Handboek Sport & Privacy

Bezoekadres	Postadres	Telefoon	Email	Web
Papendallaan 60, Arnhem	Postbus 302, 6800 AH Arnhem	+31 (0)26 483 44 00	info@nocnsf.nl	nocnsf.nl

Inhoudsopgave

1. Inleiding

In aanloop naar de inwerkingtreding van de Algemene verordening Gegevensbescherming (AVG) is in 2017 de eerste uitgave van het handboek Sport & Privacy verschenen. Sinds de inwerkingtreding van de AVG hebben de ontwikkelingen op het gebied van privacy regelgeving niet stilgestaan en is een opvolger van het handboek meer dan welkom. Dit digitale handboek is een geupdate versie met de nieuwste inzichten.

Het handboek behandelt op laagdrempelige wijze de basisprincipes van het gebruik van persoonsgegevens vanuit het gegevensbeschermingsrecht en is geschreven voor intern gebruik door sportbonden en sportverenigingen. Er wordt zoveel mogelijk aansluiting gezocht bij de dagelijkse sportpraktijk. Ook wordt getracht vage begrippen te vertalen in begrijpelijke verplichtingen.

Let op: Dit handboek is bedoeld als bron van informatie en is geen juridisch advies. Aan de inhoud van dit handboek kunnen dan ook geen rechten worden ontleend. Iedere sportbond en sportvereniging is zelf verantwoordelijk voor een correcte en volledige naleving van de privacyregels. Schakel bij twijfel over een juiste toepassing van de geldende regels altijd een specialist in.

Wij wensen je veel leesplezier!

2. Hoe gebruik je dit handboek?

2.1. Wat kan ik in dit handboek vinden?

Dit handboek behandelt het privacyrecht vanuit twee verschillende invalshoeken.

(1) Onderdeel 'Basisregels':
In dit onderdeel leggen we de basisregels uit die gelden in het privacyrecht. Dat doen we vanuit de theorie, aangevuld met sportspecifieke voorbeelden. We leggen uit wat het privacyrecht inhoudt en op wie die nu van toepassing is. We lichten de belangrijkste termen en de belangrijkste rollen toe. Vervolgens nemen we je mee in de basisprincipes die van toepassing zijn op het verwerken van persoonsgegevens.

(2) Onderdeel 'Toepassing in de sport':
In dit onderdeel gaan we in op enkele praktijkthema's waar je als sportorganisatie zoal mee te maken krijgt. We koppelen de thema's aan de belangrijkste regels omtrent de bescherming van persoonsgegevens. We hebben geprobeerd per onderwerp zoveel mogelijk eenzelfde structuur aan te houden. We verwijzen je soms terug naar het onderdeel 'Basisregels', simpelweg omdat je daar meer informatie kunt teruglezen.

2.2. Hoe is het handboek verder opgebouwd?

De onderwerpen in dit handboek worden regelmatig aangevuld met:

- Sportspecifieke voorbeelden;
- Cases (hier verwijzen we soms naar uitspraken van het Hof van Justitie);
- Verwijzingen naar belangrijke valkuilen (**Let op!**);
- Praktische tips (**Tips**);
- Verwijzingen naar externe links;
- Templates.

2.3. Hoe navigeer ik door dit handboek?

Dat hangt er vanaf. Is het onderwerp privacy of gegevensbescherming nieuw voor je? Dan adviseren we je het gehele handboek door te nemen en te beginnen met lezen bij het onderdeel Basisregels. Ben je gericht

op zoek naar informatie? Kijk dan in het menu en klik op het gewenste onderdeel. Je komt op die manier snel terecht bij het gewenste onderwerp.

2.4. Wat is het handboek niet?

Wees je ervan bewust dat dit handboek uiteindelijk niet meer is dan een intern hulpmiddel om inzicht en overzicht te krijgen in de regels omtrent gegevensbescherming. Zo geeft het handboek een praktijkgerichte beschrijving van de regelgeving, maar het is geen reglement en je kunt er geen bevoegdheden aan ontlenen. Twijfel je over toepassing van de regels? Dan adviseren we je een privacy-deskundige om raad te vragen.

ONDERDEEL BASISREGELS

3. Privacy & de AVG

3.1. Inleiding

Het recht op privacy kun je eenvoudig uitleggen als het recht om met rust gelaten te worden. Het recht op privacy is 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:

- Ruimtelijk: de vrijheid om zelf te bepalen waar je verblijft;
- Lichamelijk: de vrijheid om zelf te beslissen over jouw lichaam;
- Relationeel: de vrijheid om zelf te kiezen met wie je omgaat;
- Informationeel: de vrijheid om zelf te beschikken over jouw eigen persoonsgegevens en te bepalen wat een ander met die gegevens mag doen.

Dit handboek staat volledig in het teken van de informationele privacy. Van de vier genoemde privacy aspecten zal dit onderdeel het meeste terugkeren in de dagelijkse praktijk van jouw sportorganisatie.

3.2. De Algemene verordening gegevensbescherming (AVG)

Spreek je met iemand over (informationele) privacy, dan duurt het nooit lang voordat de term 'AVG' voorbij komt. AVG is de afkorting voor de Algemene verordening gegevensbescherming. In de AVG staan de belangrijkste regels voor het omgaan met persoonsgegevens. In de Uitvoeringswet AVG (UAVG) heeft Nederland die algemene regels verder gespecificeerd (bijvoorbeeld door bepaalde uitzonderingen toe te voegen). Het is daarom belangrijk dat je de AVG altijd samen leest met de UAVG.

In dit (digitale) handboek geven we uitleg over de belangrijkste regels omtrent de bescherming van persoonsgegevens. Wil je deze regels daadwerkelijk kunnen toepassen, dan is basiskennis van de AVG onmisbaar. Belangrijk is dat je begrijpt wat de basisregels zijn en hoe je die in de dagelijkse praktijk moet toepassen.

Externe links	Uitleg
Website EDPB	Op de website van de European Data Protection Board vind je opinies & guidelines over de AVG.
Website Autoriteit Persoonsgegevens	Op de website van de AP vind je allerlei praktische informatie en tips over de AVG.
Officiële tekst AVG	Hier lees je de officiële tekst van de AVG.
Officiële tekst UAVG	Hier lees je de officiële tekst van de UAVG.
AVG Handleiding	Hier download je een handige AVG handleiding vanuit de Rijksoverheid.

4. De belangrijkste termen

4.1. Persoonsgegeven

Een persoonsgegeven is elk gegeven over een levend en identificeerbaar persoon. Dat lijkt simpel, maar toch moeten we dit nader toelichten.

Betrekking op een persoon

De informatie moet iets zeggen over een concreet persoon. Informatie die niets zegt over een persoon is dan ook geen persoonsgegeven.

Een datum en tijdstip van een sportwedstrijd van Vereniging X is bijvoorbeeld geen persoonsgegeven, want het heeft geen betrekking op een persoon. Wanneer Vereniging X echter in de wedstrijdadministratie vastlegt dat Pietje Puk deelneemt aan de sportwedstrijd, dan is er wel sprake van een persoonsgegeven, omdat de gegevens over de sportwedstrijd dan gaan over de deelname van Pietje Puk aan de wedstrijd.

Geïdentificeerd of identificeerbaar (direct of indirect)

Een gegeven is pas een persoonsgegeven als het herleidbaar is tot een persoon. Dat betekent dat je de identiteit van iemand kunt vaststellen op basis van de informatie. Een combinatie van bijvoorbeeld de gegevens naam, adres en lidmaatschapsnummer is zo uniek, dat je ermee (hoogstwaarschijnlijk) een persoon kunt identificeren. Je kunt die persoon soms ook identificeren op basis van minder directe (dus: indirecte) gegevens. Denk aan uiterlijke kenmerken (zoals postuur, haarkleur), sociale en economische kenmerken (zoals een topsportprogramma) en online gegevens (zoals een IP-adres).

Met deze indirecte gegevens op zich is het misschien niet mogelijk één persoon te identificeren, maar wel wanneer je de gegevens met elkaar combineert of wanneer je ze koppelt aan andere beschikbare gegevens. Denk aan gegevens die je zelf tot je beschikking hebt, maar ook aan gegevens die bijvoorbeeld gemakkelijk via internet te vinden zijn. Wanneer je de identiteit van iemand dus niet direct kunt vaststellen, dan moet je je alsnog afvragen of dat wel zou kunnen. Bepalend is daarbij of je dat dan zonder al te veel inspanning voor elkaar kan krijgen.

> **Voorbeeld: teamfoto**
> 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.

Bij de beoordeling of een gegeven een persoonsgegeven is, moet je dus rekening houden met de redelijke mogelijkheden die je hebt om de informatie te herleiden tot een uniek persoon. Een beetje vreemd misschien, maar of iets een persoonsgegeven is kan dan ook per organisatie verschillen.

Let op! Soms ben je misschien van mening dat iets geen persoonsgegeven is, omdat je het niet direct kunt linken aan een persoon. Bedenk je dan altijd of je andere bestanden tot je beschikking hebt, of dat er andere informatie openbaar beschikbaar is, op basis waarvan je de informatie alsnog zou kunnen linken aan een persoon. We raden aan om informatie waarvan je vermoedt dat die direct of indirect herleidbaar is, te behandelen als persoonsgegevens.

Natuurlijk persoon

Een gegeven is alleen een persoonsgegeven als het gaat over een natuurlijk persoon. Dat betekent dat gegevens over organisaties (verenigingen, sportbonden, etc.) geen persoonsgegevens zijn. Wanneer je gegevens verwerkt van personen binnen die organisatie (medewerkers, vrijwilligers) dan is er wel weer sprake van verwerking van persoonsgegevens.

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.

Geen persoonsgegeven
Valt écht niet te achterhalen op wie informatie betrekking heeft, dan is sprake van anonimiteit. In theorie is de AVG dan niet van toepassing. Immers, de AVG is alleen van toepassing op de verwerking van persoonsgegevens. Vertrouw er echter niet zomaar op dat de AVG niet van toepassing is. Het is tegenwoordig steeds lastiger (of zelfs onmogelijk) om te zorgen dat informatie in geen enkel opzicht meer kan worden gelinkt aan een persoon (zeker wanneer bepaalde gegevens ook publiekelijk bekend zijn, denk bijvoorbeeld aan topsportprestaties).

Let op! Als we het hebben over pseudonimiseren dan is er nog wél sprake van een persoonsgegeven. Met pseudonimiseren worden identificeerbare elementen van een persoonsgegeven weggehaald en ergens anders bewaard. Omdat je deze actie weer kunt terugdraaien en je daarmee de data weer kunt koppelen aan een persoon, moeten deze gegevens als persoonsgegevens worden behandeld.

Voorbeeld: misverstand 'anonimiteit'
Een bekend misverstand van het anonimiseren van persoonsgegevens is het linken van openbare informatie aan een (lid)nummer in plaats van een naam. Het doel hiervan is 'anonimiteit', zodat niet meer te achterhalen valt op wie de informatie betrekking heeft. Echter, vaak kan de club zo'n (lid)nummer weer koppelen aan een persoon. Voor de club is het (lid)nummer dus alsnog een persoonsgegeven.

4.1.1. Bijzondere persoonsgegevens

De AVG maakt een onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die vanwege hun aard extra gevoelig zijn; bij het verwerken ervan ontstaan namelijk extra privacy-risico's. Daarom bestaan hiervoor strengere regels. Het is zelfs verboden om bijzondere persoonsgegevens te verwerken, tenzij er een specifieke uitzondering van toepassing is die de verwerking rechtvaardigt.

Bijzondere persoonsgegevens zijn gegevens over iemands:
- Ras of etnische afkomst;
- Politieke opvattingen;
- Godsdienst of levensovertuiging;
- Lidmaatschap van een vakbeweging;
- Genen;
- Biometrie (zoals vingerafdrukken);
- Gezondheid;

- Seksueel gedrag/seksuele gerichtheid.

Het begrip 'gezondheidsgegeven' moet je erg ruim opvatten. Het gaat niet alleen om medische informatie, maar om alle gegevens over iemands geestelijke of lichamelijke gezondheid. Ook gegevens over rook- en drinkgedrag, allergieën, lidmaatschap van een patiënten hulpgroep of dieetclub zijn gezondheidsgegevens.

Vaak ontstaat verwarring over (pas)foto's. Kan je een foto classificeren als een bijzonder persoonsgegeven indien je daaruit ras/etnische afkomst kan afleiden? De Autoriteit Persoonsgegevens (AP) introduceert een doelgerichte benadering als criterium. De AP vindt dat foto's geen bijzondere persoonsgegevens inhouden, indien:

- Het maken van de foto's hier niet specifiek op is gericht; en
- De foto's niet worden gebruikt voor het maken van onderscheid; en
- Het niet redelijk is om te verwachten dat anderen dat wellicht wel doen; en
- Het onvermijdelijk is dat kenmerken van bijzondere persoonsgegevens zichtbaar zijn op de foto.

Voorbeeld: teamfoto
Een teamfoto van de D4 van voetbalvereniging DSH zal geen verwerking inhouden van bijzondere persoonsgegevens. Let op, bij het maken en publiceren van foto's is vaak wel het portretrecht van toepassing. Meer hierover lees je in het onderdeel 'Beeldmateriaal'.

Let op! 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 app downloaden die is gericht op mensen met een afwijking of ziekte. Denk er ook aan dat gegevens eerst gewone persoonsgegevens kunnen zijn, maar over de tijd heen gezondheidsgegevens kunnen worden. Bijvoorbeeld gegevens van een stappenteller die intensief wordt gebruikt. Op het eerste gezicht houd je alleen het aantal stappen bij dat iemand heeft gezet. 1000 stappen per dag is geen gezondheidsgegeven, zou je zo zeggen. Uit die gegevens kan je echter na een jaar lang gebruik wellicht aflezen of iemand een goede conditie heeft. Let dus goed op de context van de informatie om te beoordelen of op enige manier sprake kan zijn van bijzondere persoonsgegevens.

Wanneer mag ik bijzondere persoonsgegevens verwerken?
Er bestaan veel wettelijke uitzonderingen op het verwerkingsverbod voor bijzondere persoonsgegevens. Een deel is geregeld in de AVG en een deel in de UAVG. De meest voor de hand liggende uitzonderingen zijn:

- De betrokkene geeft uitdrukkelijke toestemming;
- De verwerking is noodzakelijk in verband met arbeidsrecht/sociale zekerheids- en sociale beschermingsrecht;
- De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- De verwerking is noodzakelijk 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 aan de betrokkene onmogelijk blijkt.

Naast bovengenoemde, gelden er nog meer uitzonderingen. Deze kun je vinden in artikel 9 van de AVG of in de UAVG. Twijfel je of er een wettelijke uitzondering van toepassing is op je verwerking met bijzondere persoonsgegevens? Vraag dan om deskundig advies.

Een sportorganisatie komt niet vaak in 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.

Voorbeeld: sportmedische keuring
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 handboek buiten beschouwing. De arts of medisch specialist mag gezondheidsgegevens niet zonder uitdrukkelijke toestemming van de sporter verstrekken aan sportorganisaties. De sportorganisatie voert namelijk niet zelf de behandeling uit en heeft geen noodzaak bij het verwerken van de gegevens.

Voorbeeld: gezondheids-app
Als je als sportorganisatie een app laat ontwikkelen waarmee gezondheidsgegevens van sporters worden verwerkt, dan ben je mogelijk verwerkingsverantwoordelijke. Eventuele derden (zoals een IT-dienstverlener) zijn daarbij meestal verwerker. Je dient dan als sportorganisatie te zorgen voor de juiste uitzondering om het verbod op het verwerken van gezondheidsgegevens op te heffen (en deze gegevens te mogen verwerken). Waarschijnlijk heb je 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 welke persoonsgegevens door welke partijen worden verwerkt en waarom. Algemene informatie over het verwerken van persoonsgegevens wordt meestal verstrekt via een privacyverklaring. Daarnaast moet je als sportorganisatie met de IT-dienstverlener een verwerkersovereenkomst sluiten, waarin beveiliging (gezien de gevoeligheid van de gegevens) extra aandacht verdient.

Voorbeeld: sportorganisatie als werkgever
Indien je als sportorganisatie als werkgever optreedt, dan mag je maar in een paar situaties gezondheidsgegevens van personeel verwerken. Dit zijn echter zeer specifieke gevallen die we in dit handboek buiten beschouwing laten. Let wel op, als werkgever mag je in principe niet de fitheid van je werknemers monitoren door ze wearable devices (zoals stappentellers) te laten dragen. Dit mag zelfs niet als de werknemer daarvoor toestemming geeft zo stelt de AP (lees ook onderdeel ‘Basisregels’). Wil je 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 (lees ook onderdeel ‘Talent en topsport’).

Let op! Als je verwerking past binnen één van de verwerkingsgronden, moet de verwerking ook nog gerechtvaardigd zijn (een grondslag hebben) en moet je uiteraard voldoen aan alle andere eisen op het gebied van de AVG.

4.1.2. Gevoelige persoonsgegevens

Dat sommige persoonsgegevens niet ‘bijzonder’ zijn, wil nog niet zeggen dat ze niet alsnog zeer gevoelig kunnen zijn. Denk hierbij aan:

- Gegevens over iemands financiële of economische situatie;
- Gegevens over iemands locatie;

- Gegevens die kunnen worden misbruikt voor (identiteits-)fraude (bijv. kopieën van identiteitsbewijzen);
- 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).

Voor sommige van deze gevoelige gegevens geldt een algemeen verwerkingsverbod, namelijk bij strafrechtelijke gegevens en het burgerservicenummer (BSN), waarover hieronder meer informatie. Indien er geen algemeen verbod geldt, wees ook dan erg voorzichtig met het verwerken van dit soort gegevens!

Strafrechtelijke gegevens
Strafrechtelijke gegevens zijn gegevens over strafrechtelijke veroordelingen en strafbare feiten, maar ook de veiligheidsmaatregelen die daarmee verband houden (zoals een door de rechter opgelegd verbod). Deze gegevens vallen niet onder de categorie bijzondere persoonsgegevens. Gezien de gevoelige aard gelden hiervoor wel strikte regels, vergelijkbaar met die voor bijzondere persoonsgegevens. Strafrechtelijke gegevens mogen namelijk alleen worden verwerkt:

- Onder toezicht van de overheid; of
- Als de verwerking is toegestaan op grond van het Unierecht of nationaal recht (denk aan sectorspecifieke wetgeving of de UAVG). In de UAVG is dit verder uitgewerkt in de artikelen 31-33.

Tip: Een belangrijke maatstaf die je kunt gebruiken in het bepalen of iets een strafrechtelijk gegeven is, is of de gedragingen enkel een redelijk vermoeden van schuld opleveren of dat er daadwerkelijk sprake is van een zwaardere verdenking.

Hoe zit dat dan met tuchtrechtelijke gegevens?
Momenteel is nog onduidelijk of tuchtrechtelijke gegevens onder de UAVG vallen onder het begrip ‘strafrechtelijke gegevens’. In de rechtspraak is eerder geoordeeld dat tuchtrechtelijke gegevens niet onder het regime van bijzondere of strafrechtelijke persoonsgegevens vallen. Echter, in een andere uitspraak van de rechtbank Amsterdam lijkt het erop dat tuchtrechtelijke gegevens wel weer gelijkgesteld moeten worden met strafrechtelijke gegevens.

Tip: Liever geen risico lopen? Behandel dan (vooralsnog) tuchtrechtelijke gegevens als strafrechtelijke gegevens, zoals hierboven beschreven. Verder adviseren we je om de discussie in de gaten te houden.

Burgerservicenummer (BSN)
Het verwerken van het burgerservicenummer is in principe verboden, tenzij de wet dit expliciet toestaat of verplicht. Denk bijvoorbeeld aan de loonadministratie van een werkgever. Een werkgever is verplicht om een kopie van het identiteitsdocument (met daarop een zichtbaar BSN) te bewaren in de loonadministratie.

Je mag dus als sportbond of sportvereniging niet zomaar een kopie maken van iemands paspoort of identiteitskaart (waarop een BSN staat afgebeeld). Dat is een vorm van verwerking en valt 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, maar enkel sprake van inzage.

4.2. Verwerken
Er is al snel sprake van een verwerking van persoonsgegevens. Verwerken is namelijk een zeer breed begrip. Nagenoeg iedere handeling met een persoonsgegeven is in de praktijk een verwerking. Denk aan het

verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, bewaren, verplaatsen, wissen, maar ook aan het kwijtraken, lekken of manipuleren van persoonsgegevens.

Voorbeeld: verwerken van persoonsgegevens
Sportvereniging 't AVG'tje neemt de persoonsgegevens van een nieuw lid, Kees, op in het ledenbestand. 't AVG'tje factureert Kees jaarlijks voor het lidmaatschapsgeld. Bovendien verstuurt zij maandelijks een nieuwsbrief aan Kees. De opname in het ledenbestand, de facturatie en de verzending van de nieuwsbrief zijn voorbeelden van een verwerking van persoonsgegevens.

Verwerkingen vinden in de praktijk niet alleen digitaal plaats, maar ook op papier. Als sprake is van enige vorm van structuur (zodat gegevens gemakkelijk kunnen worden teruggevonden) dan is er sprake van een verwerking. Dus als persoonsgegevens op papier worden gezet met als doel om in een bestand opgenomen te worden, dan worden persoonsgegevens verwerkt. Denk bijvoorbeeld aan de papieren leden-, personeels- en wedstrijdadministratie. Enkel niet-elektronische verwerkingen die ook niet bestemd zijn om in een bestand te worden opgenomen, zijn strikt genomen geen verwerking. Denk aan losse papieren op een bureau met daarin namen van personen, een persoonlijke telefoonnotitie die je kort daarna weggooit of een mondelinge overdracht van gegevens.

Let op! In de praktijk is dat onderscheid lastig te maken. Ben je van plan om de losse papieren te ordenen in een map met naamkaartjes, de telefoonnotitie toch te bewaren of wordt de mondelinge overdracht alsnog vastgelegd in het dossier van de sporter? Dan is het vaak verstandiger om aan te nemen dat wel sprake is van een verwerking.

4.3. De betrokkene

De betrokkene is de natuurlijke persoon op wie een persoonsgegeven betrekking heeft. Het betreft de persoon van wie de persoonsgegevens moeten worden beschermd.

Voorbeeld: betrokkene
Kees wordt als lid opgenomen in het ledenbestand van 't AVG'tje. Kees is 'betrokkene' als het gaat om 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 (zoals verenigingen die lid zijn van een sportbond) zijn geen betrokkenen.

5. De belangrijkste rollen

5.1. De verwerkingsverantwoordelijke

Naast de vraag of de AVG een rol speelt, wil je natuurlijk ook weten wie zich vervolgens aan welke regels moet houden. De AVG noemt deze partij 'de verwerkingsverantwoordelijke'. Je kunt deze rol eigenlijk zien als de baas van een verwerking van persoonsgegevens: hij/zij bepaalt waarom (doel) en hoe bepaalde gegevens wel of juist niet worden verwerkt (middelen).

Voorbeeld: verwerkingsverantwoordelijke
't AVG'tje is de verantwoordelijke voor de verwerkingen van de persoonsgegevens van Kees. De vereniging bepaalt immers hoe en waarom bepaalde verwerkingen plaatsvinden (zoals ledenbeheer, facturatie en nieuwsvoorziening van leden).

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

5.1.1. Zelfstandig verwerkingsverantwoordelijke

Het is mogelijk dat dezelfde persoonsgegevens door meerdere partijen worden verwerkt, maar dan voor verschillende doelen. Deze partijen zijn dan ieder zelfstandig verantwoordelijke voor wat zij zelf met die persoonsgegevens doen.

Voorbeeld: zelfstandig verwerkingsverantwoordelijke
De persoonsgegevens van Kees (zoals zijn e-mailadres) zijn niet alleen bekend bij de sportbond, maar ook bij een sponsor, de lokale vereniging en NOC*NSF. Al deze partijen hebben een eigen doel bij het verwerken van die persoonsgegevens. Ieder van deze partijen is dus zelfstandig verantwoordelijk, omdat zij zelf (en niet de sportbond) het doel en de middelen bij de verwerkingen vaststellen.

5.1.2. Gezamenlijk verwerkingsverantwoordelijke

Vaak kun je makkelijk aanwijzen wie de verwerkingsverantwoordelijke is, maar er zijn ook complexere gevallen denkbaar. Soms zijn namelijk meerdere partijen betrokken bij dezelfde verwerking: de doeleinden en middelen worden gezamenlijk bepaald. Je bent dan gezamenlijk verantwoordelijk voor de verwerking (en ook voor het naleven van de AVG). De partijen moeten dan samen vaststellen wie waar inzicht in heeft en wie waar zeggenschap over heeft. Vaak volgt dat logischerwijs uit de relatie die de partijen hebben met de betrokkenen. Deze rolverdeling moet onderling goed worden vastgelegd (om te voorkomen dat partijen de lasten op elkaar afschuiven). Ook moet het duidelijk zijn voor de betrokkenen (dat kan bijvoorbeeld worden opgenomen in de privacyverklaring, lees ook onderdeel 'Transparantie').

Case: Facebook fan-page *(uitspraak Hof van Justitie 5 juni 2018)*
De paginabeheerder van een Facebook fan-pagina is samen met Facebook 'gezamenlijk verwerkingsverantwoordelijke' voor het verwerken van persoonsgegevens middels de Fanpagina. Omdat de paginabeheerder bepaalt (of eigenlijk invloed heeft op) welke gegevens Facebook verwerkt, is de beheerder medeverantwoordelijk. Dat de paginabeheerder alleen geanonimiseerde statistieken ontvangt is daarbij niet relevant.

Let op! Gezamenlijke verantwoordelijkheid betekent niet automatisch een gelijkwaardige verantwoordelijkheid van partijen. De mate van verantwoordelijkheid kan in de diverse fasen van de verwerking verschillen en hangt af van de invloed die iemand daadwerkelijk kan uitoefenen. Het betekent

ook niet dat beide partijen in principe toegang hebben tot alle persoonsgegevens. Het kan dus zo zijn dat je gezamenlijk verantwoordelijk bent voor een verwerking, ook al heb je geen toegang tot (alle) persoonsgegevens.

5.2. De verwerker

Veel organisaties besteden werk uit aan externe dienstverleners. Meestal gaat het dan om administratieve of IT-diensten. Hierbij worden eigenlijk altijd wel op de een of andere manier persoonsgegevens verwerkt. De organisatie bepaalt als verantwoordelijke in dat geval nog steeds het doel van de verwerking van die persoonsgegevens, maar de dienstverlener verzorgt (een deel van) de feitelijke uitvoering. Deze partij handelt in opdracht van de verantwoordelijke, zonder dat het onder diens rechtstreekse gezag staat. Zo'n dienstverlener heet in privacytermen een 'verwerker'.

Voorbeeld: verwerker
Een 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 de sportbond (en niet voor eigen doeleinden van de ICT-dienstverlener). De ICT-dienstverlener is een verwerker en de sportbond is verwerkingsverantwoordelijke voor de verwerkingen die plaatsvinden via het ledenbeheersysteem. De sportbond moet een verwerkersovereenkomst sluiten met de ICT-dienstverlener (lees ook onderdeel 'Derde partijen').

Externe links	Uitleg
Officiële fan-page uitspraak	Hier lees je de officiële fan-page uitspraak van het Hof van Justitie.

6. De basisregels bij het verwerken van persoonsgegevens

De kans is groot dat je als sportclub persoonsgegevens verwerkt. Door hier op een juiste manier mee om te gaan, help je de privacy van jouw leden en anderen te beschermen. Als je met persoonsgegevens aan de slag gaat, loop dan altijd even de basisregels na en stel jezelf de volgende vragen.

6.1. Voor welk doel gebruik ik de persoonsgegevens?

Persoonsgegevens mogen alleen worden verwerkt voor duidelijk vooraf omschreven doelen. Bedenk dus altijd vooraf wat je doel is en welke persoonsgegevens je daarvoor nodig hebt. Voor het versturen van een nieuwsbrief heb je bijvoorbeeld alleen een naam en emailadres nodig. Voor het uitvoeren van de salarisadministratie van medewerkers en vrijwilligers heb je bankrekeningnummers nodig.

Wat moet ik doen als mijn doel na verloop van tijd verandert (doelbinding)?

Het kan zijn dat je persoonsgegevens wil gebruiken voor een ander doel dan waarvoor je deze in eerste instantie hebt verzameld. In sommige gevallen mag dat. Je moet dan wel eerst beoordelen of je nieuwe doel verenigbaar is met het oorspronkelijke doel. Om dit te beoordelen kun je een verenigbaarheidstoets uitvoeren. Daartoe dien je de volgende vragen te beantwoorden:

- **Verband:** is er enige samenhang tussen de twee doelen? Hoe dichter de doelen bij elkaar liggen, hoe eerder de verdere verwerking van persoonsgegevens verenigbaar is.
- **Context:** kan een betrokkene logischerwijs verwachten dat zijn/haar persoonsgegevens ook worden gebruikt voor het nieuwe doel? Een nieuwe verwerking die leidt tot een onwenselijk verrassingseffect is waarschijnlijk niet verenigbaar.
- **Type persoonsgegevens:** zijn de gegevens niet te gevoelig? Gevoelige of bijzondere persoonsgegevens mogen minder snel voor andere doelen worden gebruikt.
- **Gevolgen:** kan worden uitgesloten dat er nadelige gevolgen zijn voor de betrokkene als de persoonsgegevens worden gebruikt voor het nieuwe doel? Als er nadelige gevolgen te bedenken zijn, is de verdere verwerking waarschijnlijk niet verenigbaar.
- **Beveiligingsmaatregelen:** zijn de persoonsgegevens voldoende beveiligd? Je mag persoonsgegevens eerder voor een nieuw doel gebruiken als je ze hebt gespseudonimiseerd of maatregelen hebt genomen om de persoonsgegevens te versleutelen.

Is het antwoord op bovenstaande vragen veelal ‘ja’, dan kun je vermoeden dat je nieuwe doel verenigbaar is met het oorspronkelijke doel. In dat geval is er geen andere grondslag nodig dan de grondslag waarop de oorspronkelijke verwerking is gebaseerd.

Let op! Je moet de betrokkene voordat de gegevens voor het nieuwe doel worden verwerkt, hierover wel informeren (zie onderdeel ‘Transparantie’).

Is het antwoord op bovenstaande vragen veelal ‘nee’, dan is het nieuwe doel zeer waarschijnlijk niet verenigbaar met het oorspronkelijke doel. Je kunt dan beter kijken of er een nieuwe grondslag is waar je de gewijzigde gegevensverwerking op kunt baseren (zie onderdeel ‘Rechtmatigheid’).

