*W. SEINEN**

Sport 2.0 en het privacyrecht

Social media zijn in een korte tijd diep doorgedrongen in de sport. Trainingsschema's en wedstrijdroosters worden elektronisch verspreid, prestaties van sporters worden door apps verzameld, verwerkt 'in the cloud', en in de vorm van analyses en grafiekjes via het internet ter beschikking gesteld aan de sporter en al zijn 'vrienden'. Als gevolg van deze ontwikkelingen worden tegenwoordig op massale schaal persoonsgegevens verwerkt. Dit artikel gaat in op de privacyrechtelijke aspecten van een aantal onlinediensten die in de sport veel worden gebruikt. Het perspectief van de sportvereniging is hierbij als uitgangspunt genomen.

In de wereld van de sport is het gebruik van internet en social media al lang niet meer voorbehouden aan topsporters met eigen communicatieadviseurs of aan computerfreaks die toevallig ook sporten. Het gebruik van internet is in de sport niet meer weg te denken. Wedstrijdschema's, uitslagen en nieuwtjes staan steeds vaker op de website van de club. Ook trainingsprogramma's en individuele prestatiegegevens worden vaak ontsloten via het internet. En het blijft allang niet meer beperkt tot 'gewoon' internet. De sporter heeft zijn weg naar social media allang gevonden. Twitter, Facebook en Hyves worden op grote schaal ingezet. Eigenlijk is dat ook niet verassend, want Nederland is een voorhoedespeler op de digitale snelweg. 1,3 miljoen Nederlanders 'twitteren', 3,5 miljoen gebruiken LinkedIn, en Facebook en Hyves hebben 7,3 respectievelijk 9,8 miljoen abonnees.[1] Last but not least, meer dan 15 miljoen Nederlanders hebben toegang tot het internet.[2]

Misschien is het zelfs wel omgekeerd, en hebben de social media de sport als doelgroep ontdekt: er zijn verschillende platforms die zich specifiek op de sport hebben toegelegd[3] en het aantal apps dat is geschreven voor de sporter is indrukwekkend. Dergelijke sport-apps gebruiken veelal de locatiegegevens van een smartphone en/of andere apparaatjes om zodoende snelheid, afstand, duur, versnelling, enz. bij te houden. Ook de hartslag van de gebruiker, zijn gewicht, leeftijd, enz. worden in deze context vaak gebruikt om nog meer op maat gesneden informatie te kunnen presenteren.

Die uitdijende stroom aan informatie die wordt gebruikt, heeft bijna altijd betrekking op natuurlijke personen: mensen van vlees en bloed. Vaak zijn dat de sporters zelf, maar ook toeschouwers en toevallige voorbijgangers kunnen de revue passeren in onlinewedstrijdverslagen, YouTube-filmpjes, tweets, krabbels en blogs. En daar komt het privacyrecht om de hoek kijken. De Nederlandse privacywet (de Wet bescherming persoonsgegevens (Wbp)) is van toepassing op de geautomatiseerde verwerking van persoonsgegevens. Een 'persoonsgegeven' in de zin van de wet is alle informatie die betrekking heeft op een 'geïdentificeerde of identificeerbare natuurlijk persoon'.[4]

De Wbp hanteert als uitgangspunt dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.[5] Het College bescherming persoonsgegevens (CBP) heeft deze regel diverse malen toegepast en zo onder meer geoordeeld dat telefoonnummers, combinaties van postcode en huisnummer, maar ook kentekens en IP-

* Mr. W. Seinen is advocaat bij CMS Derks Star Busmann te Utrecht en gespecialiseerd in het internet- en privacyrecht. De auteur dankt Silvia van Schaik en Elly Besterveld voor hun kritische beschouwing en aanvullingen.

