwerking dient een verantwoordelijke méér (soorten) informatie aan de betrokkene te verstrekken om te voldoen aan de wettelijke informeerplicht. Het gebruik van dit model is geheel voor eigen risico van de gebruiker.

PRIVACYVERKLARING

Dit is een privacyverklaring van [Officiële naam van de organisatie], gevestigd te plaats en ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer [nummer] (hierna: ["naam organisatie"]). Deze privacyverklaring omschrijft welke persoonsgegevens [naam organisatie] verwerkt en voor welke doeleinden deze persoonsgegevens worden gebruikt.

1. GEBRUIK VAN PERSOONSGEGEVENS

1.1 [Naam organisatie] verwerkt (mogelijk) de volgende persoonsgegevens van u indien u:
(a) [vul in]
(b) […]
(c) […]
Neem in 1.1 op wat de relevante aanleiding is voor de verwerkingen die je in deze privacyverklaring toelicht. Enkele suggesties:
- de website [webadres] bezoekt;
- een werknemer van [naam organisatie] bent;
- zich inschrijft voor [specificeer evenement/opleiding];
- een aankoop doet of dienst afneemt bij [naam organisatie];
- lid wordt van [vul in];
- zich aanmeldt voor nieuwsbrieven van [naam organisatie];
- via het contactformulier contact met ons opneemt;

1.2 [naam organisatie] verzamelt de volgende (persoons)gegevens:
(a) [vul in]
(b) […]
(c) […]
Neem in 1.2 puntsgewijs alle relevante categorieën op van verwerkte persoonsgegevens. Enkele suggesties: naam, adres, e-mailadres, telefoonnummer, leeftijd, geslacht, werkgever, functie, bankrekeningnummer, gegevens over aankopen, gegevens over voorkeuren, gegevens over afspraken), etc.

1.3 [naam organisatie] kan deze gegevens gebruiken om:
(a) [vul in]
(b) […]
(c) […]
Neem in 1.3 alle doeleinden op waarvoor je de in 1.2 genoemde persoonsgegevens verwerkt. Enkele suggesties:
- aankopen te doen;
- de aankoop uit te voeren, de dienst te leveren;
- het lidmaatschap te effectueren;
- nieuwsbrieven te verzenden;
- contact met u op te nemen of te onderhouden;
- de dienstverlening van [Naam] te verbeteren;
- de website te optimaliseren;

2. INFORMATIE, WIJZIGING EN BEZWAAR

2.1 U kunt contact opnemen met [Naam contactpersoon] via [telefoonnummer en/of e-mailadres] voor:
(a) meer informatie over de wijze waarop [naam organisatie] persoonsgegevens verwerkt;
(b) vragen naar aanleiding van deze privacyverklaring;
(c) inzage in de persoonsgegevens die [naam organisatie] wij met betrekking tot u verwerken;
(d) bezwaar tegen het gebruik van uw gegevens door [naam organisatie].

3. BEVEILIGING VAN UW GEGEVENS

3.1 [Naam organisatie] zal uw gegevens uitsluitend gebruiken voor de in deze privacyverklaring genoemde doeleinden en ze niet langer bewaren dan noodzakelijk.

3.2 [Naam organisatie] zal adequate technische en organisatorische maatregelen treffen om uw gegevens te beveiligen.

4. DERDEN

4.1 [Naam organisatie] zal u gegevens niet aan derden verstrekken, tenzij u / je daarvoor uw / je uitdrukkelijke toestemming heeft gegeven of [Naam] daartoe verplicht is / wij daartoe verplicht zijn op grond van de wet of een rechterlijke uitspraak.
Neem bepaling 4.1 slechts op indien geen persoonsgegevens aan derden worden verstrekt.

4.2 [Naam organisatie] verstrekt uw gegevens aan de volgende derden:
(a) [vul in]
(b) […]
(c) […]
Omschrijf in bepaling 4.2 aan welke derden persoonsgegevens kunnen worden verstrekt. Enkele suggesties: leveranciers, gelieerde organisaties.

