Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Inhoudsopgave:

DE AVG IN VOGELVLUCHT

Wat moeten organisaties doen?

Registreren van alle verwerkingsactiviteiten met persoonsgegevens, registeren datalekken

Waarborgen implementeren bij internationaal dataverkeer

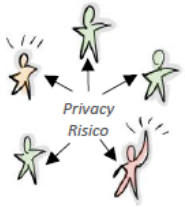
Passende beveiligingsmaatregelen treffen

Verzamelen van persoonsgegevens rechtmatig & evenredig en, indien nodig, zorgen voor eenduidige toestemming en informeren over (het doel/de doelen van) de verwerking van de persoonsgegevens

Verkrijgen van toestemming ouders voor verwerking persoonsgegevens bij kind onder 16

Raadplegen van AP voorafgaand aan bepaalde verwerkingsactiviteiten

Adequate training op het gebied van databescherming voor medewerkers met incidentele of permanente toegang tot persoonsgegevens



Uitvoeren van een gegevensbeschermings impactonderzoek (DPIA) bij nieuwe verwerkingsactiviteiten

Implementeren van gegevensbescherming "By Design" (*ingebakken privacyinstellingen)*

Verantwoordelijkheid nemen voor beveiligingsmaatregelen en verwerkingsactiviteiten van leveranciers

Functionaris gegevensbescherming benoemen (bij structureel grote hoeveelheden data of structureel bijzondere persoonsgegevens)

Op verzoek kunnen laten zien dat de organisatie voldoet aan de AVG

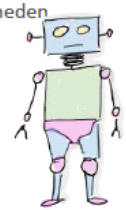
Indien nodig datalekken melden bij de Autoriteit Persoonsgegevens en betrokkenen

Wat kunnen personen doen?

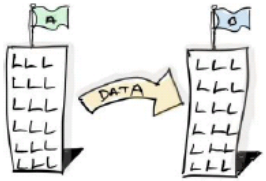
Toestemming voor gegevensverwerking intrekken

Verzoeken om kopieën van al zijn of haar gegevens en verzoek om correctie bij onjuistheden

Verzoeken om verwijdering van gegevens wanneer er geen noodzaak is deze te bewaren

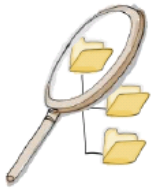


Bezwaar maken tegen geautomatiseerde beoordelingsprocessen, inclusief profileren

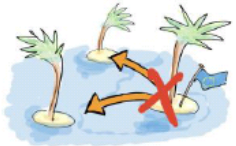


Dataportabiliteit: verzoeken om gegevens in een bruikbaar formaat beschikbaar te stellen voor verhuizing naar een andere partij

Wat kan de Autoriteit Persoonsgegevens doen?



Verzoek om inzage in het gegevensverwerkings-register en bewijs van genomen stappen om aan de AVG te voldoen



Opschorten van grensoverschrijdend dataverkeer (buiten de EU)

Opleggen van een tijdelijk verbod op gegevensverwerking, het verplichten van een datalekmelding en het verwijderen van persoonsgegevens gelasten

Boetes opleggen tot € 20 miljoen of 4% van de wereldwijde omzet voor het niet voldoen aan de AVG

Inspired by IAPP's Awareness Guide. credit to Tim Clements & IAPP

Introductie

Wat verandert er?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen sterkere privacyrechten. Organisaties die persoonsgegevens verwerken – en daar horen ook sportverenigingen toe - krijgen meer verplichtingen. Zo ontkomen clubs er niet meer aan om 'accountable' te zijn; er geldt een documentatieplicht: met documenten kunnen aantonen dat je voldoet aan de AVG. Concreet betekent dit: beleid maken en opschrijven hoe je omgaat met persoonsgegevens van je leden en fans/vrijwilligers.

Wat kan ik doen?

Als sportclub kun je nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Het allerbelangrijkste is beleid te maken en op te schrijven: hoe wil je omgaan met de persoonsgegevens van je leden? Is het oké als ieder bestuurslid of commissie zijn eigen excelletje bijhoudt? Of om ledengegevens te delen met sponsoren? Dit zijn vragen waar je als club over na moet denken en een antwoord op moet formuleren. En dat dus opschrijven…

Dataportabiliteit

Onder de AVG krijgen de mensen van wie jouw club persoonsgegevens vastlegt betere privacyrechten. Bereid je daarop voor, zodat je op tijd en op de juiste manier op verzoeken reageert. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet je ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Maak alvast een overzicht

Breng jouw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens jouw club verwerkt en met welk doel je dit doet, waar deze gegevens vandaan komen en met wie je ze deelt.