1. Zie www.marketingfacts.nl/statistieken/social-media-marketing/.
2. In 2011 had 94% van de Nederlandse huishoudens een internetaansluiting, zie het rapport 'ICT, kennis en economie 2012' van het Centraal Bureau voor de Statistiek d.d. 15 juni 2012 (www.cbs.nl).
3. In Nederland is Teamers (zie www.teamers.nl) een van de bekendste social-mediaplatforms. Op een meer experimenteel niveau is The Soccer Project (zie www.thesoccerproject.nl) bezig om een soort digitaal alternatief van de traditionele voetbalclub op te richten. Iedereen die wil kan via het platform wedstrijden organiseren of daaraan deelnemen.
4. Zie artikel 1 onder a Wbp.
5. *Kamerstukken II* 1997/98, 25 892 nr. 3, p. 47 (MvT Wbp).

adressen in de regel als persoonsgegeven worden aangemerkt.[6] De lat van identificeerbaarheid is dus niet erg hoog gelegd. Ook minder directe verwijzingen, zoals 'de keeper van Heren 1' of 'de scheidsrechter' vallen onder de reikwijdte van de Wbp, want het zal in de regel niet moeilijk zijn om met enkele muisklikken te achterhalen om wie het precies gaat.
Dat betekent dat achter vrijwel iedere 'posting' op een social-mediaplatform een verwerking van persoonsgegevens schuilgaat.

Huishoudelijk gebruik?

De Wbp is dus in beginsel van toepassing op de online-activiteiten rondom de sport. Die hoofdregel lijdt uitzondering indien de verwerking wordt geacht plaats te vinden voor 'uitsluitend persoonlijke of huishoudelijke doeleinden' (artikel 2 lid 2 onder a Wbp). Van persoonlijk of huishoudelijk gebruik in de zin van de wet is echter geen sprake wanneer de verwerking van persoonsgegevens bestaat in openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt.[7] Dat betekent dat de persoonlijke openbare websites en social-mediadiensten niet kunnen profiteren van deze uitzondering.

Daarnaast zullen ook de meeste 'gesloten' Facebook-, LinkedIn- en Hyves-pagina's van en voor sportverenigingen buiten het bereik van de genoemde uitzonderingsbepaling blijven. Immers 'huishoudelijk gebruik' ziet op de verwerking van persoonsgegevens in een (gezins)huishouding.[8] Indien de verzamelde persoonsgegevens bestemd zijn voor gebruik door meerdere personen die niet binnen eenzelfde huishouding vallen, is geen sprake meer van 'huishoudelijk gebruik'.

Gevolgen van toepasselijkheid Wbp

Laten wij er daarom van uitgaan dat de Wbp van toepassing is op de meeste Sport 2.0-initiatieven. De Wbp richt zich primair tot de degene die het doel bepaalt en de middelen stelt voor de verwerking van persoonsgegevens, in de wet aangeduid als de 'verantwoordelijke'. Daarnaast bevat de Wbp enkele bepalingen over partijen die in opdracht van een verantwoordelijke persoonsgegevens verwerken. Deze worden aangeduid als 'bewerker'. Zo is een sportvereniging bijvoorbeeld de 'verantwoordelijke' ten aanzien van het adressenbestand van de leden. De drukker die het clubblad maakt en verzendt (en voor dat doel de adressenlijst gebruikt) is de 'bewerker'.
De verantwoordelijke mag alleen maar persoonsgegevens verzamelen op grond van een van de in de wet genoemde doeleinden.[9] Die gegevens mogen vervolgens alleen maar gebruikt worden voor zover dat verenigbaar is met dat verzameldoel.[10]
Dat verzameldoel moet tevens kunnen worden aangemerkt als wettelijke rechtvaardigingsgrond voor de betrokken verwerking. De wet kent zes rechtvaardigingsgronden,[11] waarvan vooral de volgende drie relevant zijn in de context van internet en social media.
Toestemming: de betrokkene heeft voor de verwerking van diens gegevens zijn ondubbelzinnige toestemming verleend.[12]
Uitvoering overeenkomst: de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene of daarmee verband houdende voorbereidingshandelingen.[13]
Gerechtvaardigd belang: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke, terwijl zich geen zwaarder wegende belangen tegen de verwerking verzetten.[14]

De personen die worden genoemd of afgebeeld in een gemiddelde social-media-uiting, hebben niet altijd een contractuele verhouding met de afzender van het bericht, laat staan dat het posten van zijn gegevens met het oog op die rechtsband 'noodzakelijk' is. Wanneer geen expliciete toestemming is gegeven, kan vaak met succes een beroep worden gedaan op de rechtvaardigingsgrond 'gerechtvaardigd belang' (artikel 8 onder f Wbp). Voor de sporter of toeschouwer is het meestal weinig ingrijpend om op het internet genoemd te worden, terwijl de opsteller van het bericht vaak een te respecteren belang heeft bij het noemen en/of afbeelden van de personen om wie het gaat. Velen beleven plezier aan de berichten die worden geplaatst (dat is de enige verklaring voor het succes van social media). Veel berichten voorzien daarnaast ook in een concrete informatiebehoefte. Denk bijvoorbeeld aan het plaatsen van wedstrijduitslagen na een sportevenement.