Voorbeeld: sollicitatie oud-deelnemer
Stel je voor dat iemand solliciteert voor een trainersfunctie bij jouw sportbond. Wellicht ken je deze persoon al, omdat hij het jaar daarvoor deelnam aan een opleidingsprogramma van diezelfde bond. Het kan in deze 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 moet je hier voorzichtig mee zijn. De sollicitant realiseert zich wellicht niet dat jij als potentiële werkgever al over enige 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.

6.2. Heb ik een wettelijke grondslag voor de verwerking (rechtmatigheid)?

De verwerking van persoonsgegevens is alleen gerechtvaardigd als het doel van de verwerking kan worden gebaseerd op één van de zes grondslagen die zijn opgesomd in de wet. Bedenk vooraf of je een grondslag hebt voor het verwerken van persoonsgegevens.

Er zijn zes grondslagen:

- De betrokkene geeft **toestemming** voor de verwerking van zijn persoonsgegevens;
- De verwerking is noodzakelijk in verband met de **uitvoering van een overeenkomst** met de betrokkene, of om op verzoek van de betrokkene voor het sluiten van de overeenkomst maatregelen te nemen;
- De verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**;
- De verwerking is noodzakelijk om een **vitaal belang van de betrokkene te beschermen**;
- De verwerking is noodzakelijk om een **publiekrechtelijke taak te vervullen**;
- De verwerking is noodzakelijk om een **gerechtvaardigd belang te behartigen**.

Al deze grondslagen, behalve toestemming, zijn ‘noodzakelijkheidsgrondslagen’. Dat houdt in dat de verwerking alleen rechtmatig is als het daadwerkelijk nodig is voor het in de grondslag genoemde doel.

Ook als je beschikt over een geldige grondslag om persoonsgegevens te verwerken, moet je goed blijven opletten dat je alleen 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. Meer hierover lees je in onderdeel ‘Data minimalisatie’.

In de praktijk baseer je een verwerking meestal op (1) de uitvoering van een overeenkomst, (2) een wettelijke verplichting, (3) een gerechtvaardigd belang, of (4) toestemming. We lichten deze vier grondslagen daarom hierna verder toe. Qua volgorde hanteren we: meest gebruikt – minst gebruikt.

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 gegeven toestemming altijd (voor de toekomst) kan worden ingetrokken. Kun je dus hard maken dat het verwerken van persoonsgegevens noodzakelijk is ten behoeve van één van de andere doelen, dan kun je het vragen van toestemming (als grondslag) beter vermijden.

6.2.1. Grondslag: uitvoering overeenkomst

Als verwerkingsverantwoordelijke mag je persoonsgegevens verwerken als dat nodig is voor de uitvoering van een overeenkomst. Het kan ook gebeuren dat het verwerken van persoonsgegevens nodig is om voorafgaand aan het sluiten van een overeenkomst – op verzoek van betrokkene – maatregelen te nemen. Denk aan een betrokkene die contactgegevens achterlaat om in contact te komen over aangeboden trainingen door sportvereniging 't AVG'tje. Om in contact te treden zal de sportvereniging de contactgegevens moeten verwerken voordat sprake is van een overeenkomst. Een ander voorbeeld is een sollicitatieprocedure die voorafgaand aan het sluiten van een arbeidsovereenkomst wordt gevoerd.

De overeenkomst zelf mag overigens niet gericht zijn op de verwerking van persoonsgegevens. De verwerking dient een uitvloeisel te zijn van de gemaakte afspraken in de overeenkomst.

Toepassing in de sport:

- Verwerkingen noodzakelijk voor de uitvoering van de arbeidsovereenkomst;
- Verwerkingen noodzakelijk voor de uitvoering van de vrijwilligersovereenkomst;
- Verwerkingen noodzakelijk voor de uitvoering van de topsportovereenkomst;
- Verwerkingen noodzakelijk voor de uitvoering van het lidmaatschap.

Let op! Een lidmaatschap van een sportvereniging is feitelijk geen overeenkomst. Het lidmaatschap heeft echter zoveel gelijkenissen met een overeenkomst dat de verwerkingen die nodig zijn voor het uitvoeren van het lidmaatschap geschaard kunnen worden onder de grondslag overeenkomst. Immers, doordat iemand zich aanmeldt als lid gaat deze persoon akkoord met bepaalde verplichtingen die voortvloeien uit statuten en reglementen en verkrijgt het lid ook de daaraan verbonden rechten. Bijvoorbeeld, als lid mag je op trainingen komen, maar moet je eens in de zoveel tijd ook bardiensten uitvoeren. Deze combinatie van rechten en verplichtingen heeft veel gelijkenissen met een overeenkomst.

Let op! Het is belangrijk het begrip **'noodzakelijk'** strikt te interpreteren. Als de overeenkomst kan worden uitgevoerd zonder de verwerking van bepaalde persoonsgegevens, dan kun je geen gebruik maken van deze grondslag. Dus, als het verwerken van persoonsgegevens enkel handig is, maar **niet noodzakelijk**, dan dien je daarvoor een andere grondslag te hebben (veelal toestemming).

Let op! Het simpele feit dat een verwerking is gedekt in een overeenkomst, betekent niet automatisch dat de verwerking noodzakelijk is voor de uitvoering van de overeenkomst. Zelfs wanneer de specifieke verwerking wordt genoemd in de overeenkomst, betekent dat niet dat het noodzakelijk is om de overeenkomst tot stand te laten komen.

Let op! Je mag als verwerkingsverantwoordelijke deze grondslag alleen gebruiken als de betrokkene zelf partij is bij de overeenkomst. Als verwerkingsverantwoordelijke hoef je niet zelf partij te zijn bij de overeenkomst.

6.2.2. Grondslag: wettelijke verplichting

Als verwerkingsverantwoordelijke mag je persoonsgegevens verwerken als dat nodig is om te voldoen aan een wettelijke verplichting. Je kunt je hier alleen op baseren als het niet mogelijk is om aan je wettelijke plicht te voldoen zonder daarbij persoonsgegevens te verwerken.

Je kunt deze grondslag alleen gebruiken als de wettelijke plicht te vinden is in recht van de Europese Unie of recht van Nederland en als je als verwerkingsverantwoordelijk daadwerkelijk onderworpen bent aan dit recht.

Voorbeeld: kopie of scan van identiteitsbewijs
't AVG'tje is volgens de Wet op de loonbelasting verplicht een kopie of scan van het identiteitsbewijs van haar personeel op te nemen in de loonadministratie.

6.2.3. 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?
Soms is het voor het uitvoeren van bepaalde verwerkingen niet mogelijk om je te baseren op één van de overige grondslagen. Je vindt het als verwerkingsverantwoordelijke echter wel nodig om de persoonsgegevens te verwerken om op die manier de belangen van de betrokkene adequaat te kunnen behartigen. Alleen vaststellen dat je een belang hebt is niet voldoende voor de conclusie dat er sprake is van een gerechtvaardigd belang. Tegenover dat belang staat namelijk altijd het privacybelang van de betrokkene. Hoe groter dat privacybelang van die betrokkene is, des te relevanter wordt de vraag of jouw belang daar tegenop weegt.

Toetsingskader: is het belang voldoende gerechtvaardigd?
Er is in deze situatie dus sprake van een botsing van rechtsbelangen: het recht van de betrokkene versus het recht van jou als verwerkingsverantwoordelijke. Je moet als verwerkingsverantwoordelijke deze rechtsbelangen tegen elkaar wegen om te beoordelen welk belang zwaarder weegt (en of de verwerking van persoonsgegevens op basis van deze grondslag dus gerechtvaardigd is).
Het hoeft bij de grondslag gerechtvaardigd belang 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: publicatie wanbetalers
Het is voor een sportvereniging 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.

Een verwerking op basis van deze grondslag is alleen rechtmatig als aan de volgende drie cumulatieve voorwaarden is voldaan:

- De behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke; en
- De noodzaak van de verwerking van persoonsgegevens voor de behartiging van het belang; en
- De voorwaarde dat het belang van de verwerkingsverantwoordelijke zwaarder weegt dan de privacybelangen van de betrokkene, met name als de betrokkene een kind is.

Bovengenoemde betekent in de praktijk dat je altijd eerst een belangenafweging moet maken voordat je gebruik kunt maken van deze grondslag. Enkel vaststellen dat je een gerechtvaardigd belang hebt, is niet voldoende. Zie het template 'Toetsingskader gerechtvaardigd belang'. Het template geeft een toelichting op

de voorwaarden waar je aan moet voldoen en het ingevulde document kun je meteen gebruiken ter verantwoording (documentatie).

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

Let op! Wil je de grondslag gerechtvaardigd belang gebruiken voor commerciële doeleinden? Lees dan eerst het onderdeel 'Marketing'.

Let op! Houd altijd rekening met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke.

Toepassing in de sport:

- Verstrekking contactgegevens: een sportorganisatie mag contactgegevens van deelnemers verstrekken aan de trainer als dat nodig is om de deelnemers te kunnen contacteren in het kader van de training.
- Publicatie persoonlijk e-mailadres: als een functionaris van een sportorganisatie gebruikmaakt van een persoonlijk e-mailadres (in plaats van een 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 sportorganisatie).
- Monitoring ICT-gebruik: werkgevers mogen tot op zekere hoogte het ICT-gebruik van hun werknemers volgen om misbruik van het systeem te voorkomen (lees ook onderdeel 'Personeel').
- Antecedentenonderzoek: voor sommige functies heeft een werkgever een legitieme reden om een kandidaat te vragen om een Verklaring Omtrent Gedrag (VOG).

6.2.4. Grondslag: toestemming

Persoonsgegevens mogen ook worden verwerkt als de betrokkene daar voorafgaand aan de verwerking toestemming voor heeft gegeven.

Eisen toestemming

Als je besluit om toestemming als grondslag te gebruiken, dan moet die toestemming wel voldoen aan een aantal eisen.

(1) Geïnformeerd

Als je toestemming als grondslag gebruikt, moet voldoende duidelijk zijn waarvoor je toestemming vraagt. Gebruik dan ook duidelijke en eenvoudige taal. Zorg ervoor dat je voldoende informatie geeft, zodat de persoon aan wie je toestemming vraagt een weloverwogen besluit kan nemen (en later niet voor verrassingen komt te staan). Je hoeft daarbij niet te vervallen in onnodige details: teveel informatie is immers ook verwarrend. Vermeld in ieder geval:

- De identiteit van je sportorganisatie;
- De redenen waarom je persoonsgegevens gaat verwerken (doel);
- Welke persoonsgegevens je daarvoor nodig hebt.

Verdere gedetailleerde informatie kan je meestal beter opnemen in een privacyverklaring, die je op grond van de informatieplicht beschikbaar stelt (lees hiervoor onderdeel 'Transparantie').

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

(2) Specifiek
Zorg ervoor dat de toestemming specifiek op één doel is gericht. Als je meerdere doelen hebt dan moet je de betrokkene hierover informeren en voor ieder doel apart om toestemming vragen. Je mag een betrokkene dus niet in één verklaring akkoord laten gaan met (1) publicatie op de website en (2) het gebruik van gegevens voor de nieuwsbrief. Hiervoor zou je twee toestemmingsteksten op kunnen stellen.

(3) Ondubbelzinnig
Je hebt ondubbelzinnige instemming nodig van de betrokkene: er mag geen twijfel bestaan over de wil van de persoon. Er moet een actieve handeling zijn waarmee betrokkene zijn of haar wil tot uitdrukking brengt. Het simpelweg afleiden van toestemming omdat iemand niet handelt of niet protesteert, is niet toegestaan. Je mag niet uitgaan van een stilzwijgende toestemming.
Vraag bij voorkeur om schriftelijke toestemming en documenteer de verkregen toestemming zorgvuldig. Als er later discussie ontstaat over de vraag of een betrokkene toestemming heeft gegeven, rust de bewijslast op jou als verwerkingsverantwoordelijke. 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.

Voorbeeld: automatisch ingevulde vinkjes
Vraag je op digitale wijze toestemming waarbij de betrokkene een hokje moet aanvinken voor het geven van zijn toestemming? Zorg er dan voor dat het vakje niet al bij voorbaat is aangevinkt (opt-out), maar zorg dat de betrokkene dat zelf moet doen (opt-in). Wanneer het vakje namelijk al is aangevinkt is het niet duidelijk wat de echte wil van de betrokkene is (hij/zij kan het vakje over het hoofd hebben gezien).

(4) Vrije wil
Toestemming moet zonder aanwezigheid van dwang zijn gegeven. Met andere woorden: de betrokkene moet daadwerkelijk een keuze hebben (ook om te weigeren). Aan het weigeren van de toestemming mogen geen negatieve consequenties zijn verbonden.

Er zijn een aantal verhoudingen waarbij het vermoeden bestaat dat die toestemming niet uit vrije wil kan worden gegeven vanwege de afhankelijke positie van de betrokkene. Het gaat dan om een ongelijke machtsverhouding, zoals: de werkgever-werknemer relatie, de overheid-burger relatie en meer specifiek voor de sport, de coach-topsporter relatie. Het weigeren van toestemming kan namelijk potentiële negatieve gevolgen met zich mee brengen (zoals het niet krijgen van een promotie, het niet krijgen van een basisplaats, etc.).

Voorbeeld: sporter die mogelijk een A-status krijgt
Sara weet dat ze mogelijk in aanmerking komt voor een A-status. Haar coach vraagt haar om toestemming voor toegang tot de applicatie waarin zij haar menstruatiecyclus en symptomen bijhoudt. Sara voelt zich daar eigenlijk niet zo prettig bij, maar is bang dat het niet geven van toestemming het verkrijgen van een A-status negatief kan beïnvloeden. Sara besluit uit angst om toch haar toestemming te geven.

Bovengenoemd voorbeeld illustreert dat een betrokkene kan besluiten om toestemming te geven uit angst voor negatieve gevolgen. De vraag is dan: is dat uit vrije wil? Het antwoord is vaak nee. Bedenk dus vooraf goed of sprake is van een ongelijke machtsverhouding en of er eventueel (directe of indirecte) negatieve gevolgen zijn verbonden aan het geven of weigeren van toestemming.

Ook in andere situaties komt het 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. Als je op die manier om toestemming vraagt dan is die in principe niet uit vrije wil gegeven en daarmee ongeldig. Je mag dan ook geen persoonsgegevens verwerken op basis van deze grondslag.

Voorbeeld: instemmen via toepasselijke voorwaarden
Stel dat toeschouwers van een sportevenement mogelijk 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 kijken of er een andere grondslag is die je kunt gebruiken, zoals het gerechtvaardigd belang. Het uitzenden van een evenement kan 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. Zorg dan bijvoorbeeld voor een aankondiging van de live registratie op de ticket website en bij de ingang van het evenement.

Toestemming intrekken
Een betrokkene mag de verleende toestemming voor een verwerking op ieder moment intrekken. Vanaf het moment dat iemand de toestemming intrekt, mag je de persoonsgegevens niet meer gebruiken. Dit kan in de praktijk lastige gevolgen hebben. Wees ervan bewust dat voor verwerkingen waar je in de toekomst afhankelijk van bent de grondslag toestemming niet altijd handig is.
Je moet de betrokkene overigens op de hoogte stellen van zijn/haar recht om toestemming te allen tijde in te trekken. Let er ook op dat het intrekken van toestemming net zo gemakkelijk moet zijn als het geven ervan.

Toestemming van minderjarigen en/of via een derde
Is een betrokkene nog geen 16 jaar, dan mag de minderjarige betrokkene niet zelfstandig toestemming geven. Vraag in dat geval toestemming aan de wettelijk vertegenwoordiger, zoals een ouder of voogd.

Soms verkrijg je persoonsgegevens niet direct van de 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 krijgt de verkregen toestemming kan aantonen.

Let op! Een groot misverstand is dat je veel privacyregels kunt ontlopen zolang je de betrokkene maar om toestemming vraagt. Die gedachte is onjuist. Ook na het verkrijgen van toestemming moet je gewoon de privacyregels naleven. Denk bijvoorbeeld aan de informatieplicht, beveiliging en bewaartermijnen. Het enige dat je via toestemming verkrijgt is het recht (lees: een geldige grondslag) om überhaupt bepaalde persoonsgegevens te mogen verwerken.

Toepassing in de sport:

- Commerciële e-mails: 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 (meer hierover lees je in het onderdeel '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 regels omtrent cookies (meer hierover lees je in het onderdeel 'Marketing').
- Online publicatie: voor het online publiceren van persoonsgegevens (bijvoorbeeld deelnemerslijsten of contactgegevens van leden) heb je in veel gevallen toestemming nodig van de betrokkene. Vraag jezelf overigens eerst af of het noodzakelijk is om gegevens online te publiceren.

Template(s)	Uitleg
Toetsingskader gerechtvaardigd belang	Dit toetsingskader is te gebruiken als invuldocument voor jou als verwerkingsverantwoordelijke om te beoordelen of je verwerking rechtmatig is.

6.3. Heb ik vooraf helder geïnformeerd over het doel van de verwerking (transparantie)?

De verwerking van persoonsgegevens moet transparant zijn. Zorg dat je altijd voordat je de gegevens verzamelt, de betrokkene niet alleen informeert over welke gegevens 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 niet alleen een kwestie van de wet naleven, maar ook een mooie kans om te demonstreren dat jouw sportorganisatie goed omgaat met privacygevoelige informatie.

Toepassing in de sport:

- Topsporters moeten begrijpen hoe zij door de sportbond of vereniging worden gemonitord. Leg dus uit dat via een horloge hartslag, stappen en bloeddruk kan worden doorgegeven en dat die gegevens worden verwerkt in een database. Geef aan dat de voedingsapp die zij dagelijks gebruiken, hun eetpatroon doorgeeft aan de diëtist;
- Medewerkers moeten weten of hun computer- en telefoongebruik kan worden gecontroleerd en zo ja, waarvoor;
- Scheidsrechters en deelnemers aan wedstrijden moeten weten of hun persoonlijke e-mail- en telefoongegevens voor anderen zichtbaar zijn en zo ja, voor wie dan;
- Bezoekers en deelnemers van wedstrijden en evenementen moeten weten of zij kunnen worden gefilmd en/of gefotografeerd, en hoe deze beelden gebruikt kunnen worden;

6.3.1. Wanneer moet ik de betrokkene informeren?

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 daarover zo snel als mogelijk, maar in ieder geval binnen een maand

nadat je de gegevens hebt verkregen. Je hoeft de betrokkene niet te informeren als de betrokkene al over deze informatie beschikt.

6.3.2. Welke informatie moet ik verstrekken?

Als je de gegevens direct van de betrokkene verkrijgt, dan moet je tenminste de volgende informatie verstrekken:

- Je eigen identiteit (naam, vestiging, contactgegevens);
- De gegevens (of categorieën van gegevens) die je verzamelt;
- De doelen waarvoor je de gegevens verwerkt;
- De grondslag waar je de gegevens op baseert;
    - Als je gebruik maakt van de grondslag 'gerechtvaardigd belang' dan dien je dat belang toe te lichten;
    - Als je gebruik maakt van de grondslag 'toestemming' dan dien je ook aan te geven dat de betrokkene die toestemming altijd weer kan intrekken (en hoe hij/zij dat kan doen);
    - Als je gebruik maakt van de grondslag 'wettelijke plicht' of 'overeenkomst' dan dien je ook aan te geven of de betrokkene verplicht is die gegevens te verstrekken en wat het gevolg is als de betrokkene die gegevens niet verstrekt.
- De bewaartermijn (of in ieder geval de criteria voor het bepalen van de bewaartermijn);
- Indien sprake is van ontvangers: de ontvangers (of categorieën van ontvangers) van de gegevens;
- Indien sprake is van verstrekking aan derde landen: de passende waarborgen;
- Indien sprake is van geautomatiseerde besluitvorming: informatie over de logica ervan, het belang van de verwerking en de verwachte gevolgen voor de betrokkene van deze besluitvorming;
- De rechten van de betrokkene;
- Het recht om een klacht in te dienen bij de AP;
- Indien je een Functionaris Gegevensbescherming (FG) hebt aangesteld: de contactgegevens van deze persoon.

Daarnaast moet je alle overige informatie verstrekken die nodig is om een transparante verwerking te kunnen waarborgen. Dat is erg situatie afhankelijk, je moet zelf bepalen welke informatie je aanvullend wilt opnemen.

Als je de gegevens verzamelt buiten de betrokkene om (je ontvangt ze via een derde), dan moet je dezelfde informatie verstrekken. Ook moet je daarbij aangeven van wie je de persoonsgegevens hebt gekregen (bijvoorbeeld: via een vriend/vriendin die jou heeft aangemeld voor de training).

Je ziet dat veel van de informatie die je moet verstrekken ook terugkomt in het onderdeel 'Basisregels'. Voordat je een duidelijk overzicht kunt maken van welke informatie je moet verstrekken, moet je eerst al die informatie voor jezelf helder hebben.

Tip: Wees altijd duidelijk. De betrokkene moet echt kunnen begrijpen wat er met zijn/haar persoonsgegevens gebeurt en 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.

Let op! Als je de persoonsgegevens voor andere doelen gaat verwerken (zie hiervoor het onderdeel 'Doelbinding'), dan moet je de betrokkene opnieuw informeren over dat nieuwe doel, tenzij de betrokkene hier al van op de hoogte is.

6.3.3. Hoe verstrek ik informatie aan de betrokkene (in welke vorm)?

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.

Privacyverklaring

In veel situaties is een privacyverklaring (of privacy statement) een geschikt middel om de betrokkene te informeren. Een privacyverklaring is meer dan een opsomming van de verplichte elementen. Een volledige privacyverklaring bevat concrete en duidelijke taal, sluit aan op het publiek en is eenvoudig te vinden. Zie het template 'Model privacyverklaring'. Dit document kun je als basis gebruiken en naar eigen wens aanpassen. In het template vind je terug welke informatie je in ieder geval moet opnemen.

Toepassing in de sport:

- **Personeel**: informatie over personeelszaken is voor werknemers meestal op een centrale plaats digitaal te vinden, bijvoorbeeld op het intranet van de sportorganisatie. Dat is ook een geschikte manier om werknemers te informeren over de omgang met persoonsgegevens. Werkt jouw sportorganisatie niet met een intranet? Dan zijn er wellicht papieren handleidingen/brochures waar je de informatie in kunt opnemen.
- **Websitebezoekers:** de informatie voor bezoekers van een website kun je uiteraard eenvoudig op diezelfde website plaatsen in een privacyverklaring. Zorg dat de privacyverklaring ofwel op dezelfde pagina staat, ofwel te bereiken is via een sub-pagina, bijvoorbeeld door het opnemen van een link onderaan de pagina (in de footer).
- **Webwinkel:** Wanneer je als sportvereniging of sportbond online merchandise aanbiedt via een webwinkel, dan moet je je klanten informeren. De informatie voor klanten in de webshop communiceer je tijdens het bestelproces in de vorm van een privacyverklaring. Maak je gebruik van een digitaal bestelformulier, wijs dan op de privacyverklaring *(*bijvoorbeeld door middel van de tekst *"lees hier meer over hoe wij omgaan met jouw persoonsgegevens")* en plaats een duidelijk zichtbare hyperlink, die opent in een apart venster.
- **Apps:** informatie voor app-gebruikers kun je communiceren door het opnemen van een privacyverklaring in de app. Zorg ervoor dat nieuwe gebruikers bij het eerste gebruik een 'pop-up' venster te zien krijgen of wijs op de privacyverklaring (en plaats wederom een duidelijk zichtbare hyperlink) wanneer betrokkene bijvoorbeeld een account moet aanmaken.
- **Lidmaatschap/evenementen/winacties/opleidingen:** de informatie voor deelnemers/leden communiceer je op het moment dat 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, vermeld dan dat er een privacyverklaring is opgesteld. Plaats een duidelijk zichtbare hyperlink naar de privacyverklaring, die opent in een apart venster. 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.

Let op! Als je een privacyverklaring wijzigt, zorg dan dat je dit duidelijk en vóóraf communiceert met betrokkene, vooral als het gaat om ingrijpende veranderingen. Op de website van jouw organisatie kun je bijvoorbeeld tijdelijk een pop-up plaatsen, met de mededeling dat de privacyverklaring is geüpdatet.

Let op! Een veel voorkomend misverstand is het 'afvinken' van het feit dat iemand akkoord gaat met, of kennis heeft genomen van, de privacyverklaring. Een betrokkene hoeft de privacyverklaring niet af te vinken of te accepteren. Vanuit je verantwoordingsplicht moet je natuurlijk wel kunnen aantonen dat je de

betrokkene op tijd en duidelijk hebt geïnformeerd, maar het volstaat als je kunt laten zien dat een verwijzing naar de privacyverklaring onderdeel is van je proces/flow.

Externe links	Uitleg
Richtsnoeren inzake transparantie	Hier vind je de Nederlandse vertaling van de guidelines transparantie. Deze guideline verduidelijkt het onderwerp transparantie/ informatieplicht.

Template(s)	Uitleg
Model privacyverklaring	Dit model biedt een uitgangspunt voor jou als verwerkingsverantwoordelijke die de betrokkene moet informeren over de verwerking met persoonsgegevens.

6.4. Gebruik alleen gegevens die noodzakelijk zijn (minimale gegevensverwerking)

Persoonsgegevens mogen enkel worden verwerkt als ze ook daadwerkelijk nodig zijn voor het behalen van je specifieke doel. Bedenk vooraf goed welke gegevens je minimaal nodig hebt om je dienst te kunnen leveren. Ook als je beschikt over een geldige grondslag om persoonsgegevens te verwerken, moet je goed blijven opletten dat je enkel gegevens gebruikt die noodzakelijk en voldoende relevant zijn voor het doel waarvoor je verwerkt.

Als je meer informatie wilt verzamelen dan nodig voor het leveren van de dienst, dan moet er een duidelijk doel en een grondslag voor zijn. Bijvoorbeeld, het bepalen van de demografische samenstelling van het ledenbestand (op basis van een gerechtvaardigd belang). Let op! Omdat je dat doel in principe kunt bereiken met geanonimiseerde gegevens mag je die gegevens niet op individueel niveau verwerken. Dat vereist dus een extra handeling, namelijk het anonimiseren van deze data zodat ze niet meer herleidbaar zijn tot een individueel persoon.

Tip: Verzamel geen gegevens die niet nodig zijn voor het leveren van de dienst. Pas je inschrijfformulieren hierop aan en gebruik bij voorkeur geen optionele velden.

Voorbeeld: inschrijfformulier training
Als een sportvereniging een training wil organiseren (= doel) dan is het bijvoorbeeld relevant om met iemand te kunnen communiceren over de training (e-mailadres of telefoonnummer). Als je achteraf een certificaat toestuurt dan heb je ook iemands adresgegevens nodig. Vaak wordt er via inschrijfformulieren echter meer informatie verzameld dan noodzakelijk is, namelijk om het individuele sporterprofiel te verrijken/of om de gegevens te gebruiken voor andere doeleinden die niets te maken hebben met de training. Deze velden zijn niet noodzakelijk voor het bereiken van je doel en kun je beter verwijderen. Wil je toch meer informatie opvragen, dan kun je ervoor kiezen om deze velden als ‘optioneel’ mee te nemen met daarbij bijvoorbeeld een informatiebutton, waarin je uitlegt wat je met die gegevens doet. Zorg ervoor dat duidelijk is voor de betrokkene dat deze velden optioneel zijn.

Let op! Gegevens verzamelen omdat je ‘er mogelijk in de toekomst iets aan hebt’ is niet toegestaan.

6.5. Bewaar persoonsgegevens niet langer dan nodig

Persoonsgegevens mogen niet langer worden bewaard dan nodig is om je doel te bereiken (inmiddels is het vast wel duidelijk: echt alles valt en staat met het doel dat je hebt). Bedenk daarom vooraf goed hoelang je de gegevens nodig hebt. Als de gegevens niet meer nodig zijn dan moet je ze anonimiseren (je kunt ze dan bijvoorbeeld nog gebruiken voor rapportage doeleinden) of verwijderen.
Het is vrij eenvoudig om veel informatie op te slaan en eindeloos te bewaren. 'Je weet maar nooit' is daarbij een bekend argument. Toch geldt voor het bewaren van persoonsgegevens juist het tegenovergestelde. Bewaar je persoonsgegevens (bewust of onbewust) te lang, dan kan dit in strijd zijn met de wet.

6.5.1. Welke bewaartermijn moet ik hanteren?

Dat is volledig afhankelijk van de situatie en dient per onderwerp en per afdeling beoordeeld te worden. Dat vereist dus dat je allereerst goed in kaart brengt welke persoonsgegevens in de gehele organisatie op welke wijze worden verwerkt.

(1) Geldig doel om te bewaren

Stel per organisatieonderdeel vast welk doel wordt gediend met het bewaren van deze persoonsgegevens. Dit kunnen meerdere doelen zijn. Zolang het doel nog actueel en relevant is, heb je meestal een legitieme reden om de gegevens te bewaren.

> **Voorbeeld: deelnemer**
> Een deelnemer neemt in 2022 deel aan een sportwedstrijd. Ter afhandeling van de inschrijving beschik je 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 dat je dit eventueel mag bewaren voor direct marketing (mits je aan de daarvoor geldende regels voldoet!), zodat je de persoon bijvoorbeeld kan benaderen voor de volgende editie. Sommige betaalgegevens moet je voor fiscale regels misschien nog enkele jaren bewaren. Je ziet dat er verschillende bewaartermijnen kunnen gelden rondom één deelnemer aan één evenement.

(2) Wettelijke plicht

Soms heb je zelf geen belang/reden om gegevens te bewaren, maar wel een wettelijke plicht. Zo zijn bepaalde persoonsgegevens relevant voor de Belastingdienst en moeten deze 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.

(3) Uitzondering: bewaren voor historische, statistische of wetenschappelijke doeleinden

Er geldt een belangrijke uitzondering op de bewaarbeperking als daarmee een historisch, statistisch of wetenschappelijk doel is gediend. Dat betekent dat je persoonsgegevens langer mag bewaren dan noodzakelijk is voor het doel waarvoor ze oorspronkelijk zijn verkregen of verwerkt, mits het bewaren dienstbaar is aan een specifiek historisch, statistisch of wetenschappelijk doel. Let op, je moet er dan wel voor 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 niet altijd duidelijk wat hier nu precies wel of niet onder valt. Om je op weg te helpen geven we twee 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.

Tip: Het is natuurlijk niet praktisch om steeds 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 bewaarbeleid vaak deels automatiseren via software die je nu al binnen de organisatie gebruikt. Bespreek deze mogelijkheden met je ICT-leverancier.

6.5.2. Vrijstellingsbesluit als hulpmiddel

Onder de oude wetgeving (Wet bescherming persoonsgegevens) moest je verwerkingen vooraf (via een formulier) aanmelden bij de AP. De verwerkingen die uitgezonderd werden van deze plicht stonden opgenomen in het zogeheten Vrijstellingsbesluit. Volgens dat besluit hoefde je bepaalde verwerkingen niet aan te melden, mits je de gegevens niet langer bewaarde dan een specifieke periode. Het Vrijstellingsbesluit gaf daarbij per onderwerp (bijvoorbeeld leden, personeel, ICT en beveiliging) concrete termijnen.