© CMS Derks Star Busmann N.V., 2017

Deze derden gebruiken de gegevens voor: [omschrijf de doeleinden van de verkrijging door deze derden indien van toepassing]

5. MELDING AUTORITEIT PERSOONSGEGEVENS

5.1 Onze verwerking van persoonsgegevens is gemeld aan het Autoriteit Persoonsgegevens onder meldingsnummer / meldingsnummers [nummer / nummers].

Gebruik deze bepaling slechts als de verwerking is aangemeld bij de Autoriteit Persoonsgegevens.

6. WIJZIGINGEN PRIVACYVERKLARING

6.1 Het kan voorkomen dat deze verklaring in de toekomst wordt gewijzigd. Wij bevelen daarom aan om deze privacy policy regelmatig te blijven raadplegen.

Bijlage: model kernprotocol datalekken

Toelichting op het model

Dit model biedt een handvat om vast te stellen hoe de organisatie intern omgaat met eventuele datalekken. Instructies voor de gebruiker van het model zijn in blauw opgenomen.
Zorg dat het beleid eenvoudig kan worden geraadpleegd door alle personen die actief zijn binnen de organisatie.
Let op: dit protocol is slechts een model. Afhankelijk van de (inrichting van) de organisatie dienen mogelijk afwijkende of aanvullende acties in het protocol te worden opgenomen.
Het gebruik van dit model is geheel voor eigen risico van de gebruiker.

Kernprotocol datalekken [naam organisatie]

FASE 1: de constatering van een (mogelijk) beveiligingsincident

1. Zodra iemand vermoedt dat mogelijk sprake is van een beveiligingsincident, dan meldt deze persoon dit **onmiddelijk** telefonisch (of, indien dit niet mogelijk is, per e-mail) aan:
[contactpersoon incidenten]
[telefoonnummer]
[e-mailadres]
Een beveiligingsincident is een situatie waarin binnen [naam organisatie] bewaarde of gebruikte gegevens mogelijk of daadwerkelijk zijn verloren of toegankelijk zijn (geweest) voor onbevoegden. Een incident is dus niet alleen een inbreuk van buitenaf, maar bijvoorbeeld ook het verlies van een laptop, USB key of telefoon. Neem ook bij twijfelgevallen contact op met [contactpersoon incidenten]

2. Verstrek geen informatie aan derden omtrent het (mogelijke) incident!

FASE 2: onderzoek van het (mogelijke) beveiligingsincident

1. [De contactpersoon incidenten] onderzoekt zo spoedig mogelijk en zonder enig uitstel of het incident (mede) betrekking heeft/kan hebben op ***persoonsgegevens***.
Raadpleeg bij twijfel onmiddellijk een deskundige!

2. Kan het incident betrekking hebben op persoonsgegevens, dan stelt [de contactpersoon incidenten] (zowel binnen als buiten werktijd) [de contactpersoon bestuur] **onmiddellijk** telefonisch **en** per e-mail op de hoogte via:
[contactpersoon bestuur]
[telefoonnummer]
[e-mailadres]

3. [De contactpersoon incidenten] zorgt dat zoveel mogelijk informatie en activiteiten met betrekking tot het (vermoedelijke) beveiligingsincident worden geregistreerd. Deze informatie moet direct beschikbaar blijven voor raadpleging zolang als nodig is voor de behandeling van het beveiligingsincident.

© CMS Derks Star Busmann N.V., 2017

4. [De contactpersoon incidenten] zorgt dat, afhankelijk van de aard van het (vermoede) beveiligingsincident en de daarover beschikbare informatie, zonder vertraging passende maatregelen tot herstel van het beveiligingslek en/of tot voorkoming van herhaling.

FASE 3: Onderzoek meldplicht aan Autoriteit Persoonsgegevens en betrokkenen

1. Zodra [de contactpersoon bestuur] kennisneemt van het beveiligingsincident waarbij persoonsgegevens betrokken (kunnen) zijn, bepaalt het bestuur (al dan niet bijgestaan door een deskundige) of [naam organisatie] ten aanzien van de verwerking van die persoonsgegevens juridisch gezien ***verantwoordelijke*** is. **Raadpleeg bij twijfel onmiddellijk een deskundige!**

2. Indien en voor zover [naam organisatie] verantwoordelijke is, bepaalt het bestuur zonder vertraging of als gevolg van het beveiligingsincident:

a) een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens;

b) waarschijnlijk ongunstige gevolgen te verwachten zijn voor de persoonlijke levenssfeer van personen op wie de persoonsgegevens betrekking hebben;
Raadpleeg bij twijfel onmiddellijk een deskundige!