Daarnaast legt de Wbp aan de verantwoordelijke beveiligings- en informatieverplichtingen op. Hij moet de door hem verzamelde persoonsgegevens goed beveiligen en informatie te verschaffen aan degenen wier persoonsgegevens hij verwerkt. Voorts moet de verantwoordelijke van tevoren melding doen bij het CBP van de voorgeno-

6. Zie Registratiekamer 15 oktober 1993, 92.F.008 (kentekens); Registratiekamer 21 juni 1996, 95.O.043 (postcodes met huisnummers) en Registratiekamer 19 maart 2001, z2000-0340 (IP-adressen).
7. HvJ EG 6 november 2003, nr. C-101/01, *NJ* 2004, 248 (*Bodil Lindqvist*).
8. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 69-70 (MvT Wbp).
9. Artikel 7 Wbp.
10. Artikel 9 Wbp.
11. Artikel 8 onder a-f Wbp.
12. Artikel 8 onder a Wbp.
13. Artikel 8 onder b Wbp.
14. Artikel 8 onder f Wbp.

men verwerking van persoonsgegevens[15] – tenzij het een activiteit betreft die valt onder een van de wettelijke vrijstellingen (waarover hierna meer).[16]

Maar op wie rusten die verplichtingen eigenlijk?

Bij veel sportieve social-media-initiatieven is het moeilijk vast te stellen wie nu precies de verantwoordelijke is. De website van het team, de blog van de trainer, het Twitteraccount van de speler en de Teamers-pagina die door de coach is opgezet, het zijn allemaal initiatieven waar verschillende partijen hun deel aan hebben. Doorgaans zal de persoon die beslist welke inhoud wordt geplaatst als verantwoordelijke worden aangemerkt. Wanneer het gaat om de officiële website van een vereniging, dan zal dat de verantwoordelijke zijn, en niet de webmaster die de stukjes plaatst. Maar of de onlineactiviteiten van het vrijwilligerslegioen (de coaches, trainers, managers, begeleiders, organisatoren, enz.) ook zomaar aan de vereniging kunnen worden toegeschreven is ongewis.

Als er geen duidelijke regels door de club zijn gesteld, ligt het voor de hand dat degene achter het toetsenbord als (mede)verantwoordelijke heeft te gelden. Als er wel een beleid is vastgesteld, dan biedt dat vaak een goed vertrekpunt om te bepalen bij wie de zeggenschap rust over hetgeen wordt geplaatst. Naast een beoordeling van reglementen en overeenkomsten, zal ook gekeken moeten worden naar het feitelijke aandeel dat de verschillende deelnemers hebben in een online-initiatief. Een paar voorbeelden om dit te illustreren.

- Wanneer de club bepaalde leden de toegang geeft tot de website, de Hyves-pagina of andere social-mediasites van de sportvereniging – en er beleid is dat bepaalt wat er wel en niet 'gepost' mag worden, dan is de sportvereniging in beginsel zelf de verantwoordelijke. De secretaris die de wedstrijduitslagen op de site bijwerkt, zal zich achter de sportvereniging kunnen verschuilen indien hij zou worden aangesproken op grond van de Wbp.
- Wanneer de sportvereniging alleen de techniek heeft klaargezet, maar het gebruik overlaat aan de leden (bijvoorbeeld door de teams een eigen pagina op de website van de sportvereniging in beheer te geven), dan is het waarschijnlijk dat zowel de vereniging als de plaatser van de content als verantwoordelijke wordt gezien. Er zijn dan dus twee 'verantwoordelijken' die zowel ieder voor zich als gezamenlijk op naleving van de Wbp kunnen worden aangesproken.
- Wanneer het clubbeleid bepaalt dat alleen via de 'officiële' website wordt gecommuniceerd en niettemin enthousiaste leden of fans zelfstandig Facebook- of Twitteraccounts aanmaken die bedoeld zijn om over de sportvereniging te praten, dan zal de laatste in de regel niet verantwoordelijk gehouden kunnen worden voor de persoonsgegevens die in dat kader worden verwerkt.