Onder de nieuwe wetgeving (AVG) is deze aanmeldplicht verdwenen. Toch biedt het Vrijstellingsbesluit nog steeds een handige maatstaf om te beslissen welke bewaartermijn je gebruikt. 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).

Let op! 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 (dat is overigens ook een vereiste uit de AVG).

Let op! Als de European Data Protection Board (EDPB) of de AP een zienswijze publiceert over bewaartermijnen dan zal dit voortaan het uitgangspunt zijn. Houd daarom de website van de AP in de gaten.

Externe links	Uitleg
Vrijstellingsbesluit	Hier vind je het Vrijstellingsbesluit met daarin per onderwerp concrete bewaartermijnen.

6.6. Beveiliging van persoonsgegevens

Persoonsgegevens moeten goed beveiligd zijn en vertrouwelijk blijven. Dat betekent dat je vooraf moet nadenken over het juiste beveiligingsniveau en dit ook moet toepassen. Als persoonlijke informatie spoorloos raakt, eindeloos bewaard blijft of zelfs wordt gestolen, dan kan dat vervelende gevolgen hebben voor de privacy van een betrokkene. Zo kan slechte beveiliging leiden tot een datalek en vervolgens tot misbruik van deze gegevens (denk aan identiteitsfraude).

Informatiebeveiliging is een complex onderwerp, waarvan privacy slechts één stukje van de puzzel vormt. Wij beperken ons in dit handboek daarom tot de wettelijke verplichting van de verantwoordelijke om 'passende' technische en organisatorische maatregelen te nemen om de gegevens te beschermen. Dit betekent dat je vooraf moet nadenken over de beveiliging van de persoonsgegevens die je verzamelt.

Tip: De online tool van ENISA kan je helpen bij het bepalen van een passend beveiligingsniveau voor persoonsgegevens. Zie hiervoor externe links.

6.6.1. Wat zijn nu precies 'passende' beveiligingsmaatregelen?

De wet geeft slechts een algemene omschrijving van de verplichting om persoonsgegevens te beschermen, namelijk dat de verwerkingsverantwoordelijke 'passende technische en organisatorische maatregelen' moet nemen om onrechtmatige verwerking te voorkomen. Dat betekent dat je in je keuze voor het nemen van beveiligingsmaatregelen, rekening houdt met het risico van de verwerking. Om dat te bepalen, voer je eerst een risicoanalyse uit. Je kijkt dan naar de risico's voor de betrokkene op het moment dat zijn/haar persoonsgegevens bijvoorbeeld op straat komen te liggen (lek van gegevens). Je kunt je vast wel voorstellen dat het lekken van enkel een emailadres minder negatieve gevolgen heeft voor een persoon dan het lekken van inkomensgegevens. Voor inkomensgegevens zou je dus zwaardere beveiligingsmaatregelen moeten treffen. Wanneer we het hebben over risico's moet je dus denken aan de mogelijke negatieve gevolgen, zoals: discriminatie, financiële verliezen, reputatieschade of andere economische of maatschappelijke nadelen.

In je risicoanalyse let je in ieder geval op:

- De gevoeligheid van de persoonsgegevens (ook gevoelige/bijzondere?);
- De betrokkenen van wie je gegevens verwerkt (ook minderjarigen?);
- De mogelijke negatieve gevolgen;
- De soort onrechtmatige verwerking die zich mogelijk kan voordoen (zoals verlies, vernietiging, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang van persoonsgegevens);

In de praktijk wordt bij het maken van een risicobeoordeling veel gebruik gemaakt van een Data Protection Impact Assessment (DPIA). Meer hierover lees je in het onderdeel 'Het uitvoeren van een DPIA'.

Let op! Als je gegevens verwerkt dan ben je ervoor verantwoordelijk om die op een goede manier te beveiligen. Doe je dat niet, dan kan dit leiden tot negatieve gevolgen voor betrokkenen, maar ook tot negatieve gevolgen voor je sportorganisatie. Zo kan een datalek al gauw leiden tot verlies van vertrouwen, reputatieschade, media aandacht en een mogelijke boete van de AP. Een gebrek aan kennis, uitbesteding van taken aan een derde of simpelweg een gebrek aan incidenten is geen excuus om informatiebeveiliging links te laten liggen.

Mogelijke maatregelen

Heb je de risico's in kaart gebracht, dan moet je overwegen welke maatregelen in verhouding staan tot de gegevens en de risico's voor de betrokkenen. Hoe groter het risico voor de betrokkene, hoe zwaarder de maatregelen die je moet nemen. In je overweging houd je ook rekening met:

- De uitvoeringskosten;

- De aard, omvang en context van de verwerking;
- De doeleinden;
- De ernst van de risico's;
- De waarschijnlijkheid dat de risico's zich zullen verwezenlijken.

Maatregelen zijn zowel technisch als organisatorisch. Zo moet je niet alleen moderne techniek gebruiken om persoonsgegevens te beveiligen, maar moet je ook kijken naar hoe de organisatie met persoonsgegevens omgaat. Het is van belang steeds de juiste combinatie te 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: technische maatregelen
Instellen van toegangscodes, gebruik van meerfactorauthenticatie (MFA), gebruik van HTTPS, toepassen van pseudonimisering en versleuteling van gegevens, het opzetten van een firewall, het installeren van een antivirus scanner, het opslaan van gegevens in beveiligde omgevingen, software-updates, procedures voor regelmatig testen, aanvalsdetectie, etc.

Voorbeeld: organisatorische maatregelen
Beperken van toegang tot gegevens (toegangsniveaus in een autorisatiebeleid), protocollen voor veiligheidsincidenten (incl. datalekken), geheimhoudingsverklaringen, aandacht voor training & privacy bewustzijn van medewerkers.

Let op! Maatregelen moeten gedurende de hele looptijd van de verwerking passend zijn. Dat betekent dat je dit periodiek moet beoordelen. Stel dat cybercriminelen nieuwe methoden ontwikkelen om beveiligingsmaatregelen te omzeilen, dan moet je je beveiliging hier natuurlijk op aanpassen. Voorkom dat je verouderde techniek gebruikt.

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

6.6.2. Hoe zit het met informatiebeveiliging bij leveranciers en partners?

Beveiligingsmaatregelen in jouw eigen sportorganisatie hebben weinig zin als de persoonsgegevens alsnog worden blootgesteld aan risico's bij leveranciers en partners. Is jouw leverancier of partner een verwerker? Dan ben je wettelijk verplicht om in de verwerkersovereenkomst afspraken te maken over het niveau van informatiebeveiliging (meer hierover lees je in onderdeel 'Derde partijen').

Externe links	Uitleg
Beleidsregels beveiliging van persoonsgegevens	Hier vind je de in 2013 gepubliceerde Beleidsregels beveiliging persoonsgegevens – uitgangspunten in de beleidsregels zijn nog steeds van toepassing. Het onderwerp informatiebeveiliging wordt hier helder uitgelegd.
Risk level tool ENISA	Hier vind je een online tool omtrent het passend beveiligen van persoonsgegevens. Het is een tool van European Network and Information Security Agency (ENISA).

Factsheet Beveilig verbindingen van mailservers	Op deze webpagina van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid kun je de factsheet 'Beveilig verbindingen van mailservers' downloaden.
Factsheet TLS-interceptie	Op deze webpagina van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid kun je de factsheet 'TLS-interceptie' downloaden.
Fix je privacy	Op deze webpagina vind je diverse tips en adviezen over online veiligheid.
Laat je niet hack maken	Op deze webpagina lees je op een begrijpelijke manier hoe je jezelf beschermt tegen hackers.

6.7. Correcte en actuele persoonsgegevens

Persoonsgegevens die je verwerkt moeten juist zijn. Dat betekent dat je maatregelen moet nemen om ervoor te zorgen dat de gegevens die je verwerkt correct en actueel zijn. Als gegevens dat niet (meer) zijn, moet je ze updaten of verwijderen. Hiermee voorkom je dat je verkeerde conclusies trekt of dat je informatie naar bijvoorbeeld een verkeerd adres stuurt. Zo zorg je er ook voor dat je je systeem niet vervuilt met verkeerde informatie.

Tips:

- Het instellen van regels voor datavelden op een inschrijfformulier: zo moet een emailadres bijvoorbeeld een '@' omvatten om na het invullen van het formulier op 'verzenden' te kunnen klikken.
- Het regelmatig (bijvoorbeeld jaarlijks of eens per twee jaar) controleren van accountgegevens bijvoorbeeld door middel van een pop-up 'Zijn deze gegevens nog up-to-date? Ja/Nee, wijzig dan hier je gegevens'.

6.8. Het uitvoeren van een DPIA

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog privacy risico oplevert voor de betrokkene, dan ben je verplicht een gegevensbeschermingseffectbeoordeling uit te voeren. In de praktijk wordt dit vaak afgekort als DPIA (Data Protection Impact Assessment). Voordat je een verwerking start, moet je je afvragen of de verwerking waarschijnlijk een hoog risico inhoudt. Als dat het geval is, dien je voorafgaand aan die verwerking een DPIA te voltooien.

6.8.1. Wat is een DPIA?

Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.
Een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie een organisatie gegevens wil verwerken). Wat een hoog risico is, is niet altijd eenvoudig te bepalen. Verwerkingen die ogenschijnlijk onschuldig zijn, kunnen soms wel degelijk een negatieve impact hebben.

De Autoriteit Persoonsgegevens (AP) heeft een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waarvoor een DPIA nodig is. Deze lijst is afgestemd met de andere privacytoezichthouders in de Europese Unie (EU) (zie externe links).

Als het je niet (voldoende) lukt om de privacyrisico's te beperken (door maatregelen te nemen) dan moet je met de AP overleggen voordat je de verwerking start. Met andere woorden, je bent dan verplicht tot voorafgaande raadpleging. De AP beoordeelt in dat geval de aanvraag en deelt uiteindelijk de uitkomst per

brief (daarin kan een advies staan hoe je de risico's eventueel zou kunnen beperken of om helemaal niet te starten met de verwerking). Het aanvraagformulier kun je downloaden op de website (zie externe links).

Er zijn geen richtlijnen voor het uitvoeren van de DPIA. Je kunt dit zelf doen (en een template op internet opzoeken) of een externe partij inhuren om deze uit te voeren. De vorm is eigenlijk niet belangrijk (Word, Powerpoint, Excel) als je de inhoud maar compleet hebt. In externe links staat een link naar het beschikbare model van NOREA (de beroepsorganisatie van IT auditors). Dit document wordt in Nederland veel toegepast en is een uitgebreid en begrijpelijk instrument om vorm te geven aan de DPIA.

Toepassing in de sport:
In de volgende gevallen is het uitvoeren van een DPIA sowieso vereist:

- Structureel gebruik van persoonsgegevens van (minderjarige) sporters voor marketing doeleinden;
- Verwerken van persoonsgegevens voor het tegengaan van matchfixing;
- Gegevensuitwisseling met jeugdzorg en/of maatschappelijk werk om sociale problematiek of risicojongeren te signaleren;

Externe links	Uitleg
Guideline DPIA	Hier download je de guideline over DPIA's die de European Data Protection Board heeft gepubliceerd. Deze guideline verduidelijkt het een en ander rondom het uitvoeren van DPIA's en geeft criteria voor de beoordeling van een waarschijnlijk hoog risico.
Richtsnoeren DPIA	Hier vind je de Nederlandse vertaling van de guideline DPIA's. Deze guideline verduidelijkt het een en ander rondom het uitvoeren van DPIA's en wanneer een verwerking waarschijnlijk een 'hoog risico' inhoudt.
Verplichte DPIA-lijst	Hier vind je het besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een DPIA verplicht is, opgesteld door de AP.
Handreikingen NOREA	Hier vind je een o.a. een Handreiking DPIA en een Raamwerk (invuldocument in Word). Het document bevat een vragenlijst die je helpt om stapsgewijs de privacyrisico's in kaart te brengen.
Model DPIA Rijksoverheid	Hier kun je het DPIA model van de Rijksdienst downloaden.
DPIA Tool	Hier vind je een tool voor het uitvoeren van DPIA's – aangeboden door de Franse toezichthouder.
Voorafgaande raadpleging	Hier vind je alle informatie omtrent voorafgaande raadpleging (lees onderdeel 'Wat moet ik verder nog weten').
Website AP	Op deze webpagina van de AP lees je meer informatie over het uitvoeren van een DPIA en vind je een aantal checklists.

6.9. Internationale doorgifte van persoonsgegevens

In de praktijk worden er continu persoonsgegevens doorgegeven naar landen/organisaties buiten de Europese Unie. Denk aan de opslag van persoonsgegevens op servers van Amerikaanse partijen of het delen van gegevens met niet Europese aanbieders van meetapparatuur/sensoren. De AVG stelt voorwaarden aan deze internationale doorgifte.

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/MailChimp/SurveyMonkey). Je spreekt dan over de cloud, wat meestal betekent dat data (waaronder persoonsgegevens) terecht komt op servers van externe leveranciers. Die servers staan vaak in de VS. In dat geval zijn de regels voor doorgifte van toepassing, zodat je bijzondere maatregelen moet treffen.

6.9.1. Wanneer is sprake van internationale doorgifte?

De EU bestaat anno 2022 uit 27 lidstaten. Er zijn enkele landen die niet binnen de EU vallen, maar waarvoor wel dezelfde privacyregels gelden, namelijk Liechtenstein, Noorwegen en IJsland. Samen met de Europese lidstaten vormen deze landen de Europese Economische Ruimte (EER). Binnen deze ruimte mogen persoonsgegevens worden doorgegeven en verwerkt zonder extra maatregelen. Let dus goed op waar het bedrijf waar je mee samenwerkt, is gevestigd en waar hun servers staan. Wanneer buiten de EER persoonsgegevens worden doorgegeven en/of verwerkt, is sprake van internationale doorgifte.

6.9.2. Wat moet ik doen als er sprake is van internationale doorgifte?

Je mag persoonsgegevens doorgeven naar organisaties in derde landen als dat land een passend beschermingsniveau biedt. Dat is het geval als de organisatie gevestigd is in een land waarvoor een adequaatheidsbesluit geldt (zie externe links voor een lijst met landen).
Als het land niet op deze adequaatheidslijst staat, dan dien je extra maatregelen te treffen om alsnog een minimaal beschermingsniveau te kunnen bieden. Daarvoor kun je gebruik maken van standaard contractbepalingen, wellicht beter bekend onder de Engelse term: Standard Contractual Clauses (SCC's). Dit is een modelcontract dat kan worden gesloten tussen de sportorganisatie (veelal de exporterende partij) en de importerende partij, waarin de aanvullende waarborgen zijn opgenomen. Zie externe links voor de modelcontracten. We adviseren je om ook het onderdeel 'Waar moet ik op letten bij het sluiten van deze SCC's' goed door te nemen.

Andere opties om passende waarborgen te kunnen bieden, is door gebruik te maken van goedgekeurde gedragscodes of via een certificeringsmechanisme. Ondernemingen in een concernverband kunnen ook nog bindende bedrijfsvoorschriften vaststellen. Deze drie opties lichten we hier niet verder toe, omdat dit in de sportcontext veelal niet van toepassing is.

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

Let op! Voor doorgifte van persoonsgegevens naar de Verenigde Staten kon je voorheen gebruik maken van het zogenoemde EU-VS Privacy Shield. Deze is ongeldig verklaard in de Schrems-II uitspraak (zie case). Het Privacy Shield mag je dus niet meer gebruiken. Dat betekent dat je in veel gevallen een modelcontract moet gebruiken voor doorgifte naar de VS.

Case: Schrems-II *(uitspraak Hof van Justitie 16 juli 2020)*
Persoonsgegevens van Europese personen mogen niet zomaar in de VS worden verwerkt, omdat de VS de privacy-rechten van Europeanen niet voldoende beschermt. Waarom niet? Ten eerste, omdat EU-burgers geen mogelijkheid hebben om naar de rechter te stappen als zij van mening zijn dat hun gegevens onrechtmatig door de overheid worden verwerkt. Ten tweede blijkt dat de veiligheidsdiensten in de VS erg ruime toegang hebben tot alle gegevens.

Let op! Het EC heeft voor het Verenigd Koninkrijk (na het verlaten van de EU) een adequaatheidsbesluit genomen. Dat betekent dat je vrij gegevens kunt uitwisselen met het VK en je daarbij geen extra maatregelen hoeft te nemen.

6.9.3. Waar moet ik op letten bij het sluiten van deze SCC's?

Zoals je hierboven al hebt kunnen lezen, zijn SCC's standaard afspraken die in bepaalde gevallen gemaakt moeten worden als er sprake is van internationale doorgifte. Enkel het sluiten van SCC's is echter niet voldoende. Je dient namelijk te beoordelen of de wetgeving in het ontvangende land eigenlijk wel het overeengekomen beschermingsniveau kan bieden. Immers: je kunt wel standaardafspraken maken, maar als deze afspraken niet kunnen worden nagekomen vanwege wetgeving, dan ben je in feite weer terug bij af. Een dergelijke beoordeling noemen we ook wel een Transfer Risk Assessment. Raadpleeg voor (ondersteuning bij) het uitvoeren hiervan een jurist.

Wil je meer weten, lees dan de richtsnoeren van de EDPB, waarvan we hierna de externe link hebben opgenomen.

Externe links	Uitleg
Lijst adequaatheidsbesluit	Hier vind je een overzicht van de landen waarvoor een adequaatheidsbesluit geldt.
SCC's	Hier download je de SCC's templates.
Uitspraak Schrems II	Hier vind je de officiële uitspraak van het Schrems II arrest.
Artikel 49 AVG Richtsnoeren	In deze richtsnoeren legt de EDPB uit welke uitzonderingen mogelijk zijn en hoe je die moet toepassen.

6.10. Rechten van betrokkenen

Betrokkenen hebben verschillende rechten om controle te houden over het verwerken van hun persoonsgegevens. We lichten hieronder toe met welke rechten van betrokkenen je in de praktijk te maken kunt krijgen (zie tabel).

Recht op?	Wat houdt het in voor de betrokkene?
Inzage	het recht een kopie te ontvangen van de persoonsgegevens die worden verwerkt.
Vergetelheid	het recht om 'vergeten' te worden.
Rectificatie	het recht persoonsgegevens te laten wijzigen/aanvullen.
Dataportabiliteit	het recht persoonsgegevens over te laten dragen aan een andere partij.
Beperking van de verwerking	het recht om minder persoonsgegevens te laten verwerken.
Menselijke blik bij besluiten	het recht op een menselijke blik bij besluiten (indien er sprake is van geautomatiseerde besluitvorming/profilering).
Bezwaar	het recht om bezwaar te maken tegen het verwerken van persoonsgegevens.

Let op! Deze rechten zijn niet absoluut. Je hoeft dus niet altijd gehoor te geven aan een verzoek.

De volgende richtlijnen helpen bij het reageren op een verzoek.

(1) Verzoek indienen

- Zorg dat je informeert over welke rechten een betrokkene heeft (vaak doe je dit in de privacyverklaring);
- Zorg dat je informeert over hoe een betrokkene een verzoek kan indienen, bijvoorbeeld per e-mail (vaak doe je dit ook in de privacyverklaring).

(2) Verzoek beoordelen

- Controleer of de aanvraag helder en compleet is (als de vraag heel breed is, mag je best vragen of de betrokkene de vraag kan specificeren);
- Controleer de identiteit van de betrokkene. Het identificeren van een betrokkene betekent niet noodzakelijk het opvragen van een paspoort of rijbewijs. Stem de wijze van identificatie af aan de hand van de gegevens die worden gevraagd en gebruik zo mogelijk andere opties om iemand te identificeren dan door middel van een paspoort of rijbewijs. Laat bijvoorbeeld iemand met een wachtwoord inloggen op een account op een website van de sportvereniging om gegevens te kunnen opvragen;
- Onderzoek de geldigheid van het verzoek. Of een verzoek geldig is, wordt bepaald door criteria die worden gegeven in het betreffende artikel in de AVG. Voor het bepalen van de criteria kan je de website van de AP raadplegen, zie externe links.

(3) Verzoek uitvoeren

Indien het een verzoek geldig is, voer de verzochte actie dan uit. Afhankelijk van het verzoek kan het gaan om:

- Afschrift van de verzamelde gegevens verstrekken;
- Wijzigen van een gegeven (bijvoorbeeld een e-mailadres);
- Wissen van gegevens;
- Beperken van de verwerking;
- Delen/overdragen van gegevens met/aan een andere partij (direct);

- Staken van de verwerking;
- Informatie verstrekken over de profilering/automatische besluitvorming en zorgen voor menselijke tussenkomst.

(4) Overige aandachtspunten

- **Timing**: afhandeling binnen één maand na ontvangst van het verzoek, tenzij die termijn niet haalbaar is. Informeer dan de betrokkene hierover (ook binnen een maand). De termijn wordt dan met maximaal twee maanden verlengd (dat kan alleen als het verzoek complex is).
- **Vorm**: als je de aanvraag elektronisch (per e-mail) ontvangt, dien je ook elektronisch te reageren.
- **Kosten**: je mag geen kosten in rekening brengen. Hierop bestaan enkele uitzonderingen. Zo mag je bijvoorbeeld administratieve kosten in rekening brengen als iemand herhaaldelijk om een kopie van zijn persoonsgegevens verzoekt.
- **Beveiliging**: als je gegevens verstrekt (recht op inzage), deel die dan ook op een veilige manier (gebruik een veilig mailen optie of beveilig het bestand met een wachtwoord).
- **Weigering**: je mag een verzoek afwijzen als het kennelijk ongegrond is (beoordeling geldigheid), maar ook als het een buitensporig verzoek is. Bijvoorbeeld als iemand wekelijks zijn/haar dossiers opvraagt. Je moet dan wel kunnen aantonen dat er sprake is van een buitensporig verzoek.
- **Privacy derden**: controleer altijd of de gegevens die je deelt geen afbreuk doen aan de rechten en vrijheden van anderen. Als je tot die conclusie komt, verwijder die gegevens over derden dan uit de gegevens die je deelt.
- **Minderjarigen**: gaat het om gegevens van een minderjarige, dan kun je meewerken aan een verzoek van een ouder of voogd.
- **Derde partijen**: als je iemands gegevens hebt gedeeld met een derde partij, regel dan dat het verzet ook bij deze derde wordt doorgevoerd. Tenzij het onevenredig veel inspanning is of onmogelijk blijkt.
- **Klachtrecht**: als je een verzoek weigert dan moet je de betrokkene informeren over de redenen ervan. Ook moet je betrokkene informeren over de mogelijkheid om een klacht in te dienen bij de AP.

6.10.1.Recht op inzage

Een betrokkene heeft het recht om zijn persoonsgegevens in te zien en mag jouw organisatie dus vragen of, en zo ja, welke persoonsgegevens je van hem verwerkt. De betrokkene kan op deze manier controleren of jij je als verwerkingsverantwoordelijke aan de regels houdt.

Wat moet je in zo'n geval verstrekken:

- Een overzicht van de gegevens en informatie over de verwerking (vaak kun je dit uit de privacyverklaring halen);
- Verwerkingsdoeleinden (bijvoorbeeld 'ledenadministratie', 'marketing', etc.);
- Categorieën van persoonsgegevens (bijvoorbeeld 'naam', 'lidnummer', 'wedstrijdhistorie', etc.);
- Bewaartermijnen;
- Informatie over privacy-rechten (zie andere rechten hieronder);
- Informatie over het recht om te klagen bij de AP;
- Informatie over de herkomst van de gegevens (direct van de betrokkene, via vereniging, etc.);
- Informatie over geautomatiseerde besluitvorming en profilering (indien van toepassing);
- Met welke eventuele derden jij deze gegevens hebt gedeeld.

Voorbeeld: inzage-verzoek
Er zijn talloze situaties denkbaar waarin het inzagerecht in conflict komt met jouw of andermans rechten en plichten. Het is belangrijk dat je altijd een zorgvuldige afweging maakt. 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. Kijk dan in de wet of dat een gegronde reden is en je op basis daarvan het verzoek kunt afwijzen.

Let op!

- Een betrokkene kan het inzagerecht slechts uitoefenen over de eigen persoonsgegevens. Inzage in andermans persoonsgegevens is dus niet toegestaan, tenzij het een verzoek door de ouders 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.

6.10.2.Recht op vergetelheid

Een betrokkene heeft het recht om gegevens te laten verwijderen en mag jou vragen om dit te doen. Als het verzoek geldig is, dan moet je de gegevens wissen. Vervolgens moet je ook derden informeren aan wie jij die gegevens hebt verstrekt. Op die manier kunnen die derde ontvangers ook het verzoek doorvoeren. Deze kennisplicht geldt niet als het onmogelijk is of onevenredig veel inspanning vergt.

Let op! Het verzoek om gegevens te laten verwijderen zal niet altijd geldig zijn, bijvoorbeeld omdat wettelijke of overeengekomen bewaartermijnen nog niet zijn verstreken. Een simpel voorbeeld: je kunt de persoonsgegevens van een lid niet verwijderen uit je systeem als het lid nog contributie moet betalen.

6.10.3.Recht op rectificatie

Een betrokkene heeft het recht om gegevens te laten corrigeren of aan te laten passen en mag jou vragen om dit te doen. Het recht op rectificatie is bedoeld om fouten te herstellen bij onjuiste gegevens (uiteraard mag iemand vragen om een adreswijziging als hij/zij pas is verhuisd, graag zelfs!). Dit recht is niet bedoeld om een beoordeling, uitkomst of een mening te veranderen.

6.10.4.Recht op dataportabiliteit

Een betrokkene heeft het recht om gegevens over te laten dragen naar een andere gegevensdrager (of om een kopie te verstrekken) en mag jou vragen om dit te doen. Dit recht is vooral bedoeld voor grote gegevensdragers en niet vaak van toepassing op sportorganisaties.

6.10.5.Recht op beperking van de verwerking

Een betrokkene heeft het recht om een verwerking te beperken en mag jou vragen om dit te doen. Het beperken van de verwerking is eigenlijk een manier om de verwerking tijdelijk te bevriezen (vaak totdat een bezwaar of een geschil is opgelost). Als een verzoek geldig is dan zou je de persoonsgegevens tijdelijk kunnen overbrengen naar een ander systeem (zodat de gegevens niet langer beschikbaar zijn voor reguliere gebruikers) of gepubliceerde gegevens tijdelijk van de website af kunnen halen.

6.10.6.Recht op menselijke blik bij besluiten

Een betrokkene heeft het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem/haar rechtsgevolgen zijn verbonden of dat hem/haar anderszins in aanmerkelijke mate treft. Dit recht zal verder niet inhoudelijk worden behandeld omdat het waarschijnlijk minder relevant is voor de lezers van dit handboek.

6.10.7.Recht op bezwaar

Een betrokkene heeft het recht zich te verzetten tegen de verwerking. Let op, indien betrokkene dit recht kan inroepen dan heeft betrokkene ook automatisch recht op beperking van de verwerking en vergetelheid. Betreft het een bezwaar tegen direct marketing? Dan dien je ervoor te zorgen dat de persoonsgegevens niet meer voor deze doeleinden worden verwerkt. Bezwaren tegen direct marketing mag je niet weigeren.

Tip: Standaard brieven/voorbeelden van een kopie inzage kun je vinden op de website van de AP.

Externe links	Uitleg
Rechten van betrokkenen	Op deze webpagina van de AP vind je uitgebreide informatie over privacy-rechten.
Voorbeeld kopie inzage	Hier vind je een voorbeeldoverzicht inzage persoonsgegevens van de AP.

6.11. Meldplicht datalekken

Als verwerkingsverantwoordelijke moet je een datalek onder bepaalde omstandigheden melden aan de AP en soms ook aan de betrokkene.

6.11.1.Wat is een datalek?

Een datalek is een 'inbreuk in verband met persoonsgegevens'. Het gaat om een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Met andere woorden: een inbreuk op de beveiliging die het gevolg heeft dat toegang wordt gegeven tot persoonsgegevens, persoonsgegevens verloren gaan, of persoonsgegevens worden gewijzigd, zonder dat dit de bedoeling is.

Een aantal voorbeelden van datalekken (de meest voorkomende datalekken van 2020) zijn[1]:

- Persoonsgegevens verstuurd naar/afgegeven aan de verkeerde ontvanger (bijvoobeeld per ongeluk een e-mailbericht aan meerdere ontvangers in de cc versturen in plaats van bcc);
- Hacking, malware (kwaadaardige gegevens verzamelende software) en/of phishing;
- Persoonsgegevens van een verkeerde klant getoond in klantportaal;
- Apparaat, gegevensdrager (vb. externe schijf) en/of papier met daarop persoonsgegevens kwijtgeraakt of gestolen;
- Persoonsgegevens onbedoeld online gepubliceerd.

Let op! Een inbreuk op de beveiliging, oftewel een beveiligingslek, is niet hetzelfde als een datalek. Bij een beveiligingslek hoeft het niet over persoonsgegevens te gaan. Je spreekt pas van een datalek als de inbreuk op de beveiliging daadwerkelijk heeft geleid tot de hiervoor beschreven gevolgen of als dat gevolg redelijkerwijs niet valt uit te sluiten.

6.11.2.Moet ik een datalek melden aan de AP?

In principe moet een verantwoordelijk een datalak zonder onredelijke vertraging, maar uiterlijk binnen 72 uur, melden bij de AP. Dit is alleen niet verplicht indien het onwaarschijnlijk is dat het datalek leidt tot risico's op nadelige gevolgen voor de getroffen personen. Om dat te beoordelen kun je een risico-inventarisatie uitvoeren op de persoonsgegevens die je verwerkt (zie ook: tips).

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

Het datalek moet je melden op de website van de AP. Dit kun je doen door het invullen van een formulier op het meldpunt datalekken (zie externe links).

6.11.3.Moet ik een datalek melden aan de betrokkene?

Een datalek dat moet worden gemeld aan de AP, moet in sommige gevallen ook worden gemeld aan de betrokkenen zelf – de personen van wie data is gelekt. Je bent verplicht het datalek aan de betrokkenen te melden wanneer het datalek waarschijnlijk een hoog risico oplevert voor rechten en vrijheden van de betrokkenen.
Ook hier geldt dat de melding 'zonder onredelijke vertraging' moet gebeuren. Op die manier kunnen de getroffen personen namelijk maatregelen nemen om zich te beschermen tegen de mogelijke negatieve gevolgen (denk aan het opnieuw instellen van een wachtwoord).
Voor de afweging of betrokkenen moeten worden geïnformeerd, is de aard en omvang van het datalek van belang. Indien 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 waardoor het onmogelijk is voor onbevoegden om de gegevens in te zien. Denk hierbij aan beveiligingsmaatregelen zoals encryptie of hashing. Ook wanneer gegevens terecht zijn gekomen bij iemand die gebonden is aan een beroepsgeheim, hoeft het datalek niet te worden gemeld.
De risico's van het datalek moeten wel altijd in kaart worden gebracht. Het is belangrijk te beseffen dat deels versleutelde gegevens, of versleuteling op een achterhaalde wijze, géén passende beveiligingsmaatregelen zijn.