Maak beleid

De volgende stap is dat je binnen je bestuur vaststelt hoe jouw club wil omgaan met de privacy van je leden. Als kader bij deze discussie kun je de uitgangspunten 'privacy by design' en 'privacy by default' gebruiken.
Daarvoor ga je na hoe je deze beginselen binnen jouw club kunt invoeren. Privacy by design houdt in dat je er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Privacy by default houdt in dat je technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat je, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken.

Vewerkersovereenkomsten

Vraag je zelf als club af met welke partijen je zaken doet; heb je een derde ingeschakeld voor bijvoorbeeld het incasseren van de contributie? Check dan wat zij doen met de persoonsgegevens van je leden, blijven die gegevens van jouw club? Geeft die organisatie je voldoende waarborgen dat zij de persoonsgegevens van je leden veilig verwerken?

Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stappenplan

In 10 stappen voorbereid op de AVG

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Bereid u daar op voor zodat u op tijd en op de juiste manier op verzoeken reageert.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Stap 4: Data protection impact assessment
(in principe niet van toepassing voor kaatsverenigingen!)

Onder de AVG kunt u verplicht zijn een zogeheten *data protection impact assessment* (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming
(in principe niet van toepassing voor kaatsverenigingen!)

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8: Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder (in principe niet van toepassing voor kaatsverenigingen!)

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Veelgestelde vragen met antwoorden

Bron: https://avgverenigingen.nl/kennisbank/

Mag mijn vereniging beeldmateriaal van minderjarige leden publiceren?

In hoofdlijnen zijn de regels onder de AVG hetzelfde als onder de Wet bescherming persoonsgegevens (Wbp). Dat komt er op neer dat je foto's van minderjarige leden wel mag publiceren, maar alleen als je daarvoor toestemming hebt gekregen. Nieuw is dat je als vereniging moet kunnen aantonen dat deze toestemming is verleend en dat je maatregelen hebt genomen om de beelden te beschermen. We gaan op beide onderdelen verder in.

Toestemming van ouder/voogd of lid
Wil je beeldmateriaal (video/foto) publiceren van leden jonger dan 16 jaar? Dat kan online zijn, maar ook in het papieren clubblad, dan heb je toestemming nodig van zijn of haar ouder/voogd. Bij minderjarigheid, maar ouder dan 16, mag het lid daar zelf toestemming voor geven. Onder de AVG moet je de toestemming kunnen aantonen (bijvoorbeeld een handtekening op papier). En het moet bovendien makkelijk zijn om de toestemming weer in te trekken. Beelden moeten dan verwijderd worden als iemand daar later om vraagt.

Toestemming moet aan 3 voorwaarden voldoen
Om elke twijfel uit te sluiten moet de toestemming hier aan voldoen:

- Deze moet vrij en niet onder druk gegeven zijn.
- Deze moet ondubbelzinnig zijn. Je mag niet uit gaan van het principe 'wie zwijgt, stemt toe'.
- Je moet toestemming vragen voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via beeldmateriaal op de site verslag te doen van een toernooi.

TIP: vraag in een keer toestemming voor de publicatie van beeldmateriaal voor meerdere activiteiten gedurende het jaar. Je moet dan wel per activiteit aan de drie voorwaarden voldoen.

Beveiligen van beeldmateriaal
Onder de AVG moet je aan kunnen tonen dat je voldoende technische en organisatorische maatregelen hebt genomen om beeldmateriaal van minderjarige leden te beschermen.

Een praktisch voorbeeld: wil je alleen ouders en (minderjarige) leden toegang geven tot het beeldmateriaal? Dan is een aparte omgeving binnen je website, waar alleen deze groep op in kan loggen, een goede oplossing. Let wel op: deze moet wel met https beveiligd zijn. Lees meer hierover in één van onze andere kennisberichten.

Er zijn ook apps en andere online diensten op de markt die het mogelijk maken om binnen een afgeschermde groep beelden te delen. Let er wel goed op wat de aanbieder met de persoonsgegevens doet. Dat lees je terug in de privacy policy. Niet alle internationale diensten voldoen namelijk aan de regels die binnen de AVG gelden.

Doordat het privacybelang van kinderen zwaar weegt, valt het maken en publiceren van foto's van kinderen vaak niet onder het gerechtvaardigde belang.

Beeldmateriaal en sociale media:
Waar moet je op letten bij het maken en publiceren van foto's en video's?