Onlinebeeldmateriaal – even gewoon als omstreden

In de meeste gevallen zal de 'verantwoordelijke' achter een social-mediasite zich verder in de Wbp moeten verdiepen dan de hiervoor besproken basisregels. Een van de redenen daarvoor is dat er tegenwoordig zeer vaak foto's worden geplaatst of uitgewisseld langs deze kanalen. En met foto's is – vanuit een privacyrechtelijk perspectief – iets bijzonders aan de hand. Wanneer op een foto te zien is dat een sporter een getinte huidskleur heeft, of blond haar en blauwe ogen, dan bevat die foto ook gegevens omtrent het ras van de afgebeelde persoon. En dat zijn in jargon 'gevoelige persoonsgegevens'.

Aan de verwerking van gevoelige gegevens stelt de wet extra strenge eisen.[17] De vereniging of sporter die een foto op zijn website of Facebook-pagina plaatst, maakt zich in principe schuldig aan een 'verwerking van gevoelige persoonsgegevens', zodra het ras van de afgebeelde perso(o)n(en) uit de afbeelding valt op te maken.

Daarmee wordt het in één klap een stuk moeilijker om aan de Wbp te voldoen. Dat komt doordat de wet extra strenge eisen stelt aan de verwerking van gevoelige persoonsgegevens. Van de eerder genoemde rechtvaardigingsgronden blijft in wezen alleen nog de uitdrukkelijke toestemming van de betrokkene over. Dat betekent dat een foto in de regel alleen 'legaal' geplaatst kan worden als alle daarop afgebeelde personen daarvoor hun toestemming hebben gegeven. Die toestemming moet in vrijheid zijn gegeven, nadat voldoende duidelijke en concrete informatie over de voorgenomen verwerking is verschaft. Wanneer (ook) gevoelige persoonsgegevens worden verwerkt is impliciete toestemming is niet voldoende.[18] Daarnaast moet de verantwoordelijke desgevraagd kunnen aantonen dat inderdaad toestemming is verleend én dat dit is gebeurd op een wijze die overeenstemt met de wettelijke eisen.[19] Hij draagt dus de bewijslast op dit punt. In de praktijk komt het er daardoor op neer dat de toestemming schriftelijk moet worden gevraagd, of op een andere wijze die achteraf kan worden gereproduceerd.

15. Artikel 27 Wbp.
16. Artikel 29 Wbp jo. Vrijstellingsbesluit Wbp (Besluit van 7 mei 2001, *Stb.* 2001, 250), waarin onder meer een vrijstelling voor communicatiebestanden en voor ledenadministraties is opgenomen.
17. Artikel 16 Wbp bevat een algemeen verbod tot het verwerken van gevoelige gegevens; in de artikelen 17-23 worden uitzonderingen op dat verbod gegeven.
18. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 67 (MvT Wbp).
19. Dit wordt ook wel aangeduid als de 'dubbele bewijslast' die op de verantwoordelijke rust. Zie T.F.M. Hooghiemstra, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2003, p. 43.

Vele rechters hebben al geprobeerd om deze wettelijke eis met enige souplesse te interpreteren om tegemoet te komen aan maatschappelijke ideeën over wat wel en niet door de beugel kan. Ook de Nederlandse privacywaakhond, het CBP, heeft zich hier over uitgelaten. In zijn 'Richtsnoeren publicatie van persoonsgegevens op internet'[20] heeft het CBP het standpunt ingenomen dat foto's alleen onder de strenge regels voor gevoelige persoonsgegevens vallen wanneer de foto's worden gepubliceerd met het 'uitdrukkelijk doel om onderscheid te maken naar ras'. Dit standpunt is wel met waardering ontvangen, maar kan niet worden verheven tot rechtsregel.
Sterker nog, het welwillende standpunt van het CBP is sinds 2010 alweer achterhaald door jurisprudentie van de Hoge Raad. In zijn arrest van 23 maart 2010[21] (dat overigens is gewezen in een strafzaak), geeft de Hoge Raad aan dat de Wbp op dit punt duidelijk is:

'Uit de wetgeschiedenis volgt dat niet alleen gegevens die direct het ras van een persoon betreffen, maar ook gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals een foto van een persoon, als "gevoelige" informatie moet worden aangemerkt.'