6.11.4.Datalekregister

Alle datalekken (ongeacht wel/niet meldplichtig) moet je documenteren in een overzicht: het datalekregister. Diverse templates kun je gemakkelijk online downloaden.

Tips:

- Heb je geen expertise in huis om de omgang met datalekken af te handelen, schakel dan onmiddellijk een deskundige in.
- Het registreren (loggen) van informatie over wie op welk moment toegang heeft gehad tot gegevens kan helpen bij het inschatten van de omvang van een risico.
- Maak in verwerkersovereenkomsten met verwerkers altijd duidelijke afspraken over het beveiligingsniveau en het melden van datalekken.
- Zorg dat iedereen binnen je organisatie veilig met ICT omgaat en weet hoe er moet worden gehandeld zodra er een vermoeden bestaat van een datalek. Dit doe je door een datalekprotocol op te stellen voor jouw organisatie. 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 datalek 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. Nogmaals, aarzel niet om een specialist in te schakelen als je zelf niet in staat bent adequaat op te treden!

Externe links	Uitleg
Guideline personal data breach notification	Hier download je de guideline over datalekken die de European Data Protection Board (EDPB) heeft gepubliceerd. Deze guideline geeft informatie over de meldplicht datalekken.

Richtsnoeren inzake datalekken	Dit is de Nederlandse vertaling van de guidelines datalekken. Deze guideline geeft informatie over de meldplicht datalekken.
Datalekken	Op deze webpagina van de AP vind je meer informatie over de meldplicht datalekken, waaronder stappenplannen, voorbeeldlijst wel/niet melden, etc.
Meldloket datalekken	Op deze webpagina van de AP kun je een meldwaardig datalek melden.

Template(s)	**Uitleg**
Kernprotocol datalekken	Dit model biedt een uitgangspunt om vast te stellen hoe de organisatie intern omgaat met eventuele datalekken.

6.12. Verwerker

Een verwerker mag alleen handelen in opdracht van de verwerkingsverantwoordelijke. Dat neemt niet weg dat je als verwerker geen verantwoordelijkheden hebt. Ook als verwerker dien je aan een aantal eisen te voldoen. Denk bijvoorbeeld aan de registerplicht, passende beveiligingsmaatregelen, alleen met toestemming van verantwoordelijke sub-verwerkers inschakelen, meldplicht richting verantwoordelijke bij een datalek en het verlenen van medewerking bij een verzoek van de AP.

Om te bepalen wie verwerkingsverantwoordelijke en wie verwerker is, moet je je afvragen waarom deze verwerking plaatsvindt en wie de verwerking heeft geïnitieerd. Degene die beslist of en welke gegevens er worden verwerkt, met welk doel dat gebeurt en op welke wijze is de verwerkingsverantwoordelijke.

De volgende drie bevoegdheden kunnen je richting geven:

- **Juridische bevoegdheid**: als het verwerken van persoonsgegevens expliciet vanuit een taak/plicht is opgedragen aan een organisatie, dan is die partij vaak verwerkingsverantwoordelijke (denk aan het verwerken van persoonsgegevens door de Belastingdienst);
- **Impliciete bevoegdheid**: als het verwerken van persoonsgegevens niet per sé juridisch is vastgelegd (zoals de juridische bevoegdheid hierboven), maar de verwerking wel logischerwijs volgt uit de (wettelijke) taak of verplichting die aan een partij is opgedragen, dan is die partij vaak verwerkingsverantwoordelijke (denk aan een ledenadministratie van een sportvereniging);
- **Feitelijke invloed**: als een partij feitelijke invloed kan uitoefenen op het verwerken van persoonsgegevens en dus bepaalt wat er met de persoonsgegevens gebeurt, wie er toegang hebben, hoelang ze bewaard blijven e.d., dan is die partij vaak de verwerkingsverantwoordelijke.

Na het lezen van bovenstaande, kan het nog steeds zo zijn dat het niet duidelijk is of je voor een bepaalde verwerking verantwoordelijke of verwerker bent. Zo neemt een dienstverlener een proces soms zodanig over, dat je als verantwoordelijke nauwelijks kunt overzien wat deze dienstverlener precies uitspookt. Denk bijvoorbeeld aan IT-leveranciers, waarbij je als niet-deskundige al snel geneigd bent 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 verwerkingsverantwoordelijke in plaats van verwerker. Hierdoor kunnen de (juridische) rollen en verplichtingen anders liggen dan je wellicht verwacht. Laat je bij twijfel in dit soort scenario's tijdig adviseren door een deskundige!

Voorbeelden van verwerkers:

- Salarisadministratie;
- Beheer van apps;
- Hosten van websites;

- Afhandelen van ticketverkoop.

Let op! Zoals je kan lezen in 'De belangrijkste rollen' kan het zijn dat je gezamenlijk doel en middelen bepaalt. In dat geval is sprake van een gezamenlijke verantwoordelijkheid. Dit is bijvoorbeeld zo als een sportorganisatie en een sensor-leverancier gezamenlijk een sensor ontwikkelen die gezondheidsgegevens registreert en beide partijen bepalen hoe en waarom deze gezondheidsgegevens worden verwerkt.

Verwerkersovereenkomst
Als de door jou ingeschakelde dienstverlener een verwerker is, dan sluit je een verwerkersovereenkomst af. Een verwerkersovereenkomst schept een duidelijke taakverdeling en zorgt ervoor dat jij als verwerkingsverantwoordelijke kan voldoen aan de eisen uit de AVG, ook al besteed je een deel van de verwerkingen uit. Via 'templates' vind je een model verwerkersovereenkomst. Je kunt er voor kiezen om dit template te gebruiken of om het template van de dienstverlener te gebruiken. Gebruik je het model van de dienstverlener, controleer dan aan de hand van onderstaande checklist of de verplichte elementen hierin terugkomen.

Checklist verwerkersovereenkomst:
- ✓ Werkzaamheden verwerker:
  - ✓ Incl. onderwerp en duur van de verwerking;
  - ✓ Incl. de aard en doeleinden waarvoor persoonsgegevens worden verwerkt;
  - ✓ Inc. het soort persoonsgegevens en de categorieën van betrokkenen;
  - ✓ Incl. hoe hij/zij met de persoonsgegevens moet omgaan;
  - ✓ Incl. locatie van gegevens (verwerking binnen EER).
- ✓ Beveiliging:
  - ✓ Incl. beveiligingsmaatregelen (en periodieke review daarvan);
  - ✓ Incl. geheimhoudingsplicht.
- ✓ Beveiligingsincidenten (datalekken):
  - ✓ Incl. hoe verwerker een datalek moet melden;
  - ✓ Incl. het bijstand verlenen aan verwerkingsverantwoordelijke bij het vervullen van diens plicht als het gaat om melding aan betrokkenen en/of de AP.
- ✓ Rechten van betrokkenen:
  - ✓ Incl. het bijstand verlenen aan verwerkingsverantwoordelijke bij het vervullen van diens plicht om privacyrechten van betrokkenen te beantwoorden.
- ✓ DPIA (bijstand verlenen aan verwerkingsverantwoordelijke bij het uitvoeren van een DPIA).
- ✓ Onder-aanneming (voorwaarden voor het in dienst nemen van een andere verwerker).
- ✓ Vrijwaring en boete (aansprakelijkheid in geval van schade door het niet naleven).
- ✓ Audit en controle (welke vormen van toezicht je als sportorganisatie mag uitoefenen).
- ✓ Termijn en beëindiging (verplichtingen na beëindiging of ontbinding van de verwerkersovereenkomst, zoals het vernietigen/terug leveren van de persoonsgegevens).

Let op! Mogelijk moet je hier de SCC's aan toevoegen. Meer hierover lees je in het onderdeel 'Internationale doorgifte van persoonsgegevens'.

Is de dienstverlener een (zelfstandig) verwerkingsverantwoordelijke? Dan hoef je niets contractueel vast te leggen. Het inschakelen van een andere verwerkingsverantwoordelijke zal in de sportcontext enkel bij hoge uitzondering gebeuren.

Ben je samen met de dienstverlener gezamenlijk verwerkingsverantwoordelijke(n)?

Dan maak je onderling afspraken over wie invulling geeft aan de rechten en plichten uit de AVG, bijvoorbeeld wie meldt een datalek bij de AP, bij wie kan een betrokkene terecht als hij/zij gebruik wil maken van zijn rechten, wie informeert de betrokkene over de verwerking, etc.
Omdat dit niet vaak voor zal komen, gaan we hier niet heel uitgebreid op in. Wel belangrijk om hierbij nog te vermelden is dat de essentie van hetgeen je samen overeenkomt in de regeling (welke rol een ieder vervult) ook moet worden gecommuniceerd richting de betrokkenen. Hoe dat gebeurt en wiens verantwoordelijkheid dat is, dien je af te spreken in de regeling.

Externe links	Uitleg
Guideline controller processor	Hier vind je de guideline over de verschillende rollen die de European Data Protection Board (EDPB) heeft gepubliceerd. Deze guideline geeft informatie over het beoordelen van de rollen en de bijbehorende rechten en plichten.
Verantwoordelijke en verwerker	Op deze webpagina van de AP vind je meer informatie over de diverse rollen, waaronder een video met uitleg over de verwerkersovereenkomst, een voorbeeldlijst wie is de verwerker/ verwerkingsverantwoordelijke, etc.

6.13. Het verwerkingsregister

Als verwerkingsverantwoordelijke ben meestal verplicht om een register bij te houden van de verwerkingsactiviteiten waarvoor je verantwoordelijk bent. Het verwerkingsregister is een opsomming van de belangrijkste informatie over je verwerkingen met persoonsgegevens.

6.13.1. Wanneer ben ik verplicht een verwerkingsregister bij te houden?

Je bent verplicht een register bij te houden als je organisatie meer dan 250 personen in dienst heeft.

Heb je **minder** dan 250 personen in dienst, dan moet je beoordelen of:

- Je verwerkingen een hoog privacyrisico met zich meebrengen voor betrokkenen; of
- Je verwerkingen niet-incidenteel zijn; of
- Je verwerkingen ook bijzondere persoonsgegevens en/of strafrechtelijke gegevens betreffen.

Indien minimaal één van de drie bovengenoemde gevallen op jouw sportorganisatie van toepassing is, ben je alsnog verplicht een verwerkingsregister bij te houden.

Let op! Ook een verwerker dient een verwerkingsregister bij te houden.

6.13.2. Wat moet ik opnemen in het verwerkingsregister?

Je dient de volgende elementen op te nemen in het register:

- Naam en contactgegevens van de verantwoordelijke organisatie (en evt. naam en contactgegevens van gezamenlijke verantwoordelijken);
- Naam en contactgegevens van de vertegenwoordiger van de verantwoordelijke en de Functionaris Gegevensbescherming (indien van toepassing);
- Verwerkingsdoeleinden;
- Categorieën van betrokkenen;
- Categorieën van persoonsgegevens;
- Categorieën van ontvangers;
- Internationale doorgifte naar welk land/organisatie + passende waarborgen;
- Indien mogelijk: de beoogde bewaartermijnen (of de criteria hiervoor);
- Indien mogelijk: de beoogde technische en organisatorische maatregelen.

Je kan voor het verwerkingsregister gebruik maken van een softwaretool. Maar het kan ook opgenomen worden in een tekstverwerkingsbestand of een Excel spreadsheet. Er zijn online genoeg templates te vinden die je gratis kunt downloaden.

6.14. De Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) (ook wel: Data Protection Officer (DPO)) is de persoon binnen de organisatie die intern toezicht houdt op, en adviseert over, de AVG. Ook is hij/zij vaak aanspreekpunt voor de betrokkene(n), voor medewerkers en voor de AP.

6.14.1. Ben ik verplicht om een FG aan te stellen?

Je bent als sportorganisatie verplicht om een FG aan te stellen als je:

- Een overheidsinstantie of overheidsorgaan bent; en/of
- Op grote schaal individuen volgt/diens activiteiten in kaart brengt en dit een kernactiviteit is (profilering, cameratoezicht, monitoring van iemands gezondheid via wearables); en/of
- Op grote schaal bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens verwerkt en dit een kernactiviteit is.

Uiteraard mag je ook een FG aanstellen als je niet onder één van de hierboven genoemde situaties valt.

Let op! Hoewel je misschien niet verplicht bent een FG aan te stellen, kan het vaak wel verstandig zijn om in ieder geval het aandachtsgebied 'privacy' te beleggen bij één persoon. Je kunt ervoor kiezen om daadwerkelijk een FG aan te stellen (deze persoon moet dan wel dezelfde taken/bevoegdheden/positie krijgen zoals benoemd in de AVG). Je kunt er ook voor kiezen om een Privacy Officer in te huren (fulltime/parttime) of om de taken te beleggen bij een (privacy) jurist.

Tip: Je kunt een FG inhuren op basis van een servicecontract (op basis van flexibele of vaste uren). Een andere optie is om als groep organisaties een gezamenlijke FG te benoemen. Voorwaarde is dan dat deze persoon goed bereikbaar is vanuit elke sportorganisatie en in staat is om zijn/haar wettelijke taken in de praktijk uit te voeren.

Externe links	Uitleg
Aanmelden FG	Hier vind het aanmeld- en wijzigingsformulier waarop je de FG kunt aanmelden bij de AP.
Richtlijnen FG	Hier vind je de Nederlandse vertaling van de guideline voor functionarissen voor gegevensbescherming.
Uitgangspunten FG	Hier kun je de uitgangspunten rondom functionarissen voor gegevensbescherming van de AP downloaden (rollen, processen en verantwoordelijkheden).

6.15. Toezicht, sancties en aansprakelijkheid

We bespreken hierna kort wat er op je pad kan komen bij overtreding van privacy regelgeving. De belangrijkste les daarbij is misschien wel om mogelijke misstanden altijd met serieuze aandacht op te pakken. Realiseer je dat 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.

6.15.1. Handhaving door autoriteiten

Er bestaan verschillende vormen van handhaving.

(1) Formeel onderzoek

Vermoedt een autoriteit dat jouw organisatie de regels overtreedt, dan kan deze een formeel onderzoek starten. De Autoriteit Consument & Markt (ACM) handhaaft daarbij de regels rondom direct marketing en cookies. De AP houdt toezicht op alle overige privacyregels.

Je bent als sportorganisatie verplicht mee te werken aan het onderzoek. 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 advocaat in. Deze begeleidt je in de juiste opstelling tegenover de autoriteit en zorgt dat jouw belangen tijdens het onderzoek goed naar voren komen.

(2) Alternatieve interventie

In plaats van een formeel onderzoek probeert een autoriteit 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 tijdig op reageren en op korte termijn eventuele herstelmaatregelen doorvoeren. Ook in dit geval doe je er goed aan je juridisch te laten bijstaan.

(3) Dwangsommen en boetes

Concludeert een autoriteit na onderzoek dat er sprake is van een overtreding, dan kan ten eerste een zogeheten last onder dwangsom worden opgelegd. Je krijgt dan een formeel bevel 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 overtreding. De maximale boete per overtreding die de AP kan opleggen bedraagt in 2022 maar liefst € 20 miljoen (of 4% van de totale wereldwijde jaaromzet als dat cijfer hoger is). Bij de Autoriteit Consument & Markt is dat € 900.000.
Voordat een boete wordt opgelegd, geven autoriteiten meestal een bindende aanwijzing. In die bindende aanwijzing staat op welke wijze je de overtreding moet beëindigen. Negeer je die aanwijzing, dan volgt alsnog een boete. Is overigens sprake van een 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 AP 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, het onrechtmatig verstrekken van persoonsgegevens of het slecht beveiligen van persoonsgegevens.

Let op! Soms is niet jouw eigen organisatie, maar een ingeschakelde verwerker 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 verwerkersovereenkomst 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 waarmee je de verwerker verplicht tot vergoeding van eventuele claims die jij (als verantwoordelijke) ontvangt van de autoriteiten of betrokkenen.

Aansprakelijkheid

Handel je als organisatie in strijd met privacy regelgeving 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. In Nederland is al een aantal keer op grond van de AVG een vergoeding toegekend voor (immateriële) schade.

Bij opzettelijke en ernstige overtreding van bepaalde privacyregels 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.

ONDERDEEL HET DELEN VAN PERSOONSGEGEVENS

7. Het delen van persoonsgegevens

7.1. Inleiding

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

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

In dit onderdeel geven we vijf vuistregels voor het al dan niet delen van persoonsgegevens met derden. Deze vuistregels zijn afgeleid uit het onderdeel 'Basisregels'. Daarnaast behandelen we waar je op moet letten bij het uitwisselen van gegevens binnen je eigen organisatie en geven we enkele aandachtspunten voor de omgang met vrijwilligers.

Wat wordt bedoeld met 'derden'?

Met derden bedoelen we personen of organisaties die niet onder rechtstreeks gezag staan van de verantwoordelijke, maar ook geen betrokkene of verwerker zijn. Sportbonden, sportverenigingen en koepelorganisaties moeten elkaar meestal ook als derde behandelen. Dat in de sport traditioneel veel informatie wordt uitgewisseld en gezamenlijke doelen worden nagestreefd, doet daar niets aan af. Houd dus ook bij de uitwisseling met samenwerkende organisaties rekening met de hierna besproken vuistregels.

7.2. Vijf regels voor het delen van persoonsgegevens met derden

Regel 1: Bepaal of er een duidelijk doel en geldige grondslag is voor het delen van de gegevens

Het is belangrijk dat je persoonsgegevens alleen aan een derde verstrekt wanneer je daar een duidelijk doel en een geldige grondslag voor hebt. Heb je de gegevens al in je bezit en ontstaat er een andere reden (= nieuw doel) waarvoor je de gegevens met een derde wilt delen? Toets dan of het nieuwe doel verenigbaar is met het doel waarvoor je de gegevens in eerste instantie verzameld hebt. Zie onderdeel 'Basisregels'.

Sport-specifieke voorbeelden:

- De verstrekking van ledengegevens aan sponsoren voor marketingdoeleinden (= doel) op basis van toestemming (= grondslag). (Meer hierover lees je in het onderdeel 'Marketing');
- Het ter beschikking stellen van wedstrijdinformatie inclusief persoonsgegevens van deelnemers en scheidsrechters door sportbonden aan aangesloten verenigingen (= doel) op basis van het gerechtvaardigd eigen belang (= grondslag);
- De doorgifte van adresgegevens van leden aan de uitgever van het clubblad, zodat deze rechtstreeks via de uitgever kunnen worden verzonden (= doel) op basis van ofwel de uitvoering van de overeenkomst ofwel gerechtvaardigd belang (= grondslag);
- De verstrekking van persoonsgegevens van topsporters aan bijvoorbeeld reisbureaus of autoriteiten bij deelname aan evenementen (=doel) op basis van *(hier zijn meerdere grondslagen mogelijk).*

Let op! Je dient altijd te toetsen of het doel dat je nastreeft voldoende aanleiding geeft om persoonsgegevens te delen met een derde. Kun je hetzelfde doel net zo eenvoudig bereiken door het delen achterwege te laten, deel de gegevens dan niet.

Let op! Vaak wordt gedacht dat je gegevens wel mag delen omdat deze toch al openbaar (of publiekelijk bekend) zijn. Dat is niet zo. Ook al zijn persoonsgegevens wellicht al openbaar, dan nog moet je de vijf vuistregels in acht nemen om te bepalen of jouw organisatie die gegevens mag delen met een derde.

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 sportbond wordt gevraagd om verstrekking van het mobiele (privé)nummer. Denk daarbij aan een verzoek om een interview of felicitatie. Wij adviseren daar niet aan mee te werken zonder dat de persoon in kwestie hier vooraf mee heeft ingestemd. Je kunt er dus voor kiezen om de sporter vooraf om toestemming te vragen.

Regel 2: Stel vast of je de betrokkene al hebt geïnformeerd of nog moet informeren
Het is belangrijk dat de verwerking van persoonsgegevens door jouw organisatie transparant is. Dat geldt ook als je gegevens deelt met een derde (dat is namelijk een verwerking). Je moet de betrokkene hierover vooraf informeren.

Voorbeeld: lid is al op de hoogte
Je kunt er regelmatig op vertrouwen dat een lid al op de hoogte is van bepaalde gegevens uitwisselingen. Heb je een lid bijvoorbeeld ten tijde van zijn aanmelding al op de hoogte gesteld dat je voor een specifiek doeleinde zijn/haar naam en lidnummer zal delen met een koepelorganisatie (omdat je dit hebt opgenomen in de privacyverklaring)? Dan hoef je dat niet opnieuw te vertellen op het moment dat die verstrekking plaatsvindt (immers je hebt er al over geïnformeerd).

Voorbeeld: bewust niet informeren
Het komt ook voor dat je persoonsgegevens van de betrokkene hebt gedeeld met een derde, maar de betrokkene daarover op dat moment niet wil of mag informeren. Denk bijvoorbeeld aan vertrouwelijke meldingen rondom grensoverschrijdend gedrag of bepaalde communicatie met dopingautoriteiten. **Let op**, er moet dan wel een duidelijke uitzonderingsgrondslag zijn voor het achterwege laten van het informeren van de betrokkene. Zie hiervoor de uitzonderingen in Art. 41 lid 1 UAVG.

Regel 3: Beoordeel welke gegevens minimaal noodzakelijk zijn om te delen
Het is belangrijk dat je alleen de gegevens deelt die noodzakelijk en voldoende relevant zijn voor het doel waarvoor je de gegevens deelt. De persoonsgegevens van een betrokkene zijn vaak een onderdeel van bijvoorbeeld een spreadsheet, een profiel, een database, etc. Meestal hoef je maar een deel van die informatie te delen om je doel te bereiken.

Voorbeeld: beperkte informatieverstrekking sponsor
Als je e-mailadressen van leden voor de verzending van marketingmails deelt met een sponsor (wat natuurlijk alleen kan als je daar een geldige grondslag voor hebt), voorkom dan dat de sponsor toegang krijgt tot andere gegevens van deze leden. Andere informatie (zoals voor- en achternamen, geboortedata en woonplaatsen) zijn namelijk onnodig om de marketingmail te kunnen verzenden (= doel).

Regel 4: zorg bij het delen van persoonsgegevens voor een veilige overdracht
Als verwerkingsverantwoordelijke ben je verplicht bij het verwerken van persoonsgegevens passende beveiligingsmaatregelen te nemen. Dat geldt ook voor de manier waarop je persoonsgegevens deelt met derden. In het kader van de technische en organisatorische maatregelen die je moet nemen om persoonsgegevens te beveiligen, dien je er ook voor te zorgen dat de gegevens alleen terechtkomen bij de ontvanger die je voor ogen hebt. Voorkom dat data kan worden geraadpleegd door onbevoegden, want daarmee veroorzaak je een datalek. Wil je bijvoorbeeld persoonsgegevens per e-mail versturen, neem dan maatregelen om te voorkomen dat onbevoegden toegang krijgen tot de informatie. De AP geeft twee voorbeelden van passende maatregelen voor e-mail:

- Versleutel de persoonsgegevens in een e-mailbijlage (door het bestand te zippen);
- Versleutel het e-mailverkeer tussen mailservers met een of meerdere moderne internetstandaarden.

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 of het gehele informatiesysteem wordt gedeeld. In dat geval is het zeer verstandig 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 verwerkingsverantwoordelijke optreedt. Let op: dit is niet hetzelfde als de verwerkersovereenkomst.

Regel 5: Indien je deelt: documenteer de verstrekking
Zorg dat je in een later stadium nog kunt achterhalen (en aantonen) onder welke voorwaarden 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.
Gaat het om een incidentele verstrekking, documenteer dan:

- De datum van de verstrekking;
- De wijze van verstrekking;
- Welk soort persoonsgegevens zijn verstrekt;
- Het doel en de grondslag van de verstrekking;
- Wie er heeft verstrekt; en
- Aan wie de verstrekking is gericht.

Wissel je op structurele basis persoonsgegevens uit? Zorg dan dat je deze verwerking opneemt in het verwerkingsregister, zie hiervoor het onderdeel ‘Basisregels’.

7.3 Mag ik gegevens delen binnen de eigen organisatie?
Het uitwisselen van persoonsgegevens binnen je eigen sportorganisatie is geen vorm van delen zoals hierboven besproken. Zolang de uitwisseling namelijk intern plaatsvindt tussen (bijvoorbeeld) werknemers

van de sportorganisatie, is er geen sprake van verstrekking aan een derde. Toch is het belangrijk kort stil te staan bij interne gegevensuitwisseling, omdat ook hier beperkingen gelden.

Je bent namelijk verplicht om persoonsgegevens intern voldoende af te schermen vanwege de eisen van beveiliging en geheimhouding. Iemand mag alleen toegang hebben tot persoonsgegevens als dat nodig is voor de uitvoering van zijn/haar taak.

Sport-specifieke voorbeelden:

- De personeelsadministratie bevat veel vertrouwelijke gegevens en moet alleen toegankelijk zijn voor HR-medewerkers (iemand zijn/haar geboortedatum mag je dus niet zomaar delen met het overige personeel);
- Gevoelige informatie over topsporters is vatbaar voor publieke aandacht en moet daarom beschermd worden tegen onbevoegde inzage door personeel.

Tips:

- Stel duidelijke regels op voor het intern delen van informatie.
- 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. Maak hier gebruik van en zorg dat je de juiste autorisaties op basis van het need-to-know principe toepast.

Externe links	**Uitleg**
Factsheet Beveilig verbindingen van mailservers	Op deze webpagina van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid kun je de factsheet 'Beveilig verbindingen van mailservers' downloaden.
Factsheet TLS-interceptie	Op deze webpagina van het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid kun je de factsheet 'TLS-interceptie' downloaden.
Fix je privacy	Op deze webpagina vind je tips en privacyvriendelijke alternatieven voor mailen en chatten.
Laat je niet hack maken	Op deze webpagina lees je op een begrijpelijke manier hoe je jezelf beschermt tegen hackers.

ONDERDEEL LEDENADMINISTRATIE

8. Ledenadministratie

8.1. Inleiding

Sportorganisaties met individuele leden beschikken uiteraard over een ledenadministratie. Deze 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 sportorganisatie. 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 het onderdeel 'Basisregels'.

In dit onderdeel lichten we toe waar je in de omgang met de gegevens van leden voornamelijk op moet letten. We maken daarin soms onderscheid in sport op amateurniveau en sport op topsportniveau (daaronder schalen we ook selectie en talenten).

Gelaagde structuur

De sportwereld kent een 'gelaagde structuur'. Zo heeft een sporter meestal een lidmaatschap bij een sportvereniging die is aangesloten bij een sportbond, en is deze sportbond aangesloten bij NOC*NSF. Daarbij wordt vaak gesproken over indirecte leden. Dat kan verwarring veroorzaken. Zolang een sportbond geen lidmaatschap is overeengekomen met een persoon, is die persoon 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 de vereniging steeds een geldige grondslag nodig heeft voor het delen van persoonsgegevens met de sportbond of NOC*NSF. Het uitwisselen van persoonsgegevens met een derde zonder geldige grondslag is absoluut niet toegestaan. Meer hierover lees je in het onderdeel 'Het delen van persoonsgegevens'.

Tip: In de praktijk kunnen sportbonden en verenigingen dit probleem grotendeels oplossen door bijvoorbeeld het opnemen van bepaalde constructies in de statuten en/of reglementen. Aangezien dit per sporttak in Nederland behoorlijk kan verschillen, zullen we deze constructies in dit handboek niet bespreken.

8.2. Welke gegevens mag ik opnemen in mijn ledenadministratie?

Je mag natuurlijk een ledenadministratie bijhouden (= doel). Dat kun je doen op basis van het lidmaatschap (= grondslag overeenkomst). Immers: zonder deze gegevens van het lid wordt het erg lastig om de dienst te leveren (= het lid te laten sporten). Veel voorkomende (persoons)gegevens in de ledenadministratie zijn: voornaam, achternaam, lidnummer, adresgegevens, bankgegevens, niveau en eventueel geboortejaar/datum en geslacht (bijvoorbeeld voor de indeling in categorieën). Bankrekeningnummers zijn nodig om de contributie te innen en misschien zijn adresgegevens nodig om een tijdschrift te verzenden. Wil je meer gegevens vastleggen in de ledenadministratie dan noodzakelijk voor het uitvoeren van het lidmaatschap? Bedenk dan dat je daarvoor wellicht een andere grondslag nodig hebt, zoals uitdrukkelijke toestemming of een gerechtvaardigd belang.

Op topsportniveau worden vaak veel meer (persoons)gegevens van leden vastgelegd dan hierboven aangegeven. Deze gegevens zijn dan vaak geen onderdeel van de ledenadministratie, maar worden ergens anders vastgelegd. Meer hierover lees je in het onderdeel 'Talent en topsport'.

Let op! Als je als sportorganisatie een speciaal trainingsprogramma voor paralympische sporters hebt, kan het noodzakelijk zijn daarvoor de paralympische classificatie vast te leggen. Deze classificatie is een gezondheidsgegeven. Bij voorkeur vraag je hier vooraf toestemming voor.

Let op! Gebruik de gegevens uit de ledenadministratie alleen op een manier die verenigbaar is met het doel waarvoor je de gegevens uit de administratie hebt verkregen.

8.3. Hoe informeer ik mijn leden?

Je kunt leden informeren over de gegevens die je verzamelt en wat je ermee doet via een privacyverklaring. Deze kan je bekend maken aan een nieuw lid bij de inschrijving en bijvoorbeeld publiceren op de website.

8.4. Mag ik ledengegevens delen met derden?

We gebruiken in dit onderdeel het begrip 'ledenlijst'. Daarmee bedoelen we slechts een lijst met namen van personen die lid zijn van de vereniging. Dat is dus niet het integrale ledenbestand/de ledenadministratie waarin zich méér ledengegevens bevinden (zoals contactgegevens, financiële gegevens etc.). Of je ledengegevens mag delen, hangt af van de ontvanger. Zie hieronder.

8.4.1. Persoonsgegevens van leden beschikbaar stellen aan andere leden

Je mag niet zonder duidelijk doel ledengegevens beschikbaar stellen aan andere leden. Ook niet als het gaat om een afgeschermde website. Je raakt dan de controle kwijt over de circulatie van de ledenlijst. In principe zouden ledengegevens maar voor een beperkt aantal personen toegankelijk moeten zijn. Denk hierbij aan de penningmeester en secretaris in het kader van verenigingsadministratie. Wil je ledengegevens beschikbaar stellen aan leden, vraag je dan altijd af waarom, welke gegevens daarvoor minimaal noodzakelijk zijn en voor wie. Kortom, op basis van welk gerechtvaardigd belang kun je dat doen. Een aantal voorbeelden:

- Het lijkt van gerechtvaardigd belang om namen en telefoonnummers uit te wisselen binnen het eigen team, maar niet buiten het eigen team;
- Het lijkt van gerechtvaardigd belang om een lijst met namen en telefoonnummers van de B6 Jongens te delen met de trainer van de B6. Hij hoeft niet te weten wie er in de andere B-teams zitten, tenzij bepaalde teams bijvoorbeeld regelmatig invallers leveren voor de B6.