3. Indien sprake is van een situatie zoals beschreven in a) en/of b) doet het bestuur onverwijld, maar **uiterlijk binnen 72 uur** na constatering van het incident, de wettelijk voorgeschreven melding bij de Autoriteit Persoonsgegevens en/of betrokkenen.

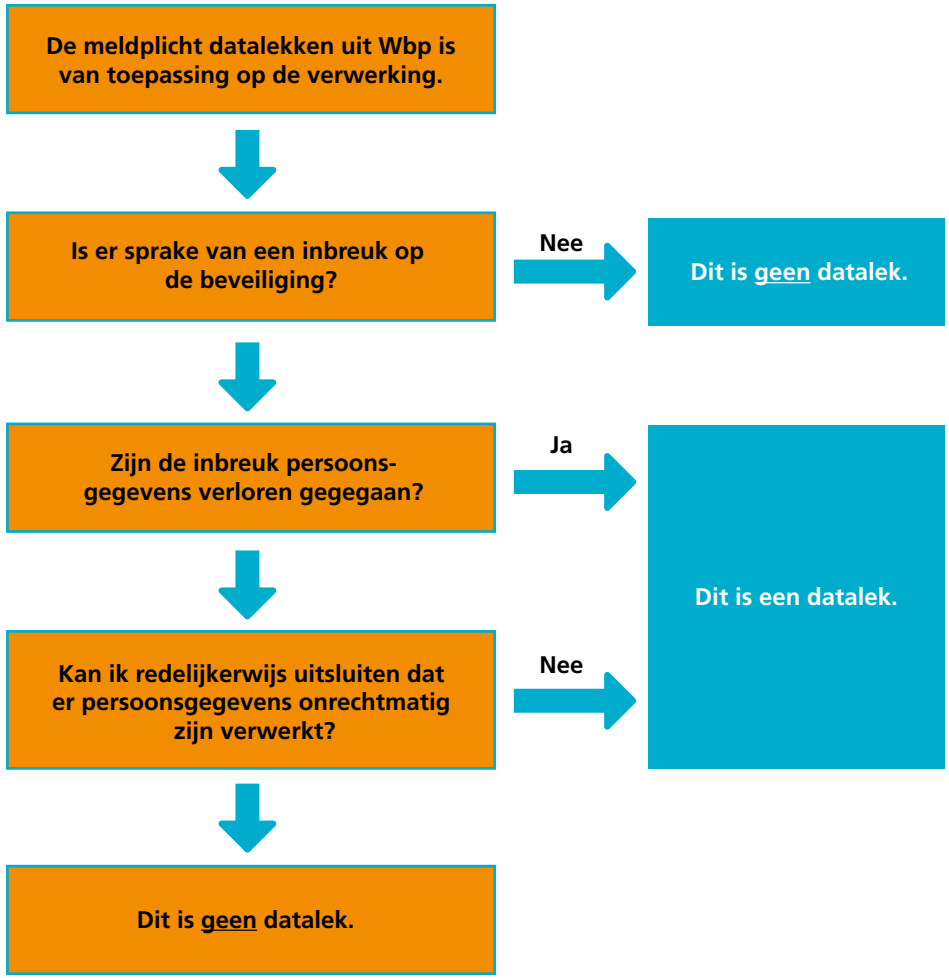
4. Het bestuur stelt een communicatieplan op voor eventuele vragen van betrokkenen, de media en overige derden. Er wordt een woordvoerder aangewezen voor externe communicatie. Lijkt het incident te leiden tot media-aandacht, bereid dan ook een persverklaring voor.