Omdat het nu eenmaal de taak van de rechter is om de wet toe te passen, en niet om de scherpe kantjes er af te vijlen, heeft Nederland het hier dus maar mee te doen. Bijna tien jaar geleden heeft het Europese Hof van Justitie overigens een net zo rechtlijnig standpunt ingenomen in het *Lindqvist*-arrest.[22] Mevrouw Lindqvist had voor de computercursus die zij volgde een homepage gemaakt, en daarop stukjes geplaatst over zichzelf en 18 van haar collega's in de kerkgemeente waar zij actief was. Zo schreef zij dat een van haar collega's haar voet had bezeerd en met gedeeltelijk ziekteverlof was. De betreffende collega was niet van tevoren geraadpleegd en had (dus) geen 'uitdrukkelijke toestemming' verleend voor het plaatsen van deze tekst over haar.

De betreffende passage is door mevrouw Lindqvist verwijderd zodra zij vernam dat haar collega niet gelukkig was met de tekst. In de ogen van de Zweedse rechtbank was het kwaad toen echter al geschied: mevrouw Lindqvist had zich schuldig gemaakt aan een verwerking van 'gevoelige persoonsgegevens',[23] zonder dat zij van tevoren een melding had gedaan bij de privacytoezichthouder en zonder dat zij uitdrukkelijke toestemming had verkregen van degenen over wie zij schreef. Voor die overtredingen van de privacywetgeving werd zij veroordeeld tot een fikse boete.

Tussenconclusie: onlinecontent valt onverkort onder de Wbp

Wat voor de blog van mevrouw Lindqvist geldt, zal ook gelden voor veel van de sportgerelateerde content die via social media wordt uitgewisseld. Hiervoor werd uiteengezet dat er zowel op Europees als op nationaal niveau principiële rechterlijke uitspraken liggen die bepalen dat de wet strikt geïnterpreteerd moet worden. Hoewel het voor menigeen tegen het rechtsgevoel indruist, zijn onlineberichten en foto's in veel gevallen niet toegestaan, ook niet wanneer zij 'onschuldig' en goed bedoeld zijn.

Wanneer men actief wordt op social media is het dus niet eenvoudig om volledig aan alle eisen van de Wbp te voldoen. Plaatst dit de sportvereniging voor de keuze tussen het vermijden van social media of het bewust schenden van de privacyregels?
Nee, zo zwart-wit is het niet. Bij de beoordeling van verwerkingen van persoonsgegevens wordt namelijk ook gekeken naar de mate van zorgvuldigheid die de verantwoordelijke heeft betracht en de gevolgen die de verwerking voor de betrokkenen heeft gehad. Indien op een blog of social-media-account goede informatie wordt verstrekt over de verwerking van persoonsgegevens en een procedure beschikbaar is om ongewenste verwerkingen effectief te laten staken, dan wordt daarmee het risico op ernstige inbreuken op de persoonlijke levenssfeer van de betrokkenen al behoorlijk beperkt. Indien vervolgens ook nog kan worden aangetoond dat de redactie heeft nagedacht over de wijze waarop met persoonsgegevens omgegaan moet worden (en zich daarbij de belangen van de betrokkenen heeft aangetrokken), dan zal er minder snel een sanctie opgelegd (kunnen) worden. Dat volgt uit het evenredigheidsbeginsel, dat eveneens een belangrijke rol speelt in het privacyrecht.[24]

De club moet positie kiezen om zichzelf en haar leden te beschermen

Het is voor zowel een sportvereniging als haar actieve leden van belang om te weten wie de verantwoordelijke is ten aanzien van de vele onlineactiviteiten rondom de club. De verantwoordelijke is namelijk degene die aan de verschillende verplichtingen uit de Wbp moet voldoen.[25] Daar waar de vereniging als de verantwoordelijke kwalificeert, zal hij dus maatregelen moeten treffen. En