Wil je toch echt ledengegevens beschikbaar stellen aan andere leden? En heb je daarvoor geen gerechtvaardigd belang? Dan kun je daarvoor het beste om toestemming vragen. Bedenk wel, dat toestemming altijd kan worden ingetrokken.

Tip: Bedenk altijd goed wat het neveneffect is van het beschikbaar stellen van ledengegevens. Zeker als het minderjarige sporters betreft. Stel Jan vindt Anneke een heel leuk meisje en komt via de ledenadministratie gemakkelijk aan haar telefoonnummer. Dat is een inbreuk op de privacy van Anneke.

8.4.2. Online publiceren (toegankelijk voor het brede publiek)

Je mag de ledenlijst niet zomaar online publiceren. De AP is van oordeel dat het online publiceren van een ledenlijst slechts is toegestaan op een voor leden afgeschermde webpagina (lees het onderdeel hierboven).

Voorbeeld: online databank

Als je als sportorganisatie 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. En zie ook het onderdeel hierboven, bedenk vooraf of je een geldige reden en grondslag hebt voor het beschikbaar stellen van die informatie; en zo ja, welke informatie en aan wie.

8.4.3. Ledengegevens delen met sponsoren voor marketingdoeleinden

Hiervoor verwijzen we je naar het onderdeel 'Marketing'.

8.5. Hoelang bewaar ik de gegevens?

Als een lid zich uitschrijft, dan hoeven zijn gegevens niet direct na het einde van het lidmaatschap te worden verwijderd. Voor een geschikte bewaartermijn kan (nog steeds) worden aangesloten bij het Vrijstellingsbesluit. In dat geval betekent dit dat je persoonsgegevens van een lid uit de ledenadministratie in principe niet langer bewaart dan twee jaar na het 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.

Wil je persoonsgegevens van oud-leden langer bewaren dan twee jaar, bijvoorbeeld omdat je iemand wellicht een paar jaar later nog wilt uitnodigen voor een reünie? Dan kun je in dat geval het lid het beste om toestemming vragen. Dat kun je bijvoorbeeld doen als onderdeel van het uitschrijfformulier. Je vraagt dan of iemand op de oud-leden of alumni-lijst geplaatst wil worden en e-mails wil ontvangen.

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. Als je deze doeleinden ook kunt bereiken met geanonimiseerde of gepseudonimiseerde gegevens, dan ben je verplicht om de gegevens te anonimiseren of pseudonimiseren.

Externe links	Uitleg
Website AP	Op deze webpagina van de AP lees je over het verzamelen en gebruiken van gegevens van leden binnen verenigingen.

ONDERDEEL ORGANISEREN WEDSTRIJDEN

9. Gegevens verzamelen voor het organiseren van wedstrijden

9.1. Inleiding

In dit onderdeel lichten we toe waar je bij het verzamelen van gegevens in het kader van een wedstrijden op moet letten. Waar relevant wordt onderscheid gemaakt tussen amateursport en topsport (daaronder schalen we ook selectie en talenten).

9.2. Welke gegevens mag ik verzamelen in het kader van de wedstrijd(organisatie)?

Wanneer een persoon zich inschrijft voor deelname (hierna: deelnemer) aan een wedstrijd dan worden daarbij logischerwijs persoonsgegevens verwerkt. De gegevens die noodzakelijk zijn voor het organiseren van de wedstrijd (= doel) worden verwerkt op basis van de inschrijving, die je kunt zien als een overeenkomst (= grondslag). Immers, je moet iemand op basis van leeftijd/geslacht/niveau kunnen indelen in de juiste poul/klasse, met iemand kunnen communiceren via e-mail over zijn/haar deelname aan de wedstrijd, de betaling kunnen innen vanaf een specifiek bankrekeningnummer, etc.

Wil je meer gegevens verwerken dan noodzakelijk voor het organiseren van de wedstrijd? Bedenk dan dat je daarvoor wellicht een andere grondslag nodig hebt, zoals uitdrukkelijke toestemming of een gerechtvaardigd belang.

9.3. Hoe informeer ik deelnemers?

Zorg ervoor dat je een deelnemer informeert over de gegevens die je in het kader van de wedstrijd verzamelt en wat je ermee doet. Dat kun je doen door dit te vermelden bij het inschrijven voor de wedstrijd (bijvoorbeeld op het inschrijfformulier) of door een algemene regel op te nemen in je algemene privacyverklaring (het is dan wel noodzakelijk dat je hiernaar linkt op het inschrijfformulier).

Let op! Indien je persoonsgegevens van deelnemers publiceert op een openbare website, dan dien je de betrokkene hierover vooraf te informeren.

9.4. Mag ik de persoonsgegevens van deelnemers delen?

Dat hangt van de situatie af. Lees hieronder verder in welke gevallen je persoonsgegevens mag delen.

9.4.1. Inschrijfgegevens

➔ Inschrijfgegevens beschikbaar stellen aan andere deelnemers

Zonder duidelijk doel mag je geen inschrijfgegevens beschikbaar stellen aan andere deelnemers. Vraag je simpelweg weer af: is het delen van persoonsgegevens noodzakelijk voor het organiseren van de wedstrijd? Zo ja, voor welke persoonsgegevens geldt dit dan? En aan wie moeten die persoonsgegevens worden gedeeld (bijvoorbeeld: alleen aan deelnemers binnen de poule of aan alle deelnemers)?

Is het delen van persoonsgegevens niet nodig voor het organiseren van de wedstrijd, maar is het delen ervan wel in het redelijke belang van jouw sportorganisatie of een derde (bijvoorbeeld andere verenigingen)? Als je dat goed kunt onderbouwen, kan je het gerechtvaardigd belang (mogelijk) als grondslag gebruiken.

Hieronder volgen voor amateursport niveau een aantal voorbeelden die je richting kunnen geven bij het zelf bepalen of het delen van persoonsgegevens al dan niet is toegestaan. Let wel, dit zijn algemene voorbeelden. Of je de persoonsgegevens in jouw geval mag delen hangt af van de specifieke omstandigheden van het geval:

- Individuele sport: het is wellicht nodig om voor- en achternaam en eventueel het niveau van deelnemers te delen met andere deelnemers in dezelfde poule of in hetzelfde team (gerechtvaardigd belang);

- Teamsport: stel dat voetbalteam VOC D5 zich heeft ingeschreven voor het Oliebollentoernooi van een bevriende club in Den Haag. Het is voor VOC niet nodig om voor- en achternaam van de teamleden van VOC D5 te delen met de Haagse club. Immers, aangeven dat VOC D5 zich heeft ingeschreven voor de wedstrijd is in dat geval waarschijnlijk voldoende.

Op topsport niveau ligt het beschikbaar stellen van inschrijfgegevens aan deelnemers eerder in de lijn van deelname aan de wedstrijd. Het is bijna inherent aan sport dat vanaf een bepaald niveau, je persoonlijke deelname aan een wedstrijd bekend wordt gemaakt. Stel jezelf als sportvereniging of bond echter nog steeds bovengenoemde vragen en zorg ervoor dat je de gemaakte afweging vastlegt.

Inschrijfgegevens (online) publiceren
Vaak is het niet noodzakelijk om inschrijfgegevens te publiceren op een openbare website, omdat de informatie maar voor een beperkte groep relevant is. In de meeste gevallen zorg je er daarom voor dat informatie alleen voor de relevante groep beschikbaar is (lees het onderdeel hierboven 'inschrijfgegevens beschikbaar stellen aan andere deelnemers'). Dit kan bijvoorbeeld door middel van een portaal waar leden voor moeten inloggen.

Wil je de persoonsgegevens van ingeschreven deelnemers toch online publiceren (op een publiekelijk toegankelijke website)? Dan moet je goed kunnen onderbouwen dat het publiceren van deze inschrijfgegevens nodig is vanuit een belang van jouw sportorganisatie of een derde (bijvoorbeeld andere verenigingen). In dat geval kun je het gerechtvaardigd belang als grondslag gebruiken. Kun je dat niet goed onderbouwen, dan kun je nog overwegen om de deelnemers om toestemming te vragen.

Op amateursport niveau zul je voor het delen van persoonsgegevens eerder uitkomen op toestemming. Op topsport niveau kun je het gerechtvaardigd belang waarschijnlijk beter beargumenteren. Immers, open publicatie op hoger sportniveau kan in het belang van zowel de sporter als de sportorganisatie zijn. Bijvoorbeeld voor potentiele sponsoren, naamsbekendheid, wervende doeleinden, etc.

Let op! Als het noodzakelijk is om een individu op een openbare lijst te publiceren, overweeg dan eerst of het mogelijk is om een lidnummer te gebruiken in plaats van een achternaam. Dat is weliswaar nog steeds een persoonsgegeven (gepseudonimiseerd), maar de publicatie ervan is minder bezwaarlijk dan die van een voor- of achternaam.

Tip: Zorg dat je als sportorganisatie altijd bewust bent van de mogelijke (negatieve) privacygevolgen voor de betrokkene van de (online) publicatie. Bij minderjarigen ligt dit bijvoorbeeld anders dan bij volwassenen.

> **Voorbeeld: scheidsrechters**
> Bij scheidsrechters lijkt het misschien logischer dat je hun naam vermeldt. Let wel, vaak ontbreekt de echte noodzaak om daar contactgegevens aan toe te voegen (zoals het mobiele telefoonnummer). Natuurlijk kun je dit wel doen als de publicatie inclusief contactgegevens echt noodzakelijk is vanuit een belang van de sportorganisatie of een derde.

9.4.2. Wedstrijdverslagen, uitslagen en standen

Met de huidige technologie is het steeds eenvoudiger om informatie over uitslagen, standen en ranglijsten in real-time online te publiceren (zodat ze beschikbaar zijn voor het brede publiek). Als de wedstrijduitslagen en standen ook persoonsgegevens bevatten (zoals naam en/of identificatienummer), dan moet je natuurlijk rekening houden met de privacyregels. Bevat de wedstrijdinformatie geen gegevens over individuele personen, maar enkel informatie op teamniveau (zoals VOC D5)? Dan kan de gemiddelde lezer deze

informatie waarschijnlijk niet gemakkelijk herleiden naar één van de teamleden. VOC kan hierdoor (als verwerkingsverantwoordelijke) gemakkelijker een beroep doen op haar gerechtvaardigd eigen belang (namelijk: verslag doen van de wedstrijd). Let op, voor VOC is de publicatie van wedstrijduitslagen wel een persoonsgegeven, omdat de club in haar ledenadministratie kan nagaan welke spelers er in de D5 zitten.

➔ **Verenigingsblad/nieuwsbrief**

Het ligt in de lijn der verwachting dat je deelnemers of leden van de eigen sportorganisatie informeert over wedstrijdstanden en uitslagen. Je kan dit doen op basis van de journalistieke uitzondering in de AVG en de UAVG. Let op, er moet wel sprake zijn van een zekere mate van nieuwswaarde. Wil je gebruik maken van deze uitzondering, dan geldt ook hier een noodzakelijkheidstoets: vrijheid van meningsuiting (verspreiden van het nieuws) vs. het belang van het individu. Als sportorganisatie kun je dus verslag doen over successen van de wedstrijd en aangeven wie er bijvoorbeeld gescoord heeft binnen de eigen sportorganisatie. Wees daarbij extra voorzichtig met verslaglegging van wedstrijden van minderjarigen. Lees hieronder verder voor online publicatie.

➔ **(Online) publicatie**

Wil je als sportorganisatie wedstrijdverslagen, uitslagen en standen online publiceren en deze toegankelijk maken voor het bredere publiek? De gemakkelijkste weg is dan om te kiezen voor het publiceren van uitslagen op teamniveau, zoals hierboven al beschreven.

Op amateursport niveau is het vaak niet noodzakelijk wedstrijdverslagen, uitslagen en standen te publiceren op een openbare website. Daarvoor kun je beter de nieuwsbrief of een afgeschermde locatie gebruiken (lees hierboven: verenigingsblad/nieuwsbrief). Wil je de gegevens toch online publiceren op een publiekelijk toegankelijke website? Zorg dan dat je een zorgvuldige belangenafweging maakt.

Op topsport niveau is het openbaar publiceren van wedstrijdverslagen, uitslagen en standen wat gebruikelijker. Je kunt dan beoordelen of je gebruik kunt maken van de grondslag gerechtvaardigd belang. Vaak zal dit in het belang van beiden zijn: voor de sporter vanwege publiciteit/herkenbaarheid en voor de sportorganisatie vanwege werving, etc. Toch geldt ook hier dat niet méér persoonsgegevens mogen worden gepubliceerd dan noodzakelijk is. Zo is het vermelden van de bloeddruk of de hartslag (wat bijzondere persoonsgegevens zijn) tijdens een sportwedstrijd natuurlijk geen geaccepteerde verwerking.

Let op! Indien je kiest voor het gerechtvaardigd belang, wees dan extra voorzichtig als het gaat om minderjarige sporters. Neem dit mee in je belangenafweging!

9.5. Welke beveiliging pas ik toe?

Zorg ervoor dat je de inschrijfgegevens passend beveiligt. Naast het toepassen van moderne beveiligingstechnieken op je applicatie (waar je de gegevens verzamelt/opslaat) is het van belang de toegang tot de gegevens te beperken. Immers, niet iedereen binnen de sportorganisatie heeft voldoende belang bij toegang tot (alle delen van) de inschrijfgegevens. Beperk iemands toegangsrechten dus op basis van zijn taken en verantwoordelijkheden.

9.6. Hoelang bewaar ik de gegevens?

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

Zoals je in het onderdeel ‘Basisregels’ kunt lezen, is het uitgangspunt dat je de persoonsgegevens niet langer bewaart dan noodzakelijk is voor het doel waarvoor je ze hebt verzameld. Zo is het waarschijnlijk niet nodig inschrijfgegevens na afloop van de wedstrijd nog te bewaren. Het kan natuurlijk wel nodig zijn om

wedstrijduitslagen en standen te koppelen aan een individu als daar een niveau aan wordt gekoppeld (zoals bij tennis). In ieder geval voor de duur van het lidmaatschap lijkt het in dat geval relevant die gegevens te bewaren. Sommige persoonsgegevens uit de wedstrijdverslagen, uitslagen en standen zal je misschien ook daarna nog 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. Als je deze doeleinden ook kunt bereiken met geanonimiseerde of gepseudonimiseerde gegevens, dan ben je daartoe verplicht.

ONDERDEEL TALENT EN TOPSPORT

10. Talent en topsport

10.1. Inleiding

Op topsport niveau verwerkt een sportorganisatie vaak meer en gevoeligere persoonsgegevens vergeleken met amateursport niveau. We bespreken hierna kort welke implicaties dit heeft voor een aantal veel voorkomende processen in de sportorganisatie. Als we het hebben over topsporters, dan bedoelen we daarmee ook talenten.

10.2. Heb ik een doel en grondslag?

10.2.1. Mag ik gezondheidsgegevens verwerken?

De persoonsgegevens van talenten en topsporters die in trainings- en begeleidingsprogramma's worden verwerkt door sportorganisaties zijn vaak deels gezondheidsgegevens. In het onderdeel 'Basisregels' is uitgelegd dat gezondheidsgegevens bijzondere persoonsgegevens zijn. Het verwerken van deze gegevens is dus niet zomaar toegestaan.

Voor jou als sportorganisatie betekent dit in de praktijk dat je slechts gezondheidsgegevens van de sporter mag verwerken als de sporter daar uitdrukkelijke toestemming voor geeft. Dat kun je regelen door middel van een toestemmingsverklaring.

Let op! Voorheen werd toestemming van een sporter nog wel eens via een contract geregeld. Momenteel wordt dat niet meer gezien als een geldige toestemming. Toestemming mag dus geen onderdeel zijn van een contract. Er moet sprake zijn van een handeling van de betrokkene die direct aangeeft of hij/zij toestemming geeft: denk aan het aanklikken van een vink box of het ondertekenen van een verklaring.

Procedures / arbitrage

Is het verwerken van gezondheidsgegevens nodig voor juridische procedures zoals bijvoorbeeld sportarbitrage? Dan is toestemming niet zo voor de hand liggend. Je dient dan te beoordelen of je daar een andere uitzonderingsgrondslag voor hebt. Voor zover het verwerken van de gegevens noodzakelijk is om een procedure te kunnen voeren, kun je beoordelen of je dit kunt doen op basis van de AVG (Artikel 9 lid 2 f).

10.2.2. Mag ik de sporter monitoren?

Topsporters worden doorgaans nauwkeurig gemonitord. Daarvoor worden diverse systemen gebruikt die (bijvoorbeeld via mobiele applicaties en wearables) allerlei aspecten in kaart brengen, zoals trainingsschema's, prestatiemetingen, communicatie met trainers en blessureoverzichten (= doel). Ook deze data bevatten vaak gezondheidsgegevens. Immers, vaak geven deze systemen direct inzicht in de gezondheidstoestand. Er wordt namelijk een lichaamsfunctie/stof gemeten, of de gegevens zijn op zichzelf geen gezondheidsgegevens, maar kunnen dat in combinatie met andere gegevens of door verloop van tijd wél worden. Ook hiervoor geldt dat je deze gegevens slechts mag verwerken als de sporter daar uitdrukkelijke toestemming voor geeft (= grondslag). Dat kun je regelen door middel van een toestemmingsverklaring.

10.2.3. Mag ik wearable-data verwerken?

Hierboven werd het gebruik van wearables al kort genoemd. Wearables zijn draagbare apparaatjes die allerlei lichaamsfuncties kunnen meten. Denk aan stappentellers, bloeddrukmeters en hartslagmeters die je op je lichaam of kleding draagt. Het analyseren van deze gegevens kan bijdragen aan het verbeteren van de sportprestatie (= doel). De gegevens die met wearables worden gegenereerd zijn vaak ook aan te merken als gezondheidsgegevens. Dit betekent dat sporters meestal uitdrukkelijke toestemming zullen moeten geven voor het verzamelen en analyseren van wearable-data (= grondslag).

Let op! Het geven van 'vrije' toestemming kan in de sportcontext problematisch zijn. Meer hierover lees je in het onderdeel 'Basisregels'.

10.3. Hoe ga ik om met het organiseren van reizen (en het daarbij delen van persoonsgegevens)?

Sport (en vooral topsport!) is een internationale aangelegenheid. Sporters, vrijwilligers en medewerkers van sportorganisaties zijn vaak op reis. Bij het boeken van deze reizen worden behoorlijk wat persoonsgegevens verwerkt. Denk aan namen, geboortedata, frequent flyer numbers en (wellicht) ook betaalgegevens van deelnemers aan het reisgezelschap. De sportorganisatie die de boeking regelt, is hierbij vaak de verwerkingsverantwoordelijke. De ontvangers (derden), zoals het reisbureau of een luchtvaartmaatschappij, zijn vervolgens zelfstandig verwerkingsverantwoordelijken voor de verwerkingen die zij op hun beurt verrichten. Met dit soort organisaties hoef je dus geen verwerkersovereenkomst te sluiten.

De verstrekking van persoonsgegevens (voor zover nodig om de reis te boeken) door de sportorganisatie aan derden kan worden gebaseerd op de grondslag: uitvoering van een overeenkomst, toestemming of een gerechtvaardigd belang.

Let op! In aanloop naar en tijdens de reis wordt nog wel eens gevraagd om een kopie van een paspoort. Het vragen van een kopie is onder de Nederlandse wetgeving niet zomaar toegestaan. Het paspoort bevat namelijk het Burgerservicenummer (BSN). Dit nummer mag alleen worden gebruikt als er een wettelijke basis voor is, en daar is maar in een beperkt aantal gevallen sprake van. Hoe je hiermee omgaat lees je in de richtsnoeren 'kopietje paspoort' van het AP, zie externe links.

10.4. Hoe ga ik om met minderjarigen?

Het verwerken van persoonsgegevens van een topsporter jonger dan 16 jaar vereist extra aandacht. Zoals we hebben uitgelegd in het onderdeel 'Basisregels' kan hij/zij namelijk niet zelfstandig toestemming geven. Aangezien voor het verwerken van gezondheidsgegevens veelal toestemming nodig zal zijn, zal die toestemming in het kader van de begeleiding van minderjarigen steeds door een ouder of voogd moeten worden verleend. Houd daar rekening mee bij het contracteren van minderjarig talent.

10.5. Welke beveiliging pas ik toe?

Realiseer je datgegevens van topsporters kunnen rekenen op extra aandacht van de buitenwereld, waaronder zich ook kwaadwillende partijen kunnen bevinden. Een goede beveiliging van de persoonsgegevens van topsporters is van groot belang om datalekken te voorkomen. Als IT-leveranciers betrokken zijn bij de verwerking van persoonsgegevens (bijvoorbeeld door het hosten van webapplicaties of apps), dan zijn deze partijen vaak verwerkers en moet een verwerkersovereenkomst worden gesloten.

Bovendien geldt voor het verwerken van gezondheidsgegevens, dat je het beveiligingsniveau hoogstwaarschijnlijk wat moet opschalen. Immers, gegevens moeten passend worden beveiligd. Ook moet je voorzichtig omgaan met het inzicht geven in deze data. Beoordeel goed welke personeelsleden/begeleidende stafleden toegang nodig hebben tot de gegevens van talenten en topsporters om hun functie uit te kunnen voeren.

Let op! Partijen die wearables aanbieden, zien zichzelf als verwerkingsverantwoordelijken. Dat betekent dat je met hen geen extra afspraken kunt maken. Indien dit soort partijen zichzelf als verwerkingsverantwoordelijke zien, beoordeel dan vóór afname/gebruik van het product, of zij wel voldoende bescherming bieden voor het verwerken van persoonsgegevens. Immers: je wilt er ten alle tijden voor zorgen dat de data van je talent en topsporters veilig zijn en bijvoorbeeld niet worden doorverkocht.

10.6. Hoelang bewaar ik de gegevens?

Hoelang je gegevens van talent en topsporters bewaart, hangt af van het doel waarvoor je deze verzamelt. Het is daarom lastig om algemene uitspraken te doen over een geschikte bewaartermijn.

In principe kun je aansluiten bij de bewaartermijn van de ledenadministratie. Immers, een talent of topsporter is vaak lid van jouw sportorganisatie. Je kunt hiervoor dus (nog steeds) aansluiten bij het Vrijstellingsbesluit, wat betekent dat je persoonsgegevens van een talent of topsporter in principe niet langer bewaart dan twee jaar na het einde van het lidmaatschap. Let wel dat, indien het niet nodig is om alle persoonsgegevens te bewaren, simpelweg omdat het niet meer bijdraagt aan de topsportbegeleiding, je verplicht bent om de gegevens tussendoor te verwijderen.

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. Als je deze doeleinden ook kunt bereiken met geanonimiseerde of gepseudonimiseerde gegevens, dan dien je de gegevens te anonimiseren of pseudonimiseren.

Let op! Wees daarbij extra voorzichtig met gezondheidsgegevens. Wil je de gegevens langer bewaren voor bovengenoemde doeleinden, zorg er dan voor dat je deze gegevens anonimiseert.

Externe links	Uitleg
Richtsnoeren 'kopietje paspoort'	De AP publiceert richtsnoeren voor het gebruik van een ‘kopietje paspoort’. De richtsnoeren geven aan welke regels gelden bij het overnemen van persoonsgegevens of het kopiëren, scannen of uitlezen van identiteitsdocumenten.

ONDERDEEL MARKETING

11. Marketing

11.1. Inleiding

In dit onderdeel bespreken we de belangrijkste regels bij het versturen van (commerciële) berichten, sociale media, winacties en cookies. Ook bespreken we of en op basis waarvan je ledengegevens mag delen met sponsoren of andere partijen.

Belangrijk om te begrijpen is dat we in dit hoofdstuk niet alleen rekening houden met de AVG. Het is namelijk de Telecommunicatiewet die de regels bepaalt als het gaat om het versturen van ongevraagde e-mails, commerciële telefoontjes en het plaatsen van cookies.

11.2. Het versturen van (commerciële) berichten

11.2.1. Wat is direct marketing?

Direct marketing is het individueel benaderen van een persoon of rechtspersoon ter promotie van een organisatie, product of dienst. Het sturen van berichten met een commerciële boodschap naar iemands e-mailadres is dus een vorm van direct marketing. Voor direct marketing via elektronische berichten gelden bijzondere regels, ook wel de 'SPAM-regels' genoemd. Deze regels lichten we hieronder verder toe.

11.2.2. Wanneer is het SPAM-verbod van toepassing?

Het SPAM-verbod geldt voor ongevraagde commerciële elektronische berichten. In de meeste gevallen gaat het dan om direct marketing; in de boodschap zit een wervend element. Welke berichten vallen hieronder? E-mails, sms'jes, appjes, directe berichten op social media, etc. Naast berichten gericht op verkoop, gaat het hier ook om berichten gericht op het vergroten van naamsbekendheid, het werven van fondsen voor een goed doel en ledenwerving.

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 (doel = service bieden) bevat, is het SPAM-verbod niet van toepassing. Zo'n nieuwsbrief mag dus door een vereniging worden verstuurd. Er moet dan wel daadwerkelijk sprake zijn van een lidmaatschap. Meer hierover lees je in het onderdeel 'Hoe zit het met gemengde nieuwsbrieven aan leden'.

Sport-specifieke voorbeelden: SPAM-verbod niet van toepassing (geen toestemming nodig):

- Het versturen van algemene mededelingen (zoals de uitnodiging voor een ledenvergadering of de verenigingsagenda, wedstrijduitslagen, evenementenagenda);
- Het versturen van een antwoord aan een persoon die een verzoek heeft ingediend via het contactformulier;
- Het versturen van een ontvangstbevestiging;
- Het versturen van een betalingsherinnering;
- Het versturen van een informatief persbericht aan journalisten.

11.2.3. Heb ik toestemming nodig voor het versturen van berichten?

We gaan er hier vanuit dat het SPAM-verbod van toepassing is (en dat het gaat om het versturen van ongevraagde commerciële elektronische berichten).

➔ **Wel toestemming nodig:**

In principe heb je voor het versturen van ongevraagde elektronische direct marketing berichten (meer hierover in het onderdeel hierboven) toestemming nodig van de ontvanger. Hierbij gaat het dan meestal om berichten als nieuwsbrieven of reclame.

Vanuit de SPAM-regels geldt het opt-in-systeem. Dat betekent dat iemand uitdrukkelijk en vooraf met het ontvangen van direct marketing berichten moet hebben ingestemd. Een opt-out (daarbij vraag je niet vooraf toestemming, maar bied je wel de gelegenheid aan de ontvanger om zich uit te schrijven) is hierbij niet voldoende!

Let op! Probeer geen toestemming te verkrijgen door het opnemen/wegstoppen van een instemmende bepaling in de algemene voorwaarden of een privacyverklaring. Dat is impliciete toestemmingsverlening: toestemming wordt dan onvoldoende uitdrukkelijk verkregen. Vraag dus altijd apart en expliciet om toestemming. Er is één uitzondering, daarover meer in het onderdeel hieronder.

➔ **Geen toestemming nodig:**

Slechts in uitzonderlijke gevallen en onder bepaalde voorwaarden heb je geen toestemming nodig. We noemen dat ook wel de 'bestaande klant uitzondering 'of 'soft opt-in'. Die uitzondering houdt in dat, wanneer je het mailadres van de ontvanger hebt verkregen doordat je iemand een product of dienst hebt verkocht, je deze persoon commerciële berichten mag sturen over eigen, soortgelijke producten of diensten. Dit mag alleen als:

- Je de ontvanger op het moment dat je zijn/haar gegevens ontvangt in het kader van de verkoop, de mogelijkheid hebt gegeven om hier een opt-out voor te geven; en
- Je de ontvanger in iedere commerciële mailing de mogelijkheid geeft om zich uit te schrijven.

Deze uitzondering is overigens niet oneindig geldig. Om de duur van de uitzondering te bepalen, moet je je inleven in de verwachting van de ontvanger: hoe lang voelt iemand zich na aankoop nog klant. Bepalend zijn daarbij o.a. de aard van het product, de levensduur en de looptijd van de overeenkomst.

Let op! Houd er rekening mee dat deze uitzondering waarschijnlijk in de nabije toekomst begrensd gaat worden. In concept regelgeving voor het Europese Parlement wordt de termijn waarbinnen iemand nog klant is namelijk begrensd. Het is verstandig om daar nu alvast op te anticiperen. Dat kan door na een bepaalde periode een bestand (record) automatisch uit je CRM (Customer Relationship Management) database te verwijderen als de ontvanger geen klant meer is, bijvoorbeeld als hij/zij een jaar lang geen product meer heeft gekocht.

Let op! Maak je gebruik van deze uitzondering voor het versturen van je commerciële berichten? Wees je dan bewust van het feit dat de inhoud van je mailing alleen mag zien op eigen, soortgelijke producten/diensten. Dat betekent dat je in je commerciële berichten geen commerciële boodschappen van derde partijen (bijvoorbeeld sponsoren van jouw vereniging) mag opnemen. Wat een soortgelijk product of dienst is, kun je bepalen aan de hand van de blik van een objectieve gemiddelde klant.

Let op! Is je bericht vrijwel geheel een commerciële boodschap van een sponsor die door de sportbond wordt verstuurd, dan gaat de bestaande klant uitzondering dus niet op. In dat geval heb je toestemming nodig van de ontvanger.

Sport-specifieke 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 hem/haar dus niet benaderen met reclame voor een evenement of opleiding (tenzij je daar uiteraard aparte toestemming voor hebt verkregen).

Een andere uitzondering is als je een bericht verstuurt aan een zakelijk e-mailadres dat bestemd én bekend is voor zulke ongevraagde berichten. Een fictief voorbeeld is het e-mailadres aanbiedingen@sportbond.nl. Let op dat een algemeen 'info@'-e-mailadres weer niet voldoet aan de eisen voor deze uitzondering. Hier mag je niet zomaar berichten aan sturen.

11.2.4.Hoe zit het met gemengde nieuwsbrieven aan leden?

Het is in de sportwereld gebruikelijk dat sportbonden aan leden 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. Er is namelijk geen duidelijke grens tussen een puur commercieel bericht of een puur dienstverlenend bericht. Zo mag een dienstverlenend bericht best eens een commercieel element bevatten. Hoe beoordeel je dan of je hiervoor om toestemming moet vragen? Bepaal wat het hoofddoel van de e-mail is: wil je enkel service bieden of heeft de e-mail hoofdzakelijk een commercieel belang? Probeer daarbij ook altijd uit te gaan van de beleving van de ontvanger (hoe wordt de e-mail ervaren)? Ga er bij twijfel vanuit dat het een commercieel bericht is en houd rekening met bovengenoemde verplichtingen. Dus: alleen versturen met toestemming of op basis van een klantrelatie.