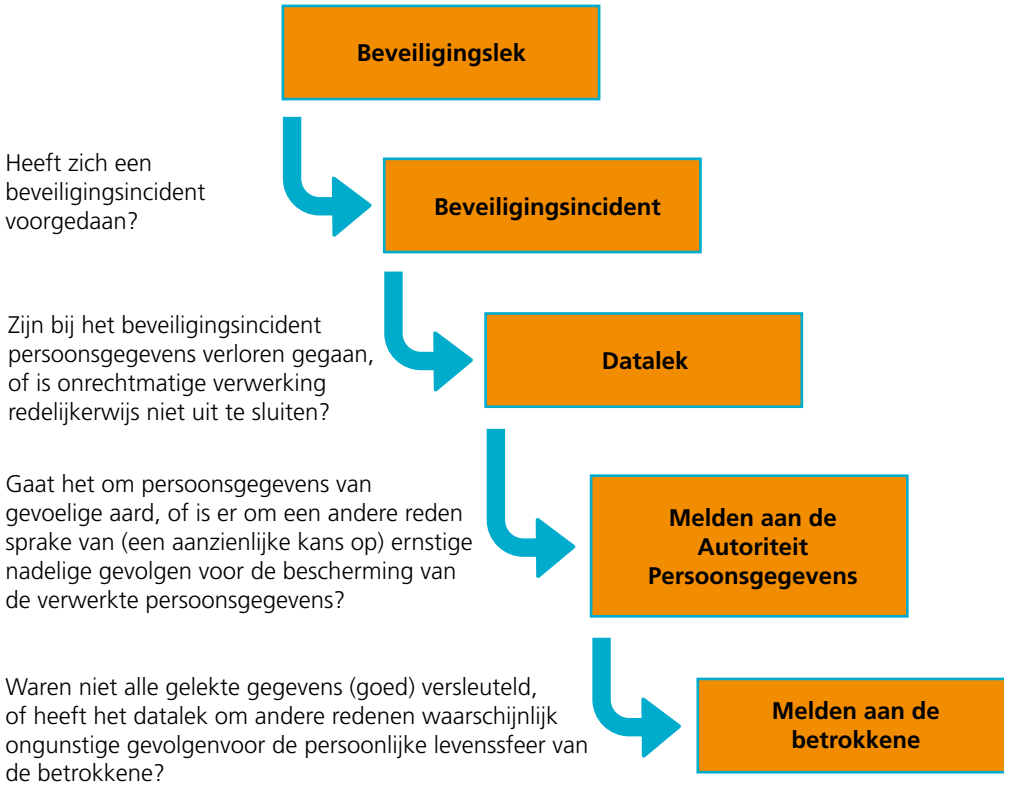
[De contactpersoon bestuur] en [contactpersoon incidenten] evalueren na afronding van het incident gezamenlijk de wijze waarop [naam organisatie] het incident is afgehandeld en stellen van deze evaluatie een schriftelijk verslag op. Waar nodig worden nieuwe maatregelen geïmplementeerd en wordt dit protocol aangepast.

© CMS Derks Star Busmann N.V., 2017

Bijlage: stroomschema's beleidsregels datalekken AP

Deze stroomschema's zijn afkomstig uit de beleidsregels datalekken van de Autoriteit Persoonsgegevens (editie december 2015).





© CMS Derks Star Busmann N.V., 2017

Trefwoordenlijst

Aanmelding
Aansprakelijkheid
Beeldmateriaal
Betrokkene
Beveiliging
Bewaartermijn
Bewerker
Bewerkersovereenkomst
Bijzondere persoonsgegevens
Boete
Bring Your Own Device
Burger Service Nummer
Cookies
Datalek
Delen (van persoonsgegevens)
Direct marketing
Doelbinding
Doorgifte
Functionaris gegevensbescherming
Gelaagde structuur
Gerechtvaardigd belang
Gezondheidsgegevens
Grondslag
Informatieplicht
Klokkenluiders
Ledenadministratie
Marketing
Management
Meldplicht datalekken
Minderjarigen
Monitoring
Opleiding
Personeel
Personeelsadministratie
Persoonsgegevens
PIA
Portretrecht
Social media
Sollicitanten
Toestemming
Verantwoordelijke
Verordening
Vrijwilligers
Verwerking
Wearables
Webwinkel
Wedstrijdadministratie
Werknemers
Wet bescherming persoonsgegevens
Winacties

© CMS Derks Star Busmann N.V., 2017

C/M/S/ Law-Now™
Law . Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

C/M/S/ e-guides
Law . Tax

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Medellín, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

www.cmslegal.com

© CMS Derks Star Busmann N.V. (February 2017)