20. College bescherming persoonsgegevens, 'Richtsnoeren publicatie van persoonsgegevens op internet', Den Haag 2007 (www.cbpweb.nl/Pages/rs_publicatie_persgeg_internet.aspx).
21. HR 23 maart 2010, *LJN* BK6331.
22. HvJ EG 6 november 2003, nr. C-101/01, *NJ* 2004, 248 (*Bodil Lindqvist*).
23. Het betrof persoonsgegevens van medische aard. In Nederland volgt het verbod om dergelijke gegevens te verwerken uit artikel 16 Wbp.
24. Het evenredigheidsbeginsel werkt door in het privacyrecht omdat de Wbp is gebaseerd op de Europese Richtlijn inzake de bescherming van persoonsgegevens (95/46) en daarmee onderworpen is aan Europees recht. Artikel 52 lid 1 van het Handvest van de grondrechten bepaalt dat beperkingen op de uitoefening van het recht op gegevensbescherming bij wet moeten worden vastgesteld en de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen, en dat, met inachtneming van het evenredigheidsbeginsel slechts beperkingen kunnen worden vastgesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.
25. De verantwoordelijke moet er onder meer op toezien dat de persoonsgegevens behoorlijk beveiligd worden, dat aan de wettelijke informatieverplichtingen wordt voldaan en hij moet verzoeken van betrokkenen om inzage in hun gegevens afhandelen.

in de gevallen waar de leden als privépersoon als de verantwoordelijke moeten worden gezien (en de vereniging zelf geen juridische risico's loopt) kan het toch in het belang zijn van de vereniging om naleving van de wet te bevorderen.

Een sportvereniging doet er daarom goed aan om te inventariseren wat voor uitingen er op het internet en social media betrekking hebben op 'haar' activiteiten, en om beleid te maken ten aanzien van het gebruik van social media en internet ten behoeve van de verenigingsactiviteiten. Ten aanzien van de 'eigen' initiatieven moet worden gekeken of er melding moet worden gedaan bij het CBP, of aan de informatieplichten is voldaan, en of de bewaarde gegevens echt allemaal nodig zijn voor het vastgestelde verzameldoel. Ten aanzien van de andere social-media-activiteiten zou de vereniging haar actieve leden moeten wijzen op hun verantwoordelijkheid om aan de privacywetgeving te voldoen. Een beetje voorlichting zou dan geen overdreven luxe zijn.

Meldplicht

Zoals gezegd moet de verantwoordelijke zich afvragen of de door hem aangelegde gegevensverzameling moet worden gemeld bij het CBP. In principe moet de verantwoordelijke ten aanzien van iedere verzameling van persoonsgegevens die hij aanlegt en verwerkt een melding doen bij het CBP.[26]

Voor een aantal veel voorkomende verwerkingen zijn door de wetgever echter vrijstellingen verleend. Daartoe is het Vrijstellingsbesluit genomen, waarin 42 soorten verwerkingen zijn opgesomd.[27]

Voor elke categorie van verwerkingen heeft het Vrijstellingsbesluit specifieke voorwaarden geformuleerd, onder andere ten aanzien van de bewaartermijn van de gegevens en de doelen waarvoor zij gebruikt mogen worden. Als er niet aan die voorwaarden wordt voldaan (bijvoorbeeld omdat de gegevens langer worden bewaard dan in de vrijstellingsvoorwaarden bepaald), zal de verantwoordelijke gewoon een melding moeten doen, ook al heeft hij een geldige reden voor het afwijken van de vrijstellingsvoorwaarden.