Tip: Een verstandige oplossing is natuurlijk om voor gemengde berichten iedere geadresseerde vooraf om toestemming te vragen. Je ondervangt hiermee het probleem dat per bericht discussie kan ontstaan over de aard (commercieel/niet-commercieel) ervan.

Let op! Het kan zo zijn dat je over adresbestanden beschikt waarbij je tot op heden geen expliciete toestemming hebt verkregen voor het verzenden van commerciële berichten. Mocht je aan die adressen gemengde berichten sturen, zorg dan minstens dat je een opt-out biedt aan de ontvangers (meer hierover in het volgende onderdeel).

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

Let op! De enkele vermelding van een sponsor, bijvoorbeeld door het plaatsen van een logo onderin de nieuwsbrief aan leden (met uitsluitend nieuws/updates), maakt de nieuwsbrief geen commercieel bericht.

11.2.5.Waar moet ik verder aan denken? Informeren & opt-out!

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

11.2.6.Ik maak gebruik van een externe partij voor het versturen van mailings, wat nu?

Voor het versturen van direct-marketing-berichten mag je uiteraard een externe partij inschakelen. Meestal zijn dit online dienstverleners (denk bijvoorbeeld aan MailChimp, Laposta, Mailerlite, etc.). Deze derde wordt meestal aangemerkt als verwerker en mag alleen berichten versturen in naam en in opdracht van jouw sportorganisatie. Zorg dat je als sportorganisatie met zulke dienstverleners een verwerkersovereenkomst sluit.

Let op! Deze online dienstverleners kunnen mogelijk privacy risico's opleveren. MailChimp bijvoorbeeld plaatst trackers in verzonden e-mails. Die trackers halen informatie op over wie/wanneer/hoe de e-mail wordt gelezen. Deze tracking informatie wordt ook voor eigen doeleinden van Mailchimp gebruikt. MailChimp is dan gedeeltelijk een verwerkingsverantwoordelijke. Lees daarom voor het gebruik de privacy informatie die de online dienstverlener ter beschikking stelt en bepaal of daar privacyrisico's inzitten die wellicht niet acceptabel zijn voor jouw sportorganisatie. Laat dit bij twijfel toetsen door een expert.

11.2.7. Hoe zit het met telefonische direct marketing?

Voor telefonische direct marketing geldt een opt-in systeem in Nederland. Dat betekent dat je toestemming nodig hebt voordat je een telemarketing gesprek kunt voeren. Deze toestemming geldt voor zowel consumenten als ondernemingen zonder rechtspersoonlijkheid (zoals een eenmanszaak). Let op: hiervoor gelden in principe dezelfde toestemmings-eisen zoals je hebt kunnen lezen in het onderdeel 'Basisregels'.

Er gelden drie uitzonderingen. In onderstaande situaties heb je géén voorafgaande toestemming nodig:

- Als de ontvanger een telefoonnummer heeft dat specifiek bestemd is voor het ontvangen van telemarketing gesprekken. De ontvanger moet dan wel bekend hebben gemaakt dat het telefoonnummer specifiek daarvoor bestemd is (bijvoorbeeld op zijn/haar website). Let op, vaak is de ontvanger een natuurlijk persoon die handelt in uitoefening van een beroep of bedrijf. Immers, een reguliere sporter zal niet over een dergelijk telefoonnummer beschikken!
- Als de bellende partij kan aantonen dat hij/zij het telefoonnummer heeft gekregen van een klant in het kader van de verkoop van een product/dienst en als hij/zij het gesprek gebruikt voor het overbrengen van communicatie voor eigen soortgelijke producten of diensten. Het gaat hier om dezelfde bestaande klant uitzondering zoals je hierboven al hebt kunnen lezen in het onderdeel over het versturen van (commerciële) berichten.
- Als de ontvanger buiten de EER is gevestigd.

Let op! Voorheen was er sprake van een opt-out systeem voor telemarketing (Bel Me Niet Register). Dat is nu niet meer van toepassing.

11.3. Sociale media

Een sportorganisatie met een social media account is verwerkingsverantwoordelijke voor de persoonsgegevens die via dat platform worden verwerkt. Als gebruikers van het platform op eigen initiatief persoonsgegevens delen, dan zijn die gebruikers daarvoor ook zelf verantwoordelijk.

Sociale media bieden vaak de mogelijkheid om gebruikers gericht te benaderen met aanbiedingen of reclame. Als dit via persoonlijke berichten gebeurt, valt dit meestal onder de strenge regels voor direct marketing en heb je hiervoor dus toestemming nodig. In die zin verschilt sociale media niet van een clubblad of een website.

11.3.1. Wat als ik een fanpage heb?

Als je als sportvereniging een fanpage in beheer hebt (bijvoorbeeld via Facebook), dan ben je samen met Facebook verantwoordelijk voor de naleving van de AVG. In AVG termen heet dat gezamenlijke verwerkingsverantwoordelijken (zie ook 'Basisregels').

Als je een fanpage hebt of een andere sociale media pagina dan moet je dit als organisatie melden in jouw privacyverklaring. Neem daarbij op welke persoonsgegevens op sociale media worden verwerkt. Je moet in die privacyverklaring ook opnemen bij wie betrokkenen hun rechten kunnen uitoefenen.

Tip: Op de website van het sociale media platform is meer informatie te vinden over het zijn van gemeenschappelijke verantwoordelijken. Op grond van artikel 26 AVG moet je met het sociale media platform afspraken maken over de onderlinge verantwoordelijkheden naar de betrokkene toe. Facebook biedt hiervoor bijvoorbeeld een Controller Addendum aan, zie externe links.

Case: Facebook pagina's
Het Hof van Justitie van de EU heeft op 5 juni 2018 een uitspraak gedaan over Facebook-pagina's. Omdat de paginabeheerder het doel van de verwerking kan bepalen is zij mede verwerkingsverantwoordelijke samen met Facebook. De beheerder bepaalt immers: de instellingen van de pagina, filters voor statistieken, of zij wel/niet demografische gegevens wilt ontvangen over de gebruikers van de pagina en kan advertenties/promoties toespitsen op de demografische kenmerken van bezoekers van zijn/haar pagina. Omdat de beheerder beïnvloedt welke gegevens Facebook verwerkt, maakt dat de beheerder medeverantwoordelijk. Niet relevant is dat de paginabeheerder enkel geanonimiseerde statistieken ontvangt.

11.3.2. Wat als ik gericht wil adverteren?

In plaats van het direct benaderen van personen kan de doelgroep ook worden bereikt via advertentietools die het sociale platform (zoals Facebook, Instagram en Twitter) zelf aanbiedt. Je levert dan persoonsgegevens of publiekscriteria aan. Deze gegevens worden door het platform gelinkt aan informatie die zij zelf al bezit over haar gebruikers. Wanneer een (potentieel) lid bijvoorbeeld een account heeft op het platform, dan kunnen aan die persoon bepaalde advertenties van de sportorganisatie getoond worden. Let op, een belangrijk nuance verschil:

- Ga je actief e-mailadressen uploaden op het sociale platform zodat je deze personen via sociale media kunt benaderen? Dan heb je daarvoor toestemming nodig (dat kan onderdeel zijn van je toestemming voor direct marketing, maar dan moet je dat wel vermelden in je toestemmingsvraag);
- Ga je op basis van (demografische) kenmerken personen via sociale media benaderen (zonder dat je in feite weet wie deze personen zijn)? Dan kun je dat mogelijk doen op grond van het gerechtvaardigd belang van de sportorganisatie.

11.4. Winacties

Als sportorganisatie kan je gebruik maken van winacties voor de promotie van eigen producten of diensten. Een winactie kan aangemerkt worden als promotioneel kansspel, waarbij een prijs wordt gegeven 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, zie externe links.

De Gedragscode promotionele kansspelen bevat ook een paar bijzondere regels voor het verwerken van persoonsgegevens, namelijk:

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

Uiteraard moet de verantwoordelijke organisator alle algemene regels voor het verwerken van persoonsgegevens in acht nemen, zie daarover het onderdeel 'Basisregels'.

Een belangrijke verplichting specifiek bij winacties is dat je de betrokkene voldoende informeert, bijvoorbeeld over:

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

Voorbeeld: winactie eigen product/dienst (bijvoorbeeld: zomerse tenniscursus)
Vaak gebruiken sportorganisaties winacties met twee doelen. Ze willen (1) hun naamsbekendheid vergroten en (2) personen op de mailinglijst kunnen zetten (voor commerciële berichten). In je communicatie moet dan helder zijn wat je moet doen om kans te maken op de zomerse tenniscursus, bijvoorbeeld: 'schrijf je in voor de nieuwsbrief & doe mee met de winactie'. Zorg in ieder geval dat:

- Je de juiste opt-in hebt voor het adverteren/versturen van de winactie (zie eerste onderdeel);
- Je alleen benodigde informatie opvraagt (data minimalisatie);
- Je een link naar de actievoorwaarden opneemt (die moet worden geaccepteerd);
- Je een link naar een privacyverklaring opneemt (die hoeft niet te worden geaccepteerd, tenzij je dit verwerkt in je actievoorwaarden);
- Indien je een opt-in vraag toevoegt, dan moet deze voldoen aan de eisen omtrent toestemming. Om de vrijwilligheid te behouden is het daarom beter te formuleren 'schrijf je in voor de nieuwsbrief & doe mee' dan 'doe mee & maak kans op'.

Het is in de praktijk vaak handig om deze informatie op te nemen in de actievoorwaarden, met daarin een specifieke alinea 'verwerking van persoonsgegevens'.

Let op! Bedenk goed op welke manier je de winactie verspreidt (via de nieuwsbrief of via sociale media). Want ook hierbij gelden de SPAM-verbod regels. De winactie zelf zal steeds moeten voldoen aan de Gedragscode.

11.5. 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 veelal bekend als de cookiewet. Waarom die naam? Omdat een cookie het bekendste voorbeeld is van het digitaal uitlezen en plaatsen van informatie. Let op: deze regels gelden ook voor andere technieken waarbij informatie wordt uitgelezen of geplaatst.

11.5.1. Wat zijn cookies?

'Cookies' is een veel gebruikte term voor middelen die door een websitehouder kunnen worden gebruikt om informatie te plaatsen op de computer, tablet of mobiele telefoon van een websitebezoeker om informatie van deze apparatuur te halen. Het kan hierbij bijvoorbeeld gaan om kleine tekstbestanden die worden opgeslagen op de apparatuur van de websitebezoeker. Andere voorbeelden zijn het verzamelen van browser informatie over de bezoeker (ook wel Browser finger printing) of het gebruik van Web beacons (kleine afbeeldingen op een webpagina die een bericht sturen naar een server als de afbeelding in de browser wordt geladen van de bezoeker). Cookies worden veelvuldig gebruikt.

Cookies kunnen gebruikers langs verschillende websites volgen en maken daarmee 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. Deze cookieregels zijn van toepassing als je informatie plaatst op de computer of de mobiele telefoon van een bezoeker of als je informatie daarvan af haalt.

11.5.2.Welke soorten cookies zijn er?

Cookies zijn grofweg onder te verdelen in drie categorieën:

- **Technisch noodzakelijke cookies:** dit zijn cookies die nodig zijn om de website (beter) te laten functioneren (ook wel functionele cookies genoemd). Denk aan cookies die een winkelwagentje van een webwinkel mogelijk maken. Immers, zou een order spontaan worden vergeten, dan zou het plaatsen van een bestelling al snel onwerkbaar worden.
- **Analytische cookies:** dit zijn cookies die worden gebruikt om beter inzicht te krijgen in het functioneren van de website. Denk aan cookies om bezoekersstatistieken bij te houden of om A/B testing te kunnen doen.
- **Tracking cookies:** dit zijn cookies die het internetgedrag (tijdens het websitebezoek, maar soms ook erna) van de gebruiker volgen. Denk aan cookies die individueel surfgedrag in de gaten houden en zo een interesse-profiel opstellen om op basis daarvan gerichte advertenties mogelijk te maken. Tracking cookies kunnen eigen cookies zijn of cookies van derden. Hieronder categoriseren we ook sociale media cookies van sociale media partijen.

Let op! Affiliate cookies vallen ook onder de categorie analytische cookies. Hiermee kan een adverteerder bijvoorbeeld bijhouden welke advertentie daadwerkelijk tot de aankoop van een product heeft geleid. Deze cookies dien je te behandelen als ‘analytische cookies met privacygevolgen’. Lees hieronder verder.

11.5.3.Verwerk ik dan persoonsgegevens als ik cookies gebruik?

Ja, vaak wel. Bij het plaatsen en uitlezen van de cookies kunnen namelijk diverse gegevens worden verzameld, zoals IP-adressen, informatie over eerder bezochte websites, informatie over de randapparatuur, etc. Er zijn behoorlijk wat zaken waar je aan moet denken bij het plaatsen van cookies. We hebben ze hieronder opgedeeld in vier stappen.

Stap 1: beoordeel of je de gebruiker wel/niet om toestemming moet vragen

Of je de gebruiker enkel hoeft te informeren over het plaatsen van cookies of dat je de gebruiker ook daadwerkelijk om toestemming moet vragen voor het plaatsen van cookies, hangt af van het type cookie. In principe komt het neer op het volgende:

- ➔ Voor het plaatsen van technisch noodzakelijke en analytische cookies geldt alleen de informatieplicht. Je bent als website eigenaar verplicht de gebruiker hierover te informeren. Je hoeft de gebruiker voor technisch noodzakelijke en analytische cookies niet om toestemming te vragen, mits het cookie geen of slechts geringe gevolgen heeft voor de privacy van de gebruiker.
- ➔ Voor het plaatsen van tracking cookies (of van analytische cookies met privacygevolgen) ben je als website eigenaar verplicht om (1) de gebruiker hierover te informeren en (2) de gebruiker om toestemming te vragen voor het plaatsen van cookies. Die toestemming moet te weigeren zijn zonder dat iemand van de site wordt geweerd.

Tip: Als je gebruik maakt van sociale media buttons op je website, dan kun je het beste werken met niet-actieve sociale media knoppen. De gebruiker maakt dan zelf bewust een keuze door te klikken op de grijze knoppen en geeft daarbij indirect toestemming. De informatieplicht blijft natuurlijk bestaan.

Stap 2: website gebruiker om toestemming vragen

De gebruiker moet zijn/haar toestemming geven voordat cookies mogen worden geplaatst. Dat betekent ook dat je de gebruiker vooraf duidelijk moet informeren over de doeleinden en de werking van de cookies. Vertel daarbij:

- Welke informatie je verzamelt;
- Hoe je de informatie verzamelt (cookies/scripts/beacons); en
- Wat je met de informatie doet.

Geef gebruikers de keuze om ermee in te stemmen dat cookies worden geplaatst, of dit te weigeren. Let op: hiervoor gelden in principe dezelfde toestemmingseisen die beschreven staan in het onderdeel basisregels.

Voorbeeld: cookies plaatsen op www.sportorganisatie.nl
Stel een website plaatst technisch noodzakelijke cookies en tracking cookies. De website dient de gebruiker om toestemming te vragen voor de tracking cookies. Deze mogen pas geplaatst worden op het moment dat iemand deze toestemming ook daadwerkelijk geeft. Voordat de toestemming is gegeven, mag de website wel al de technisch noodzakelijke cookies plaatsen. Immers, daarvoor is geen toestemming vereist. De informatie neem je op in de cookieverklaring of privacyverklaring.

Let op! De AP heeft bepaald dat Google Analytics, dat door veel bedrijven en organisaties wordt gebruikt om analyses te doen over het website bezoek gevolgen heeft voor de privacy van de gebruiker. Dat zou eigenlijk betekenen dat je de gebruiker toch om toestemming moet vragen wanneer je Google Analytics gebruikt. Houd de website van de AP in de gaten voor ontwikkelingen omtrent het gebruik van Google Analytics.

Stap 3: website gebruiker informeren
Ongeacht welke cookies je plaatst, je moet de gebruiker vooraf altijd duidelijk informeren over de doeleinden en werking van cookies. Je geeft hierbij in ieder geval de volgende informatie:

- Type cookies die door of via de website worden geplaatst (hiervoor kun je bovengenoemde categorieën gebruiken) en het gebruik van eventuele andere technieken;
- De categorieën van persoonsgegevens die via de cookies verzamelt en verwerkt worden (bijvoorbeeld: bezochte web-pagina's, IP-adressen, etc.);
- De doeleinden waarvoor de cookies worden gebruikt (denk bijvoorbeeld aan tracking, advertenties tonen en het verbeteren van de website);
- De categorieën bedrijven waaraan je de gegevens verstrekt (indien je cookies van derden plaatst);
- De bewaartermijn;
- Overige noodzakelijke informatie om een zo eerlijk mogelijk beeld te schetsen voor de gebruiker.

Je kunt de gebruiker hierover informeren door een paragraaf op te nemen in de privacyverklaring van de website of door een aparte cookieverklaring op te stellen.

Stap 4: een verwerkersovereenkomst sluiten
Als er derde partijen betrokken zijn bij het verwerken van persoonsgegevens voor je sportorganisatie dan is deze derde vaak een verwerker, bijvoorbeeld Google Analytics. In dat geval moet je een verwerkersovereenkomst sluiten. Vaak kun je dit bij derde partijen zoals Google terugvinden in je account (specifiek voor Google geldt: zie de handleiding van de AP – daarin staat uitgelegd hoe je een verwerkersovereenkomst kunt afsluiten met Google).

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. Zie externe links.

11.5.4.Heb ik een duidelijk doel en geldige grondslag voor het delen van de gegevens?
Indien je ledengegevens wilt delen met sponsoren vanwege commerciële doeleinden (= doel) dan heb je daar een geldige grondslag voor nodig. Omdat het delen van ledengegevens met sponsoren geen noodzakelijke verwerking is voor het lidmaatschap kun je geen gebruik maken van de grondslag 'overeenkomst'. Dat betekent dat je moet beoordelen of je hier een gerechtvaardigd belang voor hebt. Zo niet, dan moet je het lid om uitdrukkelijke toestemming vragen.

Let op! De AP is van mening dat een zuiver commercieel belang (waaronder dus extra inkomsten willen werven) nooit een gerechtvaardigd belang kan zijn. Op Europees niveau (vanuit de European Data Protection Board) geldt het uitgangspunt dat dit wél als gerechtvaardigd belang kan kwalificeren (namelijk: feitelijke, economische en ideële belangen). Zie hieronder de KNLTB case kort toegelicht; deze illustreert de zienswijze van de AP. Op dit moment kunnen we je helaas niet adviseren over het wel/niet gebruik maken van een gerechtvaardigd belang als je daarmee inkomsten wilt werven (en dus een commercieel belang hebt). Wil je hier ondanks de stellingname van de AP wel gebruik van maken? Gebruik dan het template voor het uitvoeren van de belangentoets. Liever op zeker spelen? Vraag dan gewoon om uitdrukkelijke toestemming. En uiteraard: houd de discussie in de gaten.

Tip: Bedenk wat je er zelf van zou vinden als jouw gegevens worden gedeeld met een sponsor voor commerciële doeleinden: wat vind je nog oké en wat vind je niet meer oké?

Case: KNLTB
Op 20 december 2019 heeft de AP de KNLTB een boete opgelegd van € 525.000,00 voor een schending van de AVG. Waarom? Omdat de AP stelt dat de KNLTB onrechtmatig persoonsgegevens van leden heeft verstrekt aan twee sponsoren. Het ging om een bestand van 300.000 leden en een bestand van 50.000 leden.

Wat was de zienswijze van de KNLTB?
De KNLTB vond dat zij een gerechtvaardigd belang had bij het doorverkopen van de persoonsgegevens, namelijk meerwaarde creëren voor het lidmaatschap en extra inkomsten verkrijgen ter compensatie van dalende contributie inkomsten door teruglopende ledenaantallen.

Wat was de visie van de AP?
Het verzamelen van de verstrekte ledengegevens was rechtmatig, omdat deze noodzakelijk waren om lid te worden van de KNLTB. Echter, het vervolgens verstrekken van deze ledengegevens aan derden voor commerciële doeleinden was volgens de AP onrechtmatig. De AP stelde dat de KNLTB hiervoor geen afdoende toestemming had gevraagd, er geen sprake was van een verenigbaar doeleinde en er ook geen sprake was van een gerechtvaardigd belang, omdat het hier zou gaan om een zuiver commercieel belang.

De KNLTB is in hoger beroep gegaan tegen het boetebesluit. Wellicht is de uitspraak al bekend op het moment dat je dit handboek leest.

11.5.5.Heb ik vooraf geïnformeerd?

Indien je een doel en grondslag hebt geformuleerd voor het delen van persoonsgegevens met sponsoren voor marketingdoeleinden zorg dan dat je de leden hier vooraf goed over informeert. Dat doe je op het moment dat je toestemming vraagt. Je kunt dit verder toelichten in de privacyverklaring van je sportorganisatie (waar je naar verwijst op het inschrijfformulier).

Maak je gebruik van de grondslag gerechtvaardigd belang? Dan moet je de leden waarvan je persoonsgegevens verstrekt, informeren over het recht van verzet tegen de verstrekking. Dat betekent dat leden gedurende een bepaalde periode eenvoudig bezwaar moeten kunnen maken tegen de verstrekken. Je moet dit recht van verzet aanbieden voordat de verwerking plaatsvindt. Als sportorganisatie kun je je leden daarover informeren via bijvoorbeeld een e-mail, een bericht in het clubblad of op de eigen website.

11.5.6.Waar moet ik verder aan denken?

Indien je gegevens aan een derde verstrekt voor commerciële doeleinden, zorg dan dat je alleen die gegevens verstrekt die nodig zijn om je doel te bereiken. Zorg er ook voor dat je de gegevens op een veilige manier verstrekt en dat je een duidelijk kader afspreekt met de sponsor (dus: wat mag de sponsor er wel/niet mee doen). Documenteer je afspraken en je belangentoets (indien je gebruik maakt van het gerechtvaardigd belang).

Externe links	Uitleg
Website DDMA	De DDMA (Data Driven Marketing Association) is een vereniging voor marketing en data. Hier vind je informatie over het inzetten van data om relevant te kunnen communiceren.
Facebook Controller Addendum	Hier vind je het Controller Addendum van Facebook.
Gedragscode promotionele kansspelen	In deze Gedragscode lees je waar je aan moet voldoen bij de inzet van promotionele kansspelen (denk aan like&win-acties).
Handleiding privacyvriendelijk instellen Google Analytics	In deze handleiding van de AP lees je hoe je Google Analytics privacyvriendelijk kunt instellen en waar je verder op moet letten.
Website ACM	Op deze webpagina van de ACM (Autoriteit Consument & Markt) lees je over het gebruik van cookies in allerlei praktijksituaties.
Case KNLTB	Hier vind je de samenvatting van de AP over de KNLTB case.

ONDERDEEL BEELDMATERIAAL

12. Beeldmateriaal

12.1. Inleiding

Voor foto's en videobeelden (hierna ook: beeldmateriaal) die je publiceert gelden niet alleen de privacy-regels, maar geldt ook het portretrecht. Daarmee kan de geportretteerde zich mogelijk verzetten tegen de publicatie van beeldmateriaal waarop hij of zij herkenbaar in beeld wordt gebracht. Het portretrecht beperkt het auteursrecht van de maker van het beeldmateriaal. De maker mag beelden niet verspreiden en/of verkopen als de geportretteerde zich op grond van het portretrecht daartegen verzet.

Laten we eerst eens kijken naar wat je wel/niet kunt met beeldmateriaal vanuit een privacyperspectief. Vervolgens geven we aan waar je nog meer op moet letten vanuit het portretrecht.

12.2. Privacy en de publicatie van beeldmateriaal

Beeldmateriaal van herkenbaar in beeld gebrachte personen kwalificeert meestal als een persoonsgegeven en heel soms zelfs een bijzonder persoonsgegeven. Een sportorganisatie die beeldmateriaal publiceert dat als persoonsgegeven wordt aangemerkt, is daarvoor verwerkingsverantwoordelijke.

Publiceer je als sportorganisatie beeldmateriaal van niet herkenbaar in beeld gebrachte personen? Dan is het niet te herleiden tot één persoon, betreft het geen persoonsgegeven en is de AVG dus ook niet van toepassing.

Let op! De AP geeft aan dat een herkenbaar postuur of een herkenbare houding al genoeg kan zijn om iemand te identificeren. Je kunt er vrijwel altijd van uitgaan dat personen op foto's en filmpjes identificeerbaar zijn.

12.2.1. Is mijn beeldmateriaal een bijzonder persoonsgegeven?

Een tijd lang bestond er twijfel over het feit of beeldmateriaal een bijzonder persoonsgegeven is als je daaruit ras, geloof, etc. kunt aflezen. De AP heeft daarover duidelijkheid gegeven: beeldmateriaal is meestal geen bijzonder persoonsgegeven, zolang je niet het doel hebt om op basis van het beeldmaterieel onderscheid te maken naar ras of geloof. Meestal zal dit niet het doel zijn bij een publicatie door een sportorganisatie. De striktere regels voor bijzondere persoonsgegevens zijn in dat geval niet van toepassing.

12.2.2. Heb ik een doel en grondslag nodig voor het maken en publiceren van beeldmateriaal? En hoe informeer ik hierover?

Ja, meestal wel, maar welk doel en welke grondslag van toepassing is hangt af van wat je met het beeldmateriaal wilt doen.

Beeldmateriaal dat wordt gebruikt om de sportprestaties te verbeteren

Beeldmateriaal dat wordt gebruikt om sportprestaties te analyseren en verbeteren kan bijvoorbeeld nodig zijn voor de uitvoering van de overeenkomst (=grondslag) (immers: de sporter wil beter worden, het beeldmateriaal is een tool om daaraan bij te dragen). In de meeste gevallen kun je dat doel behalen door alleen het maken en analyseren van het materiaal, zonder publicatie van gegevens. Wil je het beeldmateriaal toch publiceren, maar is het feitelijk niet nodig voor de uitvoering van de overeenkomst, dan heb je daarvoor een andere grondslag nodig (lees hieronder verder).

Je hebt altijd de verplichting de sporter te informeren. Dit kun je doen met de algemene privacyverklaring.

Beeldmateriaal van een sportevenement/sportwedstrijd

Beeldmateriaal van sporters en toeschouwers publiceren kan op meerdere grondslagen worden gebaseerd. Indien dit praktisch haalbaar is, kun je ervoor kiezen om hiervoor toestemming te vragen. Vaak is dat echter onpraktisch en dus ook onwenselijk. Dan kun je beoordelen of je een beroep kunt doen op het gerechtvaardigd belang. Dat belang kan zijn: persvrijheid, promotie van de sport of de vereniging/bond, wedstrijdverslaglegging of beveiliging. Wellicht kun je zelfs gebruik maken van de journalistieke uitzondering. Zo kan een fotoverslag van een sportwedstrijd al gauw een journalistiek doel hebben. In dat geval heb je dus geen toestemming nodig en mag je de beelden wel publiceren.

Let op! Als je gebruik maakt van de grondslag 'gerechtvaardigd belang' dan dien je een zorgvuldige belangenafweging te maken (zie template): het belang van de sportorganisatie versus het belang van betrokkenen. Bij de afweging kunnen diverse factoren een rol spelen, bijvoorbeeld hoe groot is het publiek aan wie je publiceert en betreft het ook minderjarigen? Bedenk vooraf goed welke mogelijke negatieve gevolgen er voor een minderjarige aan publicatie van foto's en beelden kunnen kleven. Lees ook de case VoetbalTV hieronder.

Hoe informeer ik?
Je hebt altijd de verplichting om de aanwezigen te informeren. Maak je bijvoorbeeld gebruik van camera's, dan moet dat duidelijk aangegeven worden. Je moet personen hierover informeren vóórdat ze gefilmd worden. Dat kan bijvoorbeeld met een bordje bij de ingang van een evenementlocatie, in wedstrijdreglementen, in huishoudelijke reglementen en/of in de ticketvoorwaarden.

Let op! Beeldmateriaal van sporters en toeschouwers gebruiken voor zuiver commerciële doeleinden kan alleen als je daarvoor toestemming hebt. Is het praktisch onhaalbaar om toestemming te vragen? Dan kun je ook hier beoordelen of je een beroep kunt doen op het gerechtvaardigd belang.
De AP is van mening dat een commercieel belang nooit een gerechtvaardigd belang kan zijn. Op Europees niveau (vanuit de European Data Protection Board) geldt het uitgangspunt dat deze wél als gerechtvaardigd belang kan kwalificeren (namelijk: feitelijke, economische en ideële belangen). Zie hierover ook case VoetbalTV.

Case: VoetbalTV
Op 16 juli 2020 heeft de AP VoetbalTV een boete opgelegd van € 575.000,00 voor een schending van de AVG. Waarom? Omdat de AP stelt dat VoetbalTV zonder geldige grondslag videopnamen van voetbalwedstrijden heeft gemaakt en deze beelden verder heeft verspreid.

VoetbalTV was een platform (een samenwerkingsverband tussen KNVB en Talpa Network) waar voetbalwedstrijden op amateurniveau (waaronder ook jeugdwedstrijden) live konden worden gestreamd.

Wat was de visie van de AP?
VoetbalTV heeft volgens de AP geen geldige grondslag. VoetbalTV heeft geen toestemming gevraagd en er kan volgens de AP ook geen sprake zijn van een gerechtvaardigd belang, omdat het hier zou gaan om een zuiver commercieel belang. Om die reden was de verwerking volgens de AP onrechtmatig.

Het boetebesluit is vernietigd door de rechtbank en vervolgens in hoger beroep door de Raad van State omdat de AP is uitgegaan van een verkeerde interpretatie van het begrip 'gerechtvaardigd belang'.

Hoe informeer ik?
Je bent altijd verplicht om betrokkenen te informeren. Je moet personen informeren vóórdat ze herkenbaar op beeldmateriaal verschijnen. Dat kan bijvoorbeeld met een bordje bij de ingang van een evenementlocatie, in het wedstrijdreglement, in een huishoudelijk reglement en/of in de ticketvoorwaarden.

12.3. Het portretrecht en de publicatie van beeldmateriaal

Personen die herkenbaar in beeld worden gebracht, kunnen zich soms beroepen op het portretrecht uit de Auteurswet. Volgens deze wet is een portret een afbeelding van het gelaat van een persoon. De geportretteerde heeft het recht om zich (in sommige gevallen) te verzetten tegen publicatie van een beeldopname. Het maakt daarbij uit of de portretten in opdracht zijn gemaakt, of niet. Teamfoto's en individuele spelersfoto's die op aanvraag van of namens de geportretteerde door een fotograaf zijn gemaakt, zijn voorbeelden van portretten die in opdracht zijn gemaakt. Wil je deze portretten publiceren? Dan heb je daarvoor 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 raadzaam daar standaard op te vertrouwen. Als een geportretteerde later toch bezwaar maakt tegen publicatie, sta je met lege handen.