Bronnen:
https://www.knhb.nl/kenniscentrum/whitepaper/privacyregels-waar-moet-een-vereniging-rekening-mee-houden
https://sport.nl/media/21900/questions-and-answers-avg-sportverenigingen-april-2018_v2.pdf

De nieuwe media zorgen voor steeds meer mogelijkheden als het gaat om bijvoorbeeld gebruik van foto's en video's op je website en sociale media. Maar hoe ga je daar verstandig mee om?

Mag ik foto's en filmpjes van sporters en toeschouwers publiceren?
Voor het maken en publiceren van beeldmateriaal moet de sportorganisatie toestemming hebben van herkenbaar in beeld gebrachte betrokkenen, *óf een gerechtvaardigd belang hebben*. Denk bij een gerechtvaardigd belang bijvoorbeeld aan persvrijheid, direct marketing, promotie van de organisatie of beveiliging. *Ook wedstrijdverslaggeving kan gemotiveerd onder het gerechtvaardigd belang vallen.* Een sportorganisatie mag in dat geval foto's en beelden van wedstrijden publiceren of uitzenden, ook als daarbij bijvoorbeeld toeschouwers herkenbaar in beeld komen.
De belangenafweging moet zorgvuldig zijn en de belangen van de vereniging én die van de betrokkenen moeten uitvoerig afgewogen en beschreven.

> Let op bij kinderen: hun privacybelang weegt extra zwaar. Vraag daarom uitdrukkelijk toestemming aan de ouders of voogd voordat je overgaat tot publicatie.
>
> In principe is het maken van foto's in de *openbare ruimte* en het publiceren van die foto's in de krant, het verenigingsblad of op de website van de vereniging toegestaan.

Recht van verzet tegen publicatie
Let op: iemand die toestemming geeft voor het *maken* van een foto, geeft daarmee niet per definitie toestemming voor de *publicatie* ervan. Een herkenbaar in beeld gebrachte persoon heeft in sommige gevallen het recht om zich te verzetten tegen publicatie van dergelijke beelden. In de regel zal je gehoor moeten geven aan een dergelijk verzoek. Is dit bezwaarlijk en wil je als vereniging niet aan een dergelijk verzet meewerken, vraag dan om deskundig advies.

Informeren
Zorg ervoor dat leden en toeschouwers op enige manier zijn geïnformeerd over eventuele beeldopnamen. Dat kan bijvoorbeeld in huisreglementen of met behulp van een bordje op het terrein.

Sociale media
Ook op social media ben je als vereniging verantwoordelijk voor het verspreiden van beeldmateriaal namens de vereniging via eigen sociale-media-accounts en pagina's. Je kunt overwegen om een paragraaf over social media-gebruik op te nemen in het huisreglement. De kern is uiteindelijk dat je de privacy borgt van leden/personen die dergelijke publiciteit willen vermijden, en dat je adequaat omgaat met hun eventuele klachten en verzoeken.

Kan de Autoriteit Persoonsgegevens (AP) boetes uitdelen aan verenigingen?

De Autoriteit Persoonsgegevens (AP) treedt binnen Nederland op als privacytoezichthouder. De AP is daarbij ook bevoegd om boetes uit te delen als organisaties straks de AVG overtreden. Daar vallen ook verenigingen onder.

Maximale inspanning om aan de AVG te voldoen

Volgens de regels kan de AP een boete opleggen van maximaal 20 miljoen euro. In welke vorm de AP controles uit gaat voeren of meldingen oppakt is niet bekend. Te verwachten valt dat naleving van de privacywetgeving hoog op de agenda zal staan. Niemand zit op boetes te wachten, maar bovenal is het van groot belang om goed om te gaan met privacygevoelige informatie. Doe je er het maximale aan om aan de AVG te voldoen en privacy te waarborgen, dan is de kans niet groot dat je als vereniging een boete krijgt. Dit is ook precies waarbij de stappen in ons AVG-programma helpen. Zo vergeet je niks en kan je aantonen dat je alle stappen hebt doorlopen om aan de AVG te voldoen.

AP kent twee categorieën boetes

De AP kent twee categorieën overtredingen, we geven ze kort weer plus de maximale boetes die bij de overtredingen horen:

1. Organisaties die persoonsgegevens verwerken hebben onder de AVG bepaalde verplichtingen, zoals de verantwoordingsplicht. Kom je deze niet na, dan kan de AP een boete opleggen van maximaal 10 miljoen euro. Of een boete van 2% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.
2. Overtreedt een organisatie de beginselen of grondslagen van de AVG? Of de privacyrechten van de betrokkenen? Dan kan de AP een boete opleggen van maximaal 20 miljoen euro. Of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.