Voor sportverenigingen zijn dat vooral de vrijstellingen 'lidmaatschap en begunstiging',[28] 'oud-leden en oud-leerlingen'[29] en 'communicatiebestanden'[30]. Deze vrijstellingen bieden voor de meeste social-mediatoepassingen echter geen soelaas. De social-mediapagina's komen niet in de plaats van de ledenadministratie, maar vormen een ander bestand, dat niet redelijkerwijs nodig is voor het bijhouden van de ledenadministratie. Zij worden veeleer gebruikt voor communicatie met de leden en fans. Daardoor vallen de vrijstellingen over leden en lidmaatschap af. Ook vallen social-mediapagina's vaak niet onder de vrijstelling voor 'communicatiebestanden'. Hierop kan namelijk alleen een beroep worden gedaan indien het verwerken van gegevens 'noodzakelijk' is voor het onderhouden van het contact met de betrokkenen. De meeste onlinegegevensverzamelingen bevatten veel meer gegevens dan alleen de gegevens die nodig zijn voor het versturen van berichten; denk bijvoorbeeld aan pasfoto's en verjaardagen. In dat geval is de vrijstelling 'communicatiebestanden' niet van toepassing en moet dus een melding worden verricht.

En op de kroonjuwelen passen

Gegevensverzamelingen die een aparte bespreking verdienen zijn de ledenbestanden en het spelersvolgsysteem. De gegevens die daarin staan zijn voor marktpartijen veel interessanter dan de inhoud van de website, de blogs en de tweets.

Ledenbestanden zijn interessant voor allerlei marktpartijen, omdat via de vereniging een heel specifieke doelgroep kan worden bereikt. Hoe meer gegevens over de leden bekend zijn, des te beter kan een marketeer bepalen in hoeverre het ledenbestand overeenstemt met zijn doelgroep. Over het algemeen worden zaken zoals gezinssamenstelling, leeftijd en huisadres in de ledenadministratie bijgehouden. Daarnaast komen in voorkomende gevallen ook specifiekere gegevens over de leden, zoals nationaliteit, inkomen, beroep, en vooropleiding, in het ledenbestand voor.

Sponsors verlangen vaak toegang tot het ledenbestand in ruil voor hun sponsorbijdrage. De vereniging moet in die gevallen op zijn hoede zijn. Het is niet in alle gevallen verboden om aan een sponsor gegevens te verstrekken over de leden, maar er moet wel aan een aantal voorwaarden zijn voldaan. In de meeste gevallen moet de vereniging toestemming hebben gevraagd aan zijn leden om hun gegevens te verstrekken. Soms kan die toestemming indirect worden verkregen, bijvoorbeeld via de ledenvergadering. Als het gaat om activiteiten die voor de vereniging gebruikelijk zijn of zijn goedgekeurd door de ledenvergadering, hoeft geen expliciete toestemming gevraagd te worden aan de leden.[31]

Als de gegevens worden verstrekt met het oog op direct-marketingactiviteiten moet de vereniging de leden eerst informeren over de voorgenomen verstrekking, bijvoorbeeld via het clubblad of de internetsite van de vereni-

26. Iedere geautomatiseerde verwerking van persoonsgegevens moet worden gemeld (artikel 27 Wbp), tenzij het een verwerking betreft waarvoor een wettelijke vrijstelling bestaat (art. 29 Wbp).
27. Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens, te vinden op http://wetten.overheid.nl.
28. Artikel 3 Vrijstellingsbesluit.
29. Artikel 41 Vrijstellingsbesluit.
30. Artikel 42 Vrijstellingsbesluit.
31. Zie 'Verstrekken van uw gegevens uit de ledenadministratie', CBP Informatieblad nr. 30, februari 2011, beschikbaar op www.cbpweb.nl/Pages/inf_va_ledenadministratie.aspx.

ging. Daarbij moet aan de leden een redelijke termijn worden geboden om verzet aan te tekenen tegen de verstrekking van hun gegevens voor dit doel.[32] Zodra een lid verzet aantekent, moet de vereniging het gebruik van diens gegevens voor direct marketing altijd direct beëindigen.[33] Het lid hoeft niet te zeggen waarom hij verzet aantekent en de vereniging mag geen vergoeding vragen om een verzoek in behandeling te nemen.
Verder moet uiteraard goed worden opgelet welke gegevens worden verstrekt. In beginsel mogen niet meer gegevens worden doorgegeven aan de sponsor dan hij redelijkerwijs nodig heeft voor de afgesproken doelen. Daarbij moet uiteraard ook de informatie die door de vereniging bij verkrijging van de gegevens is verschaft worden betrokken. Indien bijvoorbeeld op het inschrijfformulier is vermeld dat de gegevens alleen voor de ledenadministratie zullen worden gebruikt, kan daar niet zomaar op worden teruggekomen. In zijn algemeenheid echter, wordt een sponsor geacht voldoende te hebben aan de naw-gegevens van de leden. Specifiekere informatie uit het ledenbestand zou dan ook niet moeten worden verstrekt.