Let op! Als je toestemming krijgt, dan geldt die toestemming ook als een verwerkingsgrondslag, maar alleen als de toestemming voldoet aan de eisen van de AVG. Zie voor die eisen het onderdeel 'Basisregels'.

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 het meest wenselijk, voor zover dat in de praktijk uitvoerbaar is. Vaak kun je dit op voorhand oplossen door de betrokkene om toestemming te vragen op het inschrijfformulier (bijvoorbeeld: "ja, ik ga akkoord met de publicatie van…").

Voor portretten die niet in opdracht zijn gemaakt, geldt dat je voor het publiceren van deze portretten in principe geen toestemming nodig hebt. Wel dien je een belangenafweging te maken. Het belang van het recht op vrijheid van meningsuiting en informatie van de fotograaf/publicerende partij tegenover het privacybelang van de betrokkene. Een geportretteerde kan zich namelijk verzetten tegen publicatie van beeldmateriaal als hij/zij hiervoor een redelijk belang heeft. Of een redelijk belang van een sporter voldoende zwaarwegend is, hangt af van de afweging van dat belang ten opzichte van het publicatiebelang.

Tip: Hoe beoordeel je dat nu? Je kunt de volgende vuistregel hanteren: indien publicatie van een foto inbreuk maakt op iemands privacy of hem/haar in een negatieve of gevaarlijke context laat zien, dan kan de geportretteerde een redelijk belang hebben. Bedenk dan vooraf of je het beeldmateriaal wel wilt publiceren. Je moet je immers bewust zijn van een mogelijke uitoefening van het portretrecht.

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.

Tips:

- 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 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 wilt gebruiken. Wordt achteraf bezwaar gemaakt tegen publicatie, dan moet je dit respecteren en (voor zover mogelijk) de publicatie verwijderen;

- Een persoon kan alleen beroep doen op zijn/haar commercieel belang als hij/zij een zogenaamde 'verzilverbare populariteit' heeft. Het zou immers onredelijk zijn als een organisatie geld kan verdienen, simpelweg door het publiceren van een foto van een bekende sporter. Sporters kunnen zich daarom 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 op met het publiceren van afbeeldingen van sporters met een aanzienlijke populariteit;
- Onthoud dat je in de praktijk altijd een belangenafweging moet maken. Je bepaalt eerst of er een redelijk belang is van de geportretteerde. Als dat duidelijk is, dan kijk je wat het belang bij publicatie van de foto of video is. Om publicatie mogelijk te maken moet dat laatste belang zwaarder wegen. Ontstaat er op enig moment discussie met een geportretteerde over zijn/haar belang of over de gemaakte belangenafweging, win dan juridisch advies in.

Externe links	**Uitleg**
Website AP	Op deze webpagina van de AP lees je meer over het maken en publiceren van beeldmateriaal.

Template(s)	**Uitleg**
Toetsingskader gerechtvaardigd belang	Dit toetsingskader is te gebruiken als invuldocument voor jou als verwerkingsverantwoordelijke om te beoordelen of je verwerking rechtmatig is.

ONDERDEEL WEBWINKELS

13. Webwinkels

13.1. Inleiding

Sommige sportorganisaties verkopen online tickets en producten. Bij die verkoopprocessen worden persoonsgegevens verwerkt. Deze verwerkingen moeten uiteraard voldoen aan alle regels die zijn opgenomen in het onderdeel 'Basisregels'. In dit onderdeel lichten we enkele specifieke aandachtspunten rondom het verkoopproces in webwinkels toe.

13.2. Ben ik verwerker of verwerkingsverantwoordelijke?

Het antwoord op de vraag of de online verkoopactiviteiten, geheel of gedeeltelijk, zijn uitbesteed aan derden is belangrijk om te bepalen wie verwerkingsverantwoordelijke is. Vooral bij online verkoopkanalen laten veel sportorganisaties hun verkoopactiviteiten uitvoeren door een derde. De webshop draagt vaak een naam die sterk is gerelateerd aan de sportorganisatie, maar in feite is het de leverancier die het (verkoop)proces inricht en uitvoert. Bij volledige uitbesteding (waarbij de leverancier handelt op eigen naam en rekening) is de leverancier meestal zelf verwerkingsverantwoordelijke. Beperkt de bemoeienis van de leverancier zich tot het technisch beheer van de webshop en regelt de sportorganisatie zelf de overige processen (verzending, incasseren van betalingen, etc.), dan is de sportorganisatie waarschijnlijk verwerkingsverantwoordelijke. De leverancier is in dat laatste geval verwerker, zodat daarmee in ieder geval een verwerkersovereenkomst moet worden gesloten. Enkel in uitzonderlijke gevallen is er sprake van een gezamenlijke verantwoordelijkheid.

13.3. Heb ik een doel en grondslag?

Voor het afhandelen van bestellingen (= doel) verwerkt de verkoper voornamelijk informatie in de volgende categorieën: voor- en achternaam, contactgegevens, adresgegevens, ordergegevens en betalingsgegevens. De verkopende organisatie mag deze gegevens verwerken op grond van de uitvoering van een overeenkomst (= grondslag). Immers: zonder deze gegevens wordt het erg lastig om het bestelproces te voltooien. Voor de verwerking van deze gegevens hoef je dus geen toestemming te vragen.

Let op! Bovengenoemde geldt alleen zolang deze gegevens noodzakelijk zijn voor het bestelproces én alleen voor dat doel worden gebruikt (het afhandelen van bestellingen). Wil je de contactgegevens van bestaande klanten in de toekomst gebruiken om een commerciële aanbieding te sturen aan die klant, dan is dat een ander doel. Hiervoor heb je een andere grondslag nodig. Meer over commerciële aanbiedingen en de juiste grondslag daarvoor lees je in het onderdeel 'Marketing'.

Tip: Voorkom dat websitebezoekers zich moeten registreren met een account voordat ze een bestelling kunnen plaatsen. Als een klant namelijk alleen (eenmalig) een ticket of product wil bestellen, is de eis om je daarvoor te moeten registreren vrij onredelijk (immers: zit je er zelf op te wachten om steeds een account aan te maken als je eenmalig een product wilt bestellen?). Uiteraard kun je klanten van jouw webshop wel de mogelijkheid geven een account aan te maken. Bij voorkeur heb je dan twee opties: inloggen met een account of het verrichten van een eenmalige bestelling (gastaccount). Om een klant over te halen een account aan te maken kan je uiteraard aangeven wat de voordelen van een account zijn. Denk bijvoorbeeld aan het bijhouden van een bestelgeschiedenis indien de website bezoeker verwacht meerdere aankopen te doen.

Hoe informeer ik?

De verwerkingsverantwoordelijke is verplicht de betrokkene goed te informeren over de wijze waarop de persoonsgegevens worden verwerkt. Voor bezoekers van webwinkels kun je daarvoor een privacyverklaring gebruiken, die je duidelijk zichtbaar op de website plaatst (bijvoorbeeld in de footer van iedere pagina van de website). Het is verstandig om bezoekers die daadwerkelijk een bestelling plaatsen nog eens expliciet te

wijzen op de privacyverklaring, aangezien juist van deze groep de meeste gegevens worden verwerkt. Verwijs tijdens het bestelproces dan ook naar de privacyverklaring met een hyperlink. De bezoeker hoeft deze privacyverklaring niet te accepteren, het is enkel ter info (een veelvoorkomend misverstand).

Welke beveiliging pas ik toe?
Bij online verkoopactiviteiten is het erg belangrijk dat persoonsgegevens passend worden beveiligd tegen datalekken. Betaalgegevens van klanten zijn immers extra interessant voor kwaadwillende personen. Als je voor het technisch beheer van de webwinkel een externe IT-leverancier inschakelt, controleer dan goed welke beveiligingsmaatregelen ze toepassen. Afspraken hierover zijn onderdeel van de verwerkersovereenkomst (lees dit terug in het onderdeel 'Basisregels').

13.4. Hoelang bewaar ik de gegevens?

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. Voor informatie die valt onder de boekhoudkundige en/of fiscale bewaarplicht geldt een langere bewaartermijn. Voor beiden is dat zeven boekjaren.

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. Als je deze doeleinden ook kunt bereiken met geanonimiseerde of gepseudonimiseerde gegevens dan ben je daartoe verplicht.

13.5. Wat als ik gegevens met derden deel?

Worden in het kader van de verkoopactiviteiten persoonsgegevens verstrekt aan derden, dan heb je je te houden aan extra maatregelen. Lees daartoe het onderdeel 'Delen met derden' door.

13.6. Wat als ik gebruik wil maken van direct marketing & cookies?

Bij online verkoop heb je vrijwel altijd te maken met specifieke regelgeving voor cookies en direct marketing. Meer daarover lees je in het onderdeel '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.

Externe links	Uitleg
Algemene wet inzake rijksbelastingen	In artikel 52 van de Algemene wet inzake rijksbelastingen vind je informatie over de administratieplicht en de bijbehorende bewaartermijn.
Burgerlijk Wetboek	In artikel 10 van het Burgerlijk Wetboek vind je informatie over wat een boekjaar is.

ONDERDEEL OPLEIDING

14. Opleidingen

14.1. Inleiding

Bij het opleiden van sporters, scheidsrechters en trainers verwerk je als verantwoordelijke sportorganisatie op allerlei manieren persoonsgegevens. Deze verwerkingen moeten uiteraard voldoen aan alle regels in het onderdeel 'Basisregels'. We geven hieronder een paar specifieke aandachtspunten rondom opleidingen.

14.2. Heb ik een doel en grondslag?

Als je persoonsgegevens verwerkt in het kader van een opleidingsprogramma kun je dat meestal baseren op de uitvoering van een overeenkomst of op een gerechtvaardigd belang (= grondslag). Let op, je mag dan alleen informatie verzamelen die ook echt noodzakelijk is voor het organiseren van de opleiding/het opleidingsprogramma.

Persoonsgegevens die je in het kader van de opleiding in veel gevallen zult verwerken, zijn:

- Deelnemerslijsten;
- Contactgegevens van de cursisten;
- Dieetwensen (alleen als een ontbijt/lunch/diner onderdeel is van het programma);
- Betalingsgegevens;
- Contactgegevens docenten;
- Opleidingsresultaten (waaronder ook certificaten);
- Adresgegevens (indien je bijvoorbeeld een certificaat per post naar het huisadres stuurt);
- Ingeleverd huiswerk.

Let op! Het openbaar publiceren van opleidingsinformatie (denk aan deelnemerslijsten, uitslagen, etc.) kan niet worden gebaseerd op de overeenkomst of het gerechtvaardigd belang. Immers, het is lastig te beargumenteren dat publicatie daarvan noodzakelijk is voor het opleidingsprogramma. Wil je dit wel doen? Zorg dan dat je daarvoor specifiek toestemming vraagt aan de betrokkenen. Je kunt dit bijvoorbeeld vragen op het aanmeldingsformulier.

14.3. Hoe informeer ik?

Zorg dat je cursisten (en eventueel docenten) vooraf informeert over hoe je met hun gegevens omgaat. Dit kun je doen door middel van een privacyverklaring. Je kunt hiernaar verwijzen op het aanmeldformulier (neem bijvoorbeeld een hyperlink op).

14.4. Mag ik de gegevens delen?

In het kader van het opleidingsprogramma kan het nodig zijn om gegevens te delen met derden. Bijvoorbeeld als de docent vooraf alvast een deelnemerslijst wil ontvangen. Vraag jezelf dan wel af of dat op persoonsniveau nodig is en verstrek alleen de noodzakelijke informatie.

Voorbeeld: opleidingsresultaat delen met werkgever
Verstrek een opleidingsresultaat niet zo maar aan de werkgever van de cursist. Normaal gesproken laat je het verstrekken van die informatie over aan de cursist zelf. De cursist kan immers zelf een kopie van het certificaat aan zijn/haar werkgever verstrekken. Als je dit wel doet, zorg er dan voor dat je vooraf toestemming hebt gekregen van de cursist. Deze regel geldt ook als de werkgever (bijvoorbeeld een sportbond) de opdrachtgever is voor de training.

14.5. Welke beveiliging pas ik toe?

Zorg ervoor dat je opleidingsresultaten passend beveiligt. Naast het toepassen van moderne beveiligingstechnieken op je applicatie (waar je de gegevens opslaat) is het van belang om de toegang tot de gegevens te beperken. Immers, niet iedereen binnen de sportorganisatie heeft voldoende belang bij toegang tot opleidingsresultaten. Beperk iemands toegangsrechten dus op basis van zijn taken en verantwoordelijkheden.

14.6. Hoelang bewaar ik de gegevens?

Bewaar opleiding gerelateerde 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 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. Als je deze doeleinden ook kunt bereiken met geanonimiseerde of gepseudonimiseerde gegevens, dan ben je daartoe verplicht.

ONDERDEEL PERSONEEL

15. Personeel

15.1. Inleiding

In dit onderdeel behandelen we de sportorganisatie als werkgever. Vrijwel altijd ben je namelijk ook werkgever en verwerk je persoonsgegevens van werknemers en vrijwilligers. In dit hoofdstuk lichten we toe waar je in het kader van de AVG op moet letten als werkgever.

15.2. Sollicitanten

15.2.1. Heb ik een doel en grondslag?

Het doel van een sollicitatieprocedure is het vaststellen van de geschiktheid van een sollicitant voor de functie. Tijdens deze procedure wil je natuurlijk zoveel mogelijk informatie over het opleidings- en arbeidsverleden van de kandidaat hebben. Daarnaast wil je wellicht kunnen toetsen of een kandidaat betrouwbaar is en of de door de sollicitant verstrekte informatie waarheidsgetrouw is. Het spreekt voor zich dat je de contactgegevens van de sollicitant nodig hebt voor de uitnodiging voor een sollicitatiegesprek. Veel van deze gegevens kun je verzamelen op basis van de sollicitatie door de betrokkene, wat een verzoek tot het aangaan van een vrijwilligersrelatie of een arbeidsovereenkomst is (grondslag = overeenkomst). Referenties kun je opvragen op basis van dezelfde grondslag. Zorg dan wel dat je de eis van referenties opneemt in het gepubliceerde functieprofiel.

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 (meer hierover lees je in het onderdeel ‘Basisregels’).

FAQ: wat mag je wel/niet vragen en naar welke informatie mag je zelf op zoek gaan?

➔ **Mag ik een internetzoekopdracht uitvoeren?**

Dat hangt er vanaf. Er zijn werkgevers die een internetzoekopdracht uitvoeren bij de beoordeling wie wordt uitgenodigd voor een sollicitatiegesprek of ter voorbereiding van dat gesprek. Wanneer je zo’n zoekopdracht uitvoert, bijvoorbeeld op sociale media, vertel dit van tevoren aan de sollicitant (bijvoorbeeld in het functieprofiel of in je privacyverklaring voor sollicitanten) en beperk je 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 deze informatie ook niet op.

➔ **Mag ik iemand vragen naar zijn/haar gezondheid, zwangerschap of kinderwens?**

Nee, het is verboden om en sollicitant vragen te stellen over de gezondheid en/of het 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 alleen onderdeel uitmaken van de sollicitatieprocedure als de functie bijzondere eisen op het punt van medische geschiktheid stelt.

➔ **Mag ik een screening (laten) uitvoeren?**

Dat hangt af van de aard van de functie waarvoor iemand solliciteert en de risico’s die met deze functie samenhangen. We spreken hier overigens over screenings zoals het natrekken van een CV, het verzoeken om een Verklaring Omtrent Gedrag (VOG) en/of het verzamelen van financiële informatie.

Je mag nooit zelf onderzoek doen naar een eventueel strafrechtelijk verleden van de sollicitant. Gebruikelijk is dat je vraagt om een VOG. Als die wordt afgegeven, betekent dat dat de sollicitant in een termijn van vier jaar voorafgaand aan de afgifte van de VOG geen voor de functie relevant strafbaar feit heeft gepleegd. Soms rechtvaardigt de aard van de functie specifiek aanvullend onderzoek. Financiële functies, waarbij een werknemer toegang heeft tot aanzienlijke geldbedragen, kennen bijvoorbeeld een groter risico op fraude of diefstal dan andere functies. Bij dit soort risico's mag je daarom - onder omstandigheden - bijvoorbeeld aan de sollicitant informatie verzoeken over zijn of haar (actuele) financiële positie.

Let op! Toestemming van een sollicitant is in deze gevallen geen geldige grondslag om zijn of haar persoonsgegevens te verwerken. Immers, hoe vrij kan die toestemming gegeven worden? Vaak kun je de screening laten uitvoeren op basis van de overeenkomst (namelijk de precontractuele fase), mits het noodzakelijk is om te beoordelen of iemand een geschikte kandidaat is voor de functie. Neem de screeningseis ook op in het functieprofiel in de advertentie zodat de sollicitant vooraf weet waar hij/zij aan toe is.

15.2.2.Hoe informeer ik?

Zorg dat je sollicitanten vooraf informeert over hoe je met hun gegevens omgaat. Dit kun je doen door middel van een privacyverklaring. Je kunt hiernaar verwijzen op het sollicitatieformulier, neem bijvoorbeeld een hyperlink op. Vergeet daarin niet te informeren over alle verwerkingen die onderdeel uitmaken van de sollicitatieprocedure, zoals bijvoorbeeld een assessment, een medische keuring of een verplicht antecedentenonderzoek.

15.2.3.Mag ik de gegevens delen?

In de meeste gevallen hoef je gegevens van sollicitanten niet te verstrekken aan derden. Wil je dit om welke reden dan ook wel doen, beoordeel dan of je hier een geldig doel en grondslag voor hebt. Meer hierover lees je in het onderdeel 'Het delen van persoonsgegevens'. Zorg er dan ook voor dat je die verstrekking van informatie opneemt in je privacyverklaring.

15.2.4.Hoelang bewaar ik de gegevens?

We maken hier onderscheid in de gegevens van afgewezen sollicitanten en de gegevens van de geselecteerde kandidaat.
Gegevens van afgewezen sollicitanten bewaar je niet langer dan vier weken na het einde van de sollicitatieprocedure. Als de sollicitant daarom vraagt, moet je de gegevens eerder verwijderen. Wil je het dossier langer bewaren dan die vier weken, bijvoorbeeld omdat je iemand in de toekomst wilt benaderen voor soortgelijke functies? Dan moet je daarvoor om toestemming vragen. Die toestemming is geldig voor een periode van maximaal een jaar.

Het kan zo zijn dat het voor jouw sportorganisatie noodzakelijk is om bij te houden dat iemand eerder gesolliciteerd heeft. In dat geval kun je een langere bewaartermijn toepassen en hoef je daarvoor geen toestemming te vragen. Het is belangrijk dat je alleen gegevens bewaart die voor dat specifieke doel noodzakelijk zijn (zoals de naam van de sollicitant, de namen van personen die gesprekken hebben gevoerd en een korte omschrijving zoals de reden van afwijzing). Bewaar dus niet het volledige dossier van de sollicitatieprocedure. Bepaal zelf een passende maximale bewaartermijn voor deze gegevens.

Voor de gegevens van de geselecteerde kandidaat beoordeel je of de verzamelde informatie relevant is om op te nemen in het personeelsdossier. Indien niet relevant, dan verwijder je deze gegevens ook na maximaal vier weken.

Tips:

- Zet aanvullende selectiemiddelen (zoals assessments, screening of antecedentenonderzoeken) pas in een zo laat mogelijk stadium van de sollicitatieprocedure 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 in deze fase (nog) geen kopie maken!

15.3. Medewerkers

In dit onderdeel behandelen we een aantal onderwerpen die te maken hebben met het verwerken van persoonsgegevens tijdens het dienstverband. Wederom geldt dat je moet voldoen aan alle privacyregels in het onderdeel 'Basisregels'. Je moet er in ieder geval voor zorgen dat de gegevens die je opslaat correct zijn, dat je alleen noodzakelijke persoonsgegevens verwerkt, dat werknemers weten waarom je bepaalde gegevens aanhoudt, dat de persoonsgegevens goed beveiligd zijn en dat werknemers hun inzage- en correctierecht kunnen uitoefenen.

15.3.1. Salaris- en personeelsadministratie

Heb ik een doel en grondslag?

De salaris- en personeelsadministratie bevat persoonsgegevens van werknemers. Het gaat daarbij vooral om gegevens die je 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 jou als werkgever te behartigen.

Let op! Of je nu een papieren administratie bijhoudt of een digitale administratie, in beide gevallen verwerk je persoonsgegevens en moet je voldoen aan de AVG.

Hoe informeer ik?

Zorg dat je je personeel vooraf informeert over hoe je met hun persoonsgegevens omgaat. Dit kan door middel van een privacyverklaring. Je kunt hiernaar verwijzen in het personeelshandboek of in de arbeidsovereenkomst, neem bijvoorbeeld een hyperlink op.

Mag ik een derde inschakelen?

Als je voor de uitvoering van de arbeidsovereenkomst een derde inschakelt (zoals een salarisadministratiekantoor), sluit met die partij dan een verwerkersovereenkomst. Zorg dat je goed begrijpt hoe deze dienstverleners met jouw data omgaan. Meer hierover lees je in het onderdeel: 'Basisregels'.

Hoelang bewaar ik de persoonsgegevens?

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

15.3.2. Zieke werknemers

Heb ik een doel en grondslag?

In principe mag je als werkgever geen gezondheidsgegevens van je werknemers opvragen of opslaan. Je mag die informatie alleen opvragen als het noodzakelijk is om te voldoen aan een wettelijke verplichting, om het risico op arbeidsongeschiktheid van werknemers te beperken, of in verband met een pensioenregeling of

CAO. Persoonsgegevens die nodig zijn voor de re-integratie van een zieke werknemer mag je als werkgever verwerken.

➔ **Hoe ga ik om met een ziekmelding?**

Bij een ziekmelding mag je alleen de volgende (persoons)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. Volgens de huidige beleidsregels van de AP 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 opslaan.

➔ **Mag ik gezondheidsgegevens van medewerkers delen met andere collega's?**

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

➔ **Hoe ga ik om met re-integratie?**

Je moet als werkgever de nodige maatregelen nemen en aanwijzingen geven om je werknemer zijn eigen of andere passende arbeid te laten verrichten. Dat is onderdeel van je re-integratieverplichting. De afspraken hierover en de inzet van zowel jou als werkgever als jouw werknemer in het re-integratietraject moeten worden vastgelegd in een re-integratiedossier. Daar zullen dus ook persoonsgegevens van je werknemer in staan. In dit dossier mag je echter géén informatie opnemen over de aard en de oorzaak van de ziekte van de werknemer. Je mag wel registreren wat de werknemer wel en niet kan doen, oftewel wat de functionele mogelijkheden en beperkingen zijn.

➔ **Wat als ik verander van arbodienst/bedrijfsarts?**

Als je als 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. Gegevens waarop wel medisch beroepsgeheim rust, mag de bedrijfsarts alleen overdragen als het gaat om lopende ziektegevallen of om werknemers die binnen vier weken na betermelding opnieuw uitvallen. In principe hoef je je geen zorgen te maken over wat precies mag worden overgedragen; dat weten de arbodiensten/bedrijfsartsen zelf waarschijnlijk beter. Waar je wel op moet letten is dat je (of de arbodienst/bedrijfsarts) de betrokken werknemers vooraf informeert en dat ze de mogelijkheid krijgen om bezwaar te maken.

Hoe informeer ik?

Zorg dat je je personeel vooraf informeert over hoe je met hun gegevens omgaat. Dit kan door middel van een privacyverklaring. Je kunt hiernaar verwijzen in het personeelshandboek of in de arbeidsovereenkomst, neem bijvoorbeeld een hyperlink op.

Welke beveiliging pas ik toe?

Beperk de groep personen die toegang heeft tot verzuim- en re-integratiegegevens van werknemers zoveel mogelijk. Zorg er voor 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.

Tips:

- Ontmoedig het onrechtmatig verwerken van medische gegevens van werknemers door geen open invulvelden in (ziekte)verzuimregistratieformulieren op te nemen.
- Meer informatie vind je op de website van de AP: mijn zieke werknemer, zie externe links.

Hoelang bewaar ik de gegevens?

Je mag als werkgever informatie over een ziekmelding maximaal twee jaar na het einde van een dienstverband bewaren. Het re-integratiedossier moet binnen twee jaar na de afronding van de re-integratie worden verwijderd.

Let op! 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.

Ben je een eigenrisicodrager Ziektewet of WGA? Dan gelden langere bewaartermijnen. Als je eigenrisicodrager bent voor de Ziektewet, dien je het medisch dossier tien jaar, en overige gegevens vijf jaar, te bewaren. Nota bene: het medisch dossier wordt opgesteld en bewaard door de bedrijfsarts. Als je eigenrisicodrager bent voor de WGA, dan is het noodzakelijk gegevens over de medische keuring van de werknemers tien jaar te bewaren.

15.3.3.Controle van e-mail, internet en telefoon

Iedere werknemer heeft recht op bescherming van zijn privéleven. Dat recht geldt ook op de werkplek. Zo mag een werknemer onder werktijd privécontacten onderhouden zolang dat geen nadelige invloed heeft op de uitvoering van zijn/haar taken of op de werksfeer. Als werkgever moet je de privacy van die contacten waarborgen.

Let op! Voorafgaande instemming van de ondernemingsraad is in dit geval vereist. Meer hierover lees je hieronder in het onderdeel ‘De ondernemingsraad’.

Heb ik een doel en grondslag?

Als je het e-mail, internet- of telefoongebruik van je werknemers controleert, dan verwerk je persoonsgegevens en heb je een grondslag nodig. Het gerechtvaardigd belang (= grondslag) is hierbij het meest voor de hand liggend. Dat vereist wel een belangenafweging, waarbij we je adviseren de belangenafweging te documenteren (zie template).

Welke gerechtvaardigde belangen vanuit de werkgever zouden kunnen gelden? Dat hangt af van de omstandigheden van het geval. Mogelijk wil je kunnen vaststellen of een werknemer communicatiemiddelen van jouw sportorganisatie misbruikt (bovenmatig privégebruik), dat communicatiemiddelen worden gebruikt voor berichten met een onaanvaardbare inhoud (zoals discriminatie), of je wilt bewijs verzamelen van oneigenlijk gebruik van zakelijke communicatiemiddelen. Denk in dat laatste geval bijvoorbeeld aan een werknemer die het zakelijke emailadres gebruikt om te communiceren over verboden nevenactiviteiten, of vertrouwelijke informatie doorspeelt aan derden.

Voordat je allerlei surveillancetechnieken gaat toepassen, is het belangrijk om eerst te kijken welke minder ingrijpende maatregelen je op voorhand kunt nemen. Bedenk welke opties er zijn om verboden gedrag zoveel mogelijk technisch onmogelijk te maken. Denk hierbij aan het blokkeren van bepaalde websites, etc.

Heb je vastgesteld dat er een gerechtvaardigd belang bestaat om het e-mail-, internet- of telefoongebruik van werknemers te controleren en daarmee hun persoonsgegevens te verwerken, dan moet je dit zorgvuldig aanpakken. Hieronder volgen een aantal tips die je daarbij kunnen helpen:

- Definieer het doel van het onderzoek en stem de methode en omvang van het onderzoek hierop af. Is er 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 je 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.

Hoe informeer ik?

Je kunt een werknemer pas aanspreken op (verboden) gedrag als duidelijk is voor de werknemer wat wel en niet mag. We adviseren je dan ook een gedragscode (of een reglement monitoring ICT en internetgebruik) op te stellen waarin je uitlegt:

- Welk gedrag wel en niet is toegestaan;
- Dat sprake kan zijn van toezicht;
- Dat daarbij in specifieke gevallen ook gecontroleerd kan worden op inhoud van berichten, gesprekken en/of internetgebruik; en
- Wat de sancties zijn bij overtreding.

Hoelang bewaar ik de gegevens?

Het Vrijstellingsbesluit geeft als richtlijn dat persoonsgegevens die worden verwerkt bij ICT-gebruik door werknemers uiterlijk zes maanden nadat ze zijn verkregen of twee jaar na het einde van het dienstverband worden verwijderd. Dat is nog een behoorlijk lange termijn. Ga voor jezelf na hoelang het noodzakelijk is om de gegevens te bewaren en houd die termijn aan. Het kan onder omstandigheden noodzakelijk zijn dat je gegevens langer bewaart, bijvoorbeeld in verband met een lopende procedure.

Tip: Meer informatie vind je op de website van de AP: controle van personeel, zie externe links.

15.3.4.Cameratoezicht op de werkvloer

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

Als je als sportvereniging of sportbond zelf niet degene bent die de beslissingen neemt over (de inzet van) het cameratoezicht, maar bijvoorbeeld de verhuurder van het clubhuis, beoordeel dan eerst of je wel verwerkingsverantwoordelijke bent voor de verwerking. Hieronder gaan we in op de situatie waarin je zelf de beslissing neemt over het gebruik van cameratoezicht en dus verwerkingsverantwoordelijke bent.

De aandachtspunten die we in dit onderdeel bespreken, zijn van toepassing op het gebruik van zichtbare camera's. Indien we heimelijk cameratoezicht bedoelen, dan zullen we dit expliciet vermelden. Inzet van

verborgen camera's maakt namelijk in beginsel inbreuk op de privacy van betrokken werknemer(s) en is dan ook alleen toegestaan in specifieke uitzonderingsgevallen.

Let op! Voorafgaande instemming van de ondernemingsraad is in dit geval vereist. Meer hierover lees je hieronder in het onderdeel 'De ondernemingsraad'.

Heb ik een doel en grondslag?

De meest voorkomende vorm van cameratoezicht op de werkvloer vindt plaats door middel van zichtbare camera's en heeft als doel om diefstal en beschadiging van eigendommen tegen te gaan. Omdat cameratoezicht een grote inbreuk is op de privacy van werknemers (en bezoekers), mag je als sportorganisatie alleen camera's ophangen als je aan de volgende voorwaarden voldoet: je hebt een grondslag, het is noodzakelijk, je voert een DPIA uit en je informeert bezoekers en personeel erover.

Het gerechtvaardigd belang is de meest voor de hand liggende grondslag. Om gebruik te kunnen maken van deze grondslag dien je wel een belangenafweging te maken. We adviseren je wederom die te documenteren (zie template).
Bij het maken van je belangenafweging is het belangrijk dat je ervoor zorgt dat het cameratoezicht noodzakelijk en proportioneel is. Dit betekent dat je dit middel niet inzet als het niet nodig is en dat je bovendien 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.