Nieuwsbericht van 15 maart 2018:

Vette boete blijft uit bij niet onmiddellijk voldoen aan de AVG

15 maart 2018 Door redactie

Harde toezeggingen over boetebeleid AVG niet mogelijk

Minister Dekker gaf de Tweede Kamer daarop te kennen dat de AP hem heeft verzekerd de nadruk zeker de eerste maanden te leggen op het informeren van organisaties en ‘niet op het beboeten van de korfbalvereniging als de welwillendheid er is om aan de regels te voldoen’. Omdat de AP als toezichthouder onafhankelijk is, kon de VVD-bewindsman echter geen harde toezeggingen doen over het boetebeleid vanaf 25 mei.

Mag ik onder de AVG aan direct marketing doen?

De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) en digitale direct marketing (via e-mail, Facebook, LinkedIn of sms). De redenering is dat gewone direct marketing een organisatie geld kost en dus altijd beperkt zal blijven. Digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden, met alle gevolgen van dien. Om deze reden gelden er strengere regels voor digitale direct marketing.

Bij gewone direct marketing heb je vooraf geen toestemming nodig van degene die je benadert.
Bij digitale direct marketing heb je wel vooraf toestemming nodig.

Bij het eerste direct marketing contact moet je altijd het volgende duidelijk uitleggen:

- waarom er contact opgenomen is;
- met welke organisaties de vereniging de persoonsgegevens zal delen;
- wat de rechten zijn om bezwaar te maken tegen deze direct marketing.

Recht van bezwaar
De betrokkene heeft te allen tijde het recht om bezwaar te maken tegen de verwerking van zijn gegevens voor direct-marketingdoeleinden. Als de betrokkene een dergelijk bezwaar indient, dan mogen zijn of haar gegevens niet meer voor marketingdoeleinden worden verwerkt.

Verschillende regels voor reclamepost en digitale reclame
Voor reclamepost en digitale reclame gelden verschillende regels om een overvloed tegen te gaan. Wanneer je als organisatie bijvoorbeeld een folder verspreidt, dan kost je dat geld. Een e-mail is (als we mailpakketten en abonnementen buiten beschouwing laten) gratis, waardoor je onbeperkt e-mails kunt sturen. Als alle organisaties dat zouden doen, dan maken zij deze communicatiekanalen onbruikbaar voor mensen en organisaties.

Richting bestaande leden
Als het gaat om digitale reclame, nieuwsbrieven of gewone mailings, geldt een uitzondering voor leden. Die mag je wel blijven benaderen. Zolang je maar duidelijk in elk contact aangeeft hoe iemand zich weer kan afmelden.

Bescherm persoonsgegevens met back-ups

Om persoonsgegevens van jouw vereniging te beschermen tegen verlies of diefstal moet je back-ups maken. Veilige back-ups! Het is noodzakelijk om dat regelmatig te doen. De meeste digitale systemen maken op gezette tijden back-ups , maar niet allemaal. Ga na of dat geregeld is en of de back-ups ook veilig worden bewaard.

In veel gevallen regel je de data back-ups met je leverancier, maar je kan ook zelf voor de back-ups zorgen. Test regelmatig of het werkt en beveilig back-ups altijd met een wachtwoord. Let op: een USB-stick geldt niet als een veilige back-up. Een USB-stick is heel eenvoudig te stelen en/of te kopiëren. Voor back-ups op een externe harde schijf adviseren wij om deze steeds na een back-up los de koppelen van het systeem en achter slot en grendel te bewaren. Op deze manier zijn de persoonsgegevens ongevoelig voor ransomware. Dit is malware die een computer en/of gegevens die erop staan blokkeert en geld vraagt om de computer weer te 'bevrijden'. Niet onbelangrijk dus, met een veilige back-up heb je altijd nog de beschikking over je data. Een ransomeware aanval kan wel betekenen dat er sprake is van een datalek, loop daarom altijd het stappenplan datalekken door bij een beveiligingsincident.

Ook papieren documenten met persoonsgegevens moeten achter slot en grendel. Tip: zorg voor een sluitend sleutelbeheer met geautoriseerde personen en geheimhoudingsverklaringen. Meer over deze onderwerpen lees je in onze andere kennisberichten.

Wat zijn bijzondere persoonsgegevens?

Het BSN is dus geen bijzonder persoonsgegeven meer (maar zal waarschijnlijk ook niet door kaatsverenigingen verzameld worden).

Je privacy policy moet voor iedereen vindbaar zijn

Om aan de wet te voldoen moet de vereniging een privacy policy (privacybeleid) hebben. De mensen van wie de je persoonsgegevens hebt opgeslagen, dan wel gaat opslaan, moet je goed informeren over hoe je met persoonsgegevens omgaat en informeer je over hun rechten. Dit doe je met de privacy policy. Deze moet bovendien ook makkelijk te vinden zijn. Je website is daarvoor het meest geschikt. Je kan bijvoorbeeld in de footer de privacy policy opnemen en in al je documenten en e-mails daarnaar verwijzen.