Ten slotte moet juist in het tijdperk van digitalisering worden gelet op beveiliging van de gegevens die zich in het ledenbestand bevinden. Als verantwoordelijke rust op de vereniging de verplichting om 'passende technische en organisatorische maatregelen'[34] te treffen om verlies en ongeoorloofd gebruik van de persoonsgegevens te voorkomen.[35] Daar hoort bijvoorbeeld bij dat de computer(s) waarop de ledenbestanden staan, zich niet op algemeen toegankelijke plaatsen mogen bevinden, althans dat de ledenadministratie is voorzien van een toegangsbeveiliging met bijvoorbeeld een wachtwoord. Dat wachtwoord moet vervolgens uiteraard ook niet rondslingeren of op een Post-It-blaadje op het beeldscherm worden geplakt.

Wanneer ledenbestanden van de vereniging online worden ontsloten, ontstaan onmiddellijk nieuwe veiligheidsrisico's. De vereniging zal die moeten betrekken in haar beoordeling wanneer de ledenlijst digitaal wordt verspreid. Opnieuw geldt uiteraard dat bezien moet worden of de leden hebben ingestemd (al dan niet via de ledenvergadering) met onlineverspreiding van de ledenlijst. Als dat station is gepasseerd moet worden bepaald hoe elektronische verspreiding kan worden ingericht op een wijze die de belangen van de leden voldoende beschermt. Het rondsturen van een Excel-bestand leidt al snel tot bovenmatige (niet-noodzakelijke) verwerking van persoonsgegevens en maakt het erg eenvoudig om de gehele ledenlijst te gebruiken voor niet-toegestane doeleinden. Het plaatsen op het internet is zo mogelijk nog onverstandiger, omdat in dat geval de kans wordt vergroot dat niet-leden toegang krijgen tot de gegevens. Daarentegen is een module op het afgeschermde gedeelte van de website van de vereniging, waar men leden kan opzoeken, in principe 'veiliger' dan de ouderwetse stencils. De gegevens zijn dan namelijk minder gemakkelijk in hun geheel over te nemen en eventuele fouten kunnen effectiever worden hersteld.[36]

Slot

Het is beslist geen sinecure om onlineactiviteiten op een manier op te zetten die voldoet aan de eisen van de Wbp. Dat geldt in het bijzonder in de sport, omdat veel sportieve gegevens tegelijkertijd ook 'gevoelige persoonsgegevens' zijn, voor de verwerking waarvan extra strenge wettelijke eisen gelden. Is de keuze dan beperkt tot niets doen met internet of bewust de wet overtreden? Niet helemaal. Bij de beoordeling in concrete gevallen maakt het veel verschil of de verantwoordelijke zich heeft gehouden aan de eisen van zorgvuldigheid en proportionaliteit. Daarom is het aan te raden om bij iedere uiting op internet of op social-mediaplatforms na te gaan welke persoonsgegevens worden gepubliceerd, en je af te vragen of dat nodig en gepast is. Als iemand vervolgens bezwaar maakt tegen de publicatie van zijn naam, foto of andere persoonsgegevens is het verstandig om daar correct naar te handelen. Wie zich aan die basisregels houdt, zal een stuk minder snel in de (privacyrechtelijke) problemen komen, want in Nederland wordt zelden opgetreden tegen goedbedoelende twitteraars en bloggers.

32. Zie 'Verstrekken van uw gegevens uit de ledenadministratie', CBP Informatieblad nr. 30, februari 2011.
33. Artikel 41 lid 2 Wbp.
34. Artikel 13 Wbp.
35. Artikel 13 Wbp.
36. Denk aan bijvoorbeeld het per abuis vermelden van een geheim telefoonnummer. Bij verspreiding van ledenlijsten op papier kan dit niet worden teruggedraaid, terwijl de onlineledenlijst vrijwel ongemerkt zal kunnen worden aangepast.