Wil je heimelijk cameratoezicht inzetten, omdat er bijvoorbeeld sprake is van een verdenking? Vraag je dan eerst af of je het doel op een andere manier kunt bereiken. Zo niet, neem dan in je belangenafweging het belang van privacy vs. het belang van waarheidsvinding mee.

Case: heimelijk cameratoezicht
Een supermarkt had heimelijk cameratoezicht ingezet op een supermarktmedewerker die ervan werd verdacht Engelse drop en appelflappen te eten zonder daar (vooraf) voor te betalen. Het hof heeft geoordeeld dat dit te ver gaat. De werkgever had namelijk eerst bij de supermarktmedewerker de huisregels nog eens onder de aandacht moeten brengen vóórdat een zwaar middels als heimelijke cameratoezicht ingezet mocht worden. In deze huisregels stond bovendien niet duidelijk wat medewerkers met beschadigde of niet verkoopbare producten moesten doen.

Let op! Als je als werkgever carmeratoezicht structureel of voor een lange periode inzet om diefstal en fraude door werknemers te bestrijden, dan ben je verplicht om een DPIA uit te voeren. Als je als werkgever een verborgen camera inzet (heimelijk cameratoezicht) dan moet je hiervoor ook een DPIA uitvoeren (let op: ook als het gaat om incidentele toepassing).

Let op! Houd er rekening mee dat beelden niet bruikbaar zijn voor de beoordeling van het functioneren van werknemers. Dat doel vindt de AP onverenigbaar met het doel (beveiliging) waarvoor de beelden zijn verzameld.

Hoe informeer ik?

Je bent verplicht om je werknemers en bezoekers te laten weten dat (en voor welk doel) je gebruik maakt van cameratoezicht. Dit kan bijvoorbeeld door een bordje te plaatsen bij de ingang van je sportcomplex,

kantine of kantoor. Indien de mogelijkheid bestaat dat je heimelijk cameratoezicht inzet in geval van zware verdenkingen/overtredingen, dan dien je dat ook vooraf aan werknemers kenbaar te maken. Op welk moment je dit middel inzet, kun je uitleggen in je gedragscode. Bovendien kun je hierover informeren in je privacyverklaring. Indien je heimelijk cameratoezicht inzet, dan hoef je de werknemer daar niet vooraf over te informeren (anders is het geen heimelijk toezicht meer). De informatieplicht geldt echter nog steeds, in dat geval moet je de werknemer daarover achteraf persoonlijk informeren.

Welke beveiliging pas ik toe?
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.

Tip: Meer informatie vind je op de website van de AP: cameratoezicht op de werkplek, zie externe links.

Hoelang bewaar ik de gegevens?
Camerabeelden mogen niet langer worden bewaard dan noodzakelijk is. De AP geeft hiervoor een richtlijn van maximaal vier weken. Natuurlijk geldt: als er een incident is vastgelegd, zoals bijvoorbeeld diefstal, dan mag je de beelden langer bewaren, namelijk tot het incident is afgehandeld.

Wat als er een verzoek om gegevens binnenkomt van politie of toezichthouder?
Het is mogelijk dat de politie, een overheidsinstantie of een toezichthouder informatie over een werknemer opvraagt. Je mag als werkgever de camerabeelden alleen doorgeven aan derden wanneer aan de voorwaarden voor doorgifte van die persoonsgegevens 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 de camerabeelden doorgeven. De politie kan bijvoorbeeld bepaalde informatie vorderen als een werknemer wordt verdacht van een misdrijf. Vraag bij een vordering altijd om een schriftelijke vordering. Deze moet verwijzen naar de wettelijke bevoegdheid waarop de vorderende instantie zich beroept, de naam en contactgegevens bevatten van degene die vordert en een duidelijke beschrijving van de gegevens die worden gevorderd. Alleen bij een geldige vordering kan je als organisatie een beroep doen op je wettelijke verplichting tot verstrekking van de gegevens. Schakel bij twijfel een advocaat of jurist in om je te laten adviseren.

Beoordeel in gevallen waarin je informatie aan instanties verstrekt ook zorgvuldig of je de betrokken werknemer(s) daarover mag of moet informeren. Je mag de werknemer bijvoorbeeld niet informeren wanneer dat in het belang is van de voorkoming, opsporing of vervolging van strafbare feiten. Meestal staat dat specifiek benoemd in de schriftelijke vordering.

15.3.5. Bring Your Own Device

Bring Your Own Device (BYOD) betekent dat werknemers voor het uitvoeren van hun werkzaamheden een eigen telefoon of laptop gebruiken. Dit kan praktisch zijn, maar het betekent ook dat de werknemer zakelijke gegevens verwerkt op zijn privé apparaat. Ook voor deze verwerkingen ben je verwerkingsverantwoordelijke. Ook bij BYOD moet je dus zorgen dat persoonsgegevens volledig in overeenstemming met de AVG (zie onderdeel ‘Basisregels’) worden verwerkt en niet in verkeerde handen vallen.

Ondanks de risico’s die ontstaan bij het verwerken van zakelijke gegevens op een privé apparaat zullen veel sportorganisaties toch uitgaan van BYOD. Dat is in veel gevallen ook logisch. Lees daarom hieronder waar je rekening mee dient te houden.

Tips:

- Win deskundig IT-advies in vóórdat je BYOD toestaat. Je moet nauwkeurig in kaart brengen welke gegevens werknemers wel en niet via de eigen telefoon of computer mogen versturen. Je moet ook specifieke BYOD-beveiligingsmaatregelen treffen. Er zijn veel dienstverleners die je daarbij kunnen helpen.
- Stel een duidelijk intern personeelsbeleid op en maak dit beleid beschikbaar voor het personeel. Leg precies uit wat wel en niet mag en eis dat werknemers hun software op BYOD apparaten up-to-date houden.
- Zorg dat bedrijfs- en privégegevens duidelijk gescheiden blijven, bijvoorbeeld door het gebruik van een zakelijke applicatie.
- Bedenk of je een BYOD apparaat (dus privé telefoon of laptop van je werknemer) in een mobile device monitoring system wil onderbrengen. Als je dat doet, informeer de betrokkene hierover. Vraag ook toestemming voor het toepassen van veiligheidsregels, zoals als het op afstand wissen van een gestolen of verloren BYOD.
- Bedenk hoe bedrijfsinformatie bij uitdiensttreding van de werknemer weer veilig aan de werkgever kan worden overgedragen.

15.4. Vrijwilligers

Veel sportorganisaties maken 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 over vrijwilligers vaak minder uitdrukkelijk gezag uitgeoefend en zijn werkafspraken minder strikt of zelfs helemaal niet aanwezig.

Een gebrek aan controle op vrijwilligers is vanuit privacy-opzicht erg riskant. Jouw organisatie is in de rol van verwerkingsverantwoordelijke namelijk verplicht om ervoor te zorgen dat vrijwilligers (net als werknemers) persoonsgegevens enkel gebruiken op de wijze die door de organisatie wordt opgedragen. Schiet je daar als sportorganisatie in tekort, dan kan dit leiden tot sancties en aansprakelijkheid.

Tips:

- Zorg dat vrijwilligers zijn gebonden aan geheimhouding. Als je een vrijwilligersovereenkomst sluit, kun je daarin een specifieke geheimhoudingsclausule opnemen. Sluit je geen vrijwilligersovereenkomst dan kan je een aparte geheimhoudingsovereenkomst sluiten.
- Beperk de toegang tot persoonsgegevens zodat vrijwilligers alleen toegang hebben tot gegevens die strikt noodzakelijk zijn voor de uitvoering van hun taak.
- Stel een 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 de toegang tot informatie direct te beëindigen! Zorg ook dat alle persoonsgegevens worden teruggegeven, en waar nodig worden gewist van privéapparatuur van de vrijwilliger.

15.5. De ondernemingsraad

Je bent als sportorganisatie verplicht om een ondernemingsraad in te stellen als er 50 of meer personen werkzaam zijn. Het gaat hier om het gemiddelde aantal werknemers met een arbeidsovereenkomst, waarbij het niet uitmaakt of de werknemer een vast of tijdelijk contract heeft. Werknemers die je inhuurt via een uitzendingsbureau tellen niet mee. Je kunt er als werkgever ook vrijwillig voor kiezen om een ondernemingsraad in te stellen.

Als je verplicht bent om een ondernemingsraad in te stellen, dan betekent dat vervolgens ook dat je enkel bepaalde besluiten kunt nemen na instemming van de ondernemingsraad. Van dit instemmingsrecht is onder meer sprake bij het vaststellen, wijzigen of intrekken van privacybeleid bij werknemers, zoals het beleid over de controle van e-mail, internet en telefoon of over cameratoezicht op de werkvloer (personeelsvolgsystemen).

Tip: Meer informatie vind je op de website van de AP: ondernemingsraad, zie externe links.

15.6. Klokkenluiders

Je bent als sportorganisatie verplicht om een klokkenluidersregeling in te stellen als er 50 of meer personen werkzaam zijn. Het gaat hier om het gemiddelde aantal werknemers met een arbeidsovereenkomst. Hieronder vallen werknemers, maar ook zzp'ers, vrijwilligers, flexwerkers en stagiaires. Meer hierover lees je op de website van het Huis voor klokkenluiders. Zie hiervoor de externe links. Uiteraard kun je er als werkgever ook voor kiezen om deze regeling vrijwillig te implementeren.

Externe links	Uitleg
Artikel 4 Wet op de medische keuringen	In artikel 4 van de Wet op de medische keuringen lees je meer over medische keuringen in verband met het aangaan en wijzigen van een arbeidsverhouding.
Mijn zieke werknemer	Op deze webpagina van de AP lees je meer over zieke werknemers.
Controle van personeel	Op deze webpagina van de AP lees je meer over controle van personeel.
Cameratoezicht op de werkplek	Op deze webpagina van de AP lees je meer over cameratoezicht op de werkplek.
EDPB Videosurveillance Guidelines	Dit is de Engelstalige versie van de richtlijnen van de EDPB voor het verwerken van persoonsgegevens via camera en video apparatuur.
Ondernemingsraad	Op deze webpagina van de AP lees je meer over de Ondernemingsraad.
Huis voor Klokkenluiders	Op deze webpagina van het Huis voor Klokkenluiders lees je meer over de regels over klokkenluiden.

Template(s)	Uitleg
Toetsingskader gerechtvaardigd belang	Dit toetsingskader is te gebruiken als invuldocument voor jou als verwerkingsverantwoordelijke om te beoordelen of je verwerking rechtmatig is.

BIJLAGE TOETSINGSKADER GERECHTVAARDIGD BELANG

Toelichting op het toetsingskader

Dit toetsingskader is gebaseerd op de normuitleg van de Autoriteit Persoonsgegevens. Het is te gebruiken als invuldocument voor jou als verwerkingsverantwoordelijke om te beoordelen of je voldoet aan de cumulatieve voorwaarden die worden gesteld aan de grondslag 'gerechtvaardigd belang'. En dus: of je verwerking rechtmatig is.

Instructies voor de gebruiker van het template zijn in het groen opgenomen. Invulvelden zijn in het geel opgenomen.

Tip:

Bewaar dit document goed. Indien je gebruik maakt van het gerechtvaardigd belang dan wil je immers kunnen laten zien dat je een juiste belangenafweging heb gedaan.

TOETSINGSKADER GERECHTVAARDIGD BELANG

Voorwaarde 1: heb je een gerechtvaardigd belang?

Je hebt een belang als de verwerking van persoonsgegevens een bepaalde waarde voor je organisatie heeft. Dit belang moet echt, concreet en rechtstreeks zijn. Het belang hoeft geen rechtsbelang te zijn. Onder omstandigheden kan ook een financieel of zuiver commercieel belang een gerechtvaardigd belang zijn. Dit kunnen belangen zijn van jou als verwerkingsverantwoordelijke zelf of van een derde.

Enkele voorbeelden van gerechtvaardigde belangen:

- Een veilig en gezond leven hebben of eigendommen beschermen in een dreigende situatie;
- De privésfeer beschermen;
- Grensoverschrijdend gedrag in werkrelaties onderzoeken en beëindigen;
- Fraude, oplichting of ander onrechtmatig gedrag tegengaan;
- Iemand aansprakelijk stellen voor schade;
- Bestaande klanten na een aankoop informeren over soortgelijke, eigen producten of diensten;
- Computersystemen goed beveiligen en beschermen;
- Zorgplichten nakomen voor werknemers en/of klanten.

Voorbeelden van geen ‘gerechtvaardigde belangen’:

- Algemeen belang van de samenleving;
- Het zonder gerechtvaardigd belang volgen van het gedrag van werknemers;
- Het zonder gerechtvaardigd belang volgen van (sport)gedrag van (potentiële) sporters.

Is het belang voldoende duidelijk en specifiek verwoord?
Het belang dat je nastreeft dient voldoende duidelijk en specifiek verwoord te zijn.
[Beoordeel en beschrijf zo concreet mogelijk het belang dat je nastreeft – voorkom een vage omschrijving]

Is het belang rechtmatig?
Het belang dat je nastreeft mag niet in strijd zijn met de wet.
[Beoordeel en beschrijf of het belang dat je nastreeft niet in strijd is met de wet/het recht]

Is er sprake van een ‘echt’ belang?
Het belang dat je nastreeft mag niet speculatief, toekomstig of afgeleid zijn.
[Beoordeel en beschrijf waarom het belang zich momenteel aandient voor je organisatie – en dus niet ‘mogelijk in de toekomst’]

Voorwaarde 2: is de verwerking noodzakelijk om het belang te behartigen?

Is de verwerking écht nodig om het hierboven genoemde belang te behartigen? Leg uit hoe het verwerken van persoonsgegevens leidt tot het behalen van het doel dat je nastreeft. Beantwoord daarbij de volgende vragen.

Noodzakelijkheid: leidt het verwerken van persoonsgegevens tot het behalen van het doel dat je nastreeft? Is de verwerking daarvoor echt nodig?
[Beoordeel en beantwoord]

Subsidiariteit: is het doel op een andere manier te bereiken, die minder nadelig is voor de betrokkene(n)?
[Beoordeel en beantwoord]

Proportionaliteit: staat de inbreuk voor de betrokkene in verhouding tot het doel van de gegevensverwerking?
[Beoordeel en beantwoord]

Voorwaarde 3: wegen de belangen van de verwerkingsverantwoordelijke zwaarder?
Je dient een afweging te maken tussen de belangen van jezelf en de belangen van de betrokkene (balanstoets). Houd rekening met de volgende factoren:

- Gevolgen (of mogelijke gevolgen) van de verwerking voor de betrokkene – houd daarbij extra rekening met minderjarigen en/of kwetsbare individuen!;
- De waarborgen die jij als verwerkingsverantwoordelijke (of derde partij) hebt genomen om ongewenste gevolgen voor de betrokkene te voorkomen of te beperken;
- De ernst van de inmenging op het grondrecht van de betrokkene;
- Of de betrokkene de verwerking min of meer kan verwachten (ligt het in de lijn der verwachting of zal hij/zij verbaasd zijn: gebruik je boerenverstand).

[Beoordeel en beschrijf of de belangen van jouw organisatie zwaarder wegen dan de belangen van de betrokkene(n)]

Conclusie
Vat je conclusies uit bovenstaande beoordelingen samen in een aantal paragrafen en geef expliciet aan of die conclusies een basis geven voor een positieve rechtmatig eigen belang afweging. Documenteer zowel een positieve als een negatieve afweging. Zorg dat je dit document administreert en indien nodig in de toekomst kan verstrekken, bijvoorbeeld in het kader van een controle van de AP.

[Beoordeel en beschrijf of bovengenoemde beoordelingen voldoende basis geven voor een positieve belangenafweging]

BIJLAGE: MODEL PRIVACYVERKLARING

Toelichting op het model
Deze modelverklaring biedt een uitgangspunt voor jou als verwerkingsverantwoordelijke die de betrokkene moet informeren over je verwerking met persoonsgegevens. Instructies voor de gebruiker van het model zijn in het groen opgenomen. Invulvelden zijn in het geel opgenomen.

Let op!
Dit template is slechts een model. Afhankelijk van de aard van de verwerking moet je als verwerkingsverantwoordelijke méér (soorten) informatie aan de betrokkene verstrekken om te voldoen aan je wettelijke informatieplicht. Het gebruik van dit model is geheel voor eigen risico van de gebruiker.

Tip:
Zorg er altijd voor dat de privacyverklaring eenvoudig kan worden geraadpleegd door de betrokkene.

PRIVACYVERKLARING [Naam organisatie]

Laatste update: [datum laatste update]

Dit is de privacyverklaring van [officiële naam van de organisatie](hierna: ['naam organisatie'], 'we', 'wij', 'ons' of 'onze'). Deze privacyverklaring omschrijft welke persoonsgegevens [naam organisatie] verwerkt en voor welke doeleinden deze persoonsgegevens worden gebruikt.

1. Welke persoonsgegevens gebruiken wij en waarom?

Geef in dit onderdeel in de sub-paragrafen per type verwerking aan welke persoonsgegevens je daarvoor verwerkt en waarom. Een aantal suggesties voor type(n) verwerkingen:

- De website [webadres] bezoekt (*opgenomen als voorbeeld in sub-paragraaf 1.1*);
- Een werknemer van [naam organisatie] bent;
- Je inschrijft voor [specificeer evenement/opleiding];
- Een aankoop doet of dienst afneemt bij [naam organisatie];
- Lid wordt van [vul in];
- Je aanmeldt voor nieuwsbrieven van [naam organisatie];
- Via het contactformulier contact met ons opneemt.

1.1. [Voorbeeld: website bezoek]

[Naam organisatie] verwerkt persoonsgegevens van jou als je [voorbeeld: de website bezoekt].

Geef vervolgens per type verwerking een overzicht van alle relevante categorieën van de persoonsgegevens die je daarvoor verwerkt. Enkele suggesties: naam, adres, e-mailadres, telefoonnummer, leeftijd, geslacht, werkgever, functie, bankrekeningnummer, gegevens over aankopen, gegevens over voorkeuren, gegevens over afspraken), etc. Je hoeft niet elk dataveld op te sommen, een categorie mag ook.

Wanneer je [voorbeeld: onze website bezoekt] dan verzamelen we daarvoor de volgende categorieën van persoonsgegevens: [vul in: welke categorieën van persoonsgegevens].

Geef daarna een overzicht van de doeleinden waarvoor je de hierboven opgesomde persoonsgegevens verwerkt. Enkele suggesties:

- Aankopen te doen;
- De aankoop uit te voeren, de dienst te leveren;
- Alle werkzaamheden rondom het lidmaatschap uit te voeren;
- Nieuwsbrieven te verzenden;
- Contact met je op te nemen of te onderhouden;
- De dienstverlening van [naam] te verbeteren;
- De website te optimaliseren.

Deze gegevens gebruiken wij om: [vul in: doeleinden]

Geef hieronder een overzicht van de grondslagen die je gebruikt voor de verwerking van persoonsgegevens. Probeer de grondslagen in je tekst weer te koppelen aan de verwerking.

Enkele suggesties (advies om deze nog nader toe te lichten!):

- De verwerking is nodig voor de uitvoering van de overeenkomst (en de fase voorafgaand daaraan), namelijk om jouw inschrijving als lid uit te kunnen voeren (zoals het verwerken van betalingen, het versturen van informatie etc.);
- Je hebt toestemming gegeven;
- De verwerking is nodig om te voldoen aan een wettelijke verplichting;
- De verwerking is nodig voor de behartiging van ons gerechtvaardigd belang. Bijvoorbeeld voor het verbeteren van onze dienstverlening.

Voor het verwerken van jouw persoonsgegevens is er een grondslag nodig. Voor deze verwerking zijn de volgende grondslag(en) van toepassing: [vul in: grondslag(en)].

Indien je gebruik maakt van de grondslag toestemming, geef dan ook aan wat er gebeurt als die toestemming niet wordt verstrekt, en hoe iemand zijn/haar toestemming weer kan intrekken. Suggestie: jou in te schrijven als lid.

Als je geen toestemming wilt geven dan zijn wij helaas niet in staat om [vul in]. Als je ons wel toestemming geeft voor het verwerken van je persoonsgegevens dan geldt dat je altijd het recht hebt je toestemming weer in te trekken. Dat kan door [beschrijf]. Let op, het intrekken van toestemming heeft geen terugwerkende kracht. Alle verwerkingen die al hebben plaatsgevonden, blijven rechtmatig.

Geef hieronder een overzicht van de bewaartermijnen die gelden voor de verwerking. Als je geen termijn kunt noemen, leg dan uit welke logica je gebruikt. Als je gegevens na een bepaalde periode anonimiseert, benoem dat dan ook. Suggesties:

- We bewaren je betalingsgegevens in ieder geval zolang jij lid bent en verwijderen deze gegevens zeven jaar nadat jij je hebt uitgeschreven (wettelijke plicht);
- Wij bewaren je inschrijving voor een training zolang jij lid bent en verwijderen deze gegevens direct nadat jij je hebt uitgeschreven (overeenkomst).

We bewaren je gegevens: [vul in].

1.2. [Voorbeeld: lid wordt van]

Herhaal wat je in paragraaf 1.1. hebt gedaan tot je al je type(n) verwerkingen hebt opgenomen.
Een aantal suggesties voor type(n) verwerkingen:

- De website [webadres] bezoekt;
- Een werknemer van [naam organisatie] bent;
- Je inschrijft voor [specificeer evenement/opleiding];
- Een aankoop doet of dienst afneemt bij [naam organisatie];
- Lid wordt van [vul in];
- Je aanmeldt voor nieuwsbrieven van [naam organisatie];
- Via het contactformulier contact met ons opneemt.

Probeer de verwerking weer te koppelen aan je doel en grondslag. Voorbeeld bij verwerking [lid wordt van]: Wij verwerken die gegevens om je als lid te kunnen registreren en je deel te laten nemen aan trainingen en andere voorzieningen van de club (= doel). Als grondslag geldt jouw verzoek om lid te worden en/of het uitvoeren van de overeenkomst die wij met je hebben [het lidmaatschap].

2. Worden deze gegevens gedeeld met anderen?

Geef hieronder een overzicht van categorieën van verwerkers. Je hoeft je verwerkers dus niet bij naam te noemen, je mag het in categorieën indelen. Denk aan de leveranciers waar je mee samenwerkt en die persoonsgegevens verwerken t.b.v. jouw organisatie. Suggesties: hosting van de website, gegevensanalyses, chatfunctionaliteit, e-mail marketing etc.

Wij verstrekken gegevens aan externe serviceproviders die diensten voor ons verlenen, zoals: [vul in].

Geef een overzicht van categorieën van derden en leg ook uit waarom je dat doet. Suggestie: NOC*NSF (zie het KISS-reglement voor de daadwerkelijke tekst), andere gelieerde organisaties.

Daarnaast verstrekken wij gegevens aan: [vul de organisatie(s) in en omschrijf de doeleinden van de verkrijging door deze derden].

Verder verstrekken wij geen persoonsgegevens aan andere partijen, tenzij jij hier toestemming voor geeft of wanneer [naam organisatie] verplicht is gegevens te verstrekken op grond van de wet of een rechterlijke uitspraak.

3. Worden je gegevens uitgewisseld buiten de Europese Unie?

Geef hier aan of de gegevens worden verwerkt buiten de EU.

Indien dat niet het geval is en je maakt bijvoorbeeld gebruik van Microsoft of Amazon Webservices met een datacenter binnen de Europese grenzen, dan geldt de volgende suggestie: Wij verwerken jouw persoonsgegevens op het grondgebied van de Europese Unie (EU). Jouw gegevens worden opgeslagen in een datacenter van [naam dienstverlener], waarbij we hebben gekozen voor de locatie van het datacenter binnen de Europese grenzen.

Indien dat wel het geval is, leg dan uit met welke partij en welke waarborgen je hebt getroffen om ervoor te zorgen dat persoonsgegevens beschermd blijven volgens Europese normen en in overeenstemming met toepasselijke wetgeving inzake gegevensbescherming.

4. Minderjarig?

Geef aan of je gegevens verzamelt van minderjarigen en zo ja, hoe je daarmee omgaat. Vooral bij toestemming dien je hier extra toe te lichten dat er ook toestemming nodig is van ouder/voogd. Indien er vrijwel geen gegevens worden verzameld van minderjarigen of je maakt geen gebruik van toestemming, kun je een algemene tekst opnemen zoals hieronder.

Indien jij jonger bent dan 16 jaar en je wilt je gebruik maken van één van onze diensten dan moedigen we je aan om dat onder toezicht van jouw ouder(s) of wettelijke vertegenwoordiger(s) te doen.

5. Wat zijn je privacyrechten?

Geef aan welke privacyrechten een persoon heeft. Aan dit onderdeel hoef je waarschijnlijk niets te wijzigen.

Op grond van de wet heb je verschillende rechten. Je hebt het recht om jouw persoonsgegevens in te zien die wij van jou verwerken, jouw gegevens te laten wijzigen of verwijderen. Daarnaast heb je het recht van bezwaar, het recht op beperking en op gegevensoverdraagbaarheid. Als je gebruik wilt maken van één van je rechten neem dan contact met ons op via onderstaande gegevens (zie hiervoor ‘Bij wie kan ik terecht voor vragen?’).

Wij behandelen jouw verzoek zo snel mogelijk, maar in ieder geval binnen een maand. Mocht de beantwoording van jouw verzoek onverhoopt meer tijd kosten, dan informeren we jou hierover binnen een maand. Het kan namelijk zijn dat vanwege de complexiteit van het verzoek en/of het aantal verzoeken de beantwoordingstermijn langer wordt.

Naast bovenstaande rechten staat het je altijd vrij een klacht in te dienen bij de Autoriteit Persoonsgegevens. De contactgegevens van de autoriteit staan op de website www.autoriteitpersoonsgegevens.nl.

Wij kunnen bij alle vragen/verzoeken vragen om nader bewijs van jouw identiteit. Dit doen we om te voorkomen dat we persoonsgegevens aan de verkeerde partij verstrekken of ten onrechte wijzigingen aanbrengen in de persoonsgegevens of de wijze waarop wij de persoonsgegevens verwerken.

6. Bij wie kan ik terecht voor vragen?

Geef hieronder aan bij wie de lezer terecht kan voor vragen over privacy. Indien je een Functionaris Gegevensbescherming hebt aangemeld, adviseren we je om hier zijn/haar contactgegevens op te nemen.

Heb je vragen over de verwerking van persoonsgegevens door [naam organisatie] of wil je gebruik maken van één of meer van je privacyrechten? Neem dan contact met ons op via onderstaande gegevens.

[naam organisatie]
[Kamer van Koophandel nummer]
[Indien van toepassing: naam van de Functionaris Gegevensbescherming]
[Adres]
[Email]

BIJLAGE MODEL KERNPROTOCOL DATALEKKEN

Toelichting op het model

Dit model biedt een handvat om vast te stellen hoe de sportorganisatie intern omgaat met eventuele datalekken. Zorg dat het beleid eenvoudig kan worden geraadpleegd door alle personen die actief zijn binnen de organisatie.

Instructies voor de gebruiker van het model zijn in het groen opgenomen. Invulvelden zijn in het geel opgenomen.

Let op! Dit protocol is slechts een model. Afhankelijk van de (inrichting van de) sportorganisatie 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]

Met een datalek bedoelen we een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'. Met andere woorden, een inbreuk op de beveiliging die het gevolg heeft dat toegang wordt gegeven tot persoonsgegevens, persoonsgegevens verloren gaan, of persoonsgegevens worden gewijzigd, zonder dat dit gevolg de bedoeling is.

Een aantal voorbeelden van datalekken (de meest voorkomende datalekken 2020) zijn[2]:

- Persoonsgegevens verstuurd naar/afgegeven aan de verkeerde ontvanger (vb. per ongeluk cc-bericht);
- Hacking, malware (kwaadaardige gegevens verzamelende software) en/of phishing;
- Persoonsgegevens van verkeerde klant getoond in klantportaal;
- Apparaat, gegevensdrager (vb. externe schijf) en/of papier met daarop persoonsgegevens kwijtgeraakt of gestolen;
- Persoonsgegevens onbedoeld online gepubliceerd.

FASE 1: de constatering van een informatiebeveiligingsincident
Zodra iemand vermoedt dat mogelijk sprake is van een informatiebeveiligingsincident, meldt deze persoon dit onmiddellijk telefonisch (of, indien dit niet mogelijk is, per e-mail) aan: [contactpersoon datalekken][telefoonnummer] [e-mailadres]. Ook bij twijfelgevallen!

FASE 2: onderzoek van het (mogelijke) beveiligingsincident
[De contactpersoon datalekken] onderzoekt zo spoedig mogelijk en zonder enig uitstel of als een gevolg van het incident (mogelijk) persoonsgegevens onbevoegd toegankelijk waren, onbevoegd toegang is verkregen tot persoonsgegevens of persoonsgegeven verloren zijn gegaan. Raadpleeg bij twijfel onmiddellijk een deskundige!

Indien persoonsgegevens betrokken waren bij het incident zoals hiervoor beschreven, dan stelt [de contactpersoon datalekken] (zowel binnen als buiten werktijd) [de contactpersoon bestuur] onmiddellijk telefonisch en per e-mail op de hoogte via: [contactpersoon bestuur] [telefoonnummer][e-mailadres].

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

[De contactpersoon datalekken] zorgt dat, afhankelijk van de aard van het (vermoede) datalek en de daarover beschikbare informatie, zonder vertraging passende maatregelen tot herstel van het datalek en/of tot voorkoming van herhaling worden genomen.

FASE 3: Onderzoek meldplicht aan Autoriteit Persoonsgegevens en betrokkenen
Zodra [de contactpersoon bestuur] kennisneemt van het datalek 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 verwerkingsverantwoordelijke is. Raadpleeg bij twijfel onmiddellijk een deskundige!

[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

Indien en voor zover [naam organisatie] verwerkingsverantwoordelijke is, bepaalt het bestuur zonder vertraging of als gevolg van het datalek:

- Het datalek een risico inhoudt voor de rechten en betrokkenen wiens persoonsgegevens zijn getroffen door het datalek (melding bij de AP); en
- Of het risico dat is geïdentificeerd waarschijnlijk als een hoog risico kan worden gekwalificeerd voor de betreffende betrokkenen (aanvullende melding bij de betrokkenen).

Raadpleeg bij twijfel onmiddellijk een deskundige!

Indien sprake is van een situatie zoals hierboven beschreven, doet het bestuur onverwijld, maar uiterlijk binnen 72 uur na constatering van het incident, de wettelijk voorgeschreven melding bij de AP en/of betrokkenen.

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 datalek te leiden tot media-aandacht, bereid dan ook een persverklaring voor. Bij een melding aan betrokkenen moet in ieder geval ingegaan worden op de mogelijke persoonlijke negatieve gevolgen en de maatregelen die de betrokkenen kunnen nemen om die gevolgen te beperken.

[De contactpersoon bestuur] en [contactpersoon datalekken] 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.