Inhoud privacy policy

In de privacy policy breng je mensen op de hoogte van hun rechten zoals:

- inzagerecht;
- recht op rectificatie;
- recht om vergeten te worden;
- recht op beperking van verwerking;
- recht op overdraagbaarheid van gegevens;
- recht van bezwaar.

Stichting AVG heeft een privacy policy geschreven die alle deelnemers voor de eigen vereniging kunnen gebruiken als basis.

Aandachtspunt

Een persoon heeft altijd het recht om zijn persoonsgegevens in te zien. Je kunt deze persoon een kopie van bijvoorbeeld het aanmeldingsformulier met zijn of haar gegevens overhandigen.

Do's en don'ts op je werkplek

Om privacybescherming meer handen en voeten te geven binnen je organisatie adviseren we te werken met do's en don'ts voor op je werkplek. Hieronder een paar voorbeelden:

- Blokkeer altijd je beeldscherm bij het verlaten van jouw werkplek;
- Laat documenten met persoonsgegevens nooit onbeheerd achter op je bureau of bij de printer;
- Kies nooit voor automatisch opslaan van inloggegevens op je computer;
- Besef dat openbare netwerken niet veilig zijn;
- Let op wat je deelt via sociale media;
- Bedek altijd je webcam om 'meekijken' te voorkomen;
- Gebruik nooit de inlog van een collega en geef je inloggegevens ook niet door aan een collega;
- Zorg ervoor dat je mobiele telefoon beveiligd is met een inlogcode of vingerherkenning.

Zorg dat alle software veilig en altijd up-to-date is!

Je bent verplicht om alle persoonsgegevens goed te beveiligen en je moet kunnen aantonen hoe je dit hebt gedaan. Dit geldt voor alle ICT-systemen die je gebruikt. Het betekent dat je verplicht alle software up-to-date moet houden. Dit doe je door het aanzetten van het automatisch ophalen en installeren van updates van de software. Zorg bovendien ook voor goede antivirussoftware en maak goede afspraken met al je softwareleveranciers. Ga na of zij voldoen aan de nieuwe wetgeving. Bij twijfel, schakel een AVG-professional in.

Extra aandacht bij wachtwoorden

Beveiliging betekent niet alleen automatische updates en antivirussoftware. Zorg dat alle medewerkers goede veilige wachtwoorden gebruiken en zet een wachtwoord op alles waarmee persoonsgegevens worden verwerkt! Zowel op de computer, laptop, mobiele telefoon of USB. Maar ook op je Excelbestanden. Wees er ook van bewust dat je niet overal hetzelfde wachtwoord gebruikt en verander regelmatig wachtwoorden. En pas op met het delen van wachtwoorden met collega's.

Hoe weet ik of mijn verenigingswebsite veilig is?

De veiligheid van je website is ook van groot belang. Maar hoe weet je of deze veilig is? Je kunt zelf controleren of de verenigingswebsite veilig is via www.internet.nl. Dit is een initiatief van de Internetgemeenschap en de Nederlandse overheid. Voer je website-adres in op deze site en je krijgt onmiddellijk een analyse van de sterke en zwakke punten van de toegangsbeveiliging. Zo kun je eenvoudig checken of de internetverbinding, e-mail en website wel voldoen aan moderne internetstandaarden.

HTTPS

Let op! Als je persoonsgegevens verzamelt via de website, moet je in ieder geval https gebruiken. Dit is al het geval als je een (contact)formulier op de site gebruikt of een optie aanbiedt voor nieuwsbriefaanmeldingen. Https (beveiliging) voorkomt dat onbevoegde derden mee kunnen lezen met het verkeer naar de website. De professionals van stichting AVG kunnen jouw vereniging hier verder over adviseren.

Nooit gegevens opslaan buiten de EU! Hoe pak je dat aan?

De AVG is Europese wetgeving. De wetgever is extra streng als je persoonsgegevens wilt opslaan buiten de EU. Bij clouddiensten wordt er bijvoorbeeld vaak gebruik gemaakt van opslag buiten de EU, waar andere regels gelden. Deze zijn veelal niet in lijn met de Europese wetgeving. Check daarom of je dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat. Dat kan bijvoorbeeld om een mailinglist of ledenlijst gaan. In de verwerkersovereenkomst kun je dit vastleggen.

Extra aandacht bij online diensten

Bij online diensten (zoals Dropbox, WeTransfer enz.) is het een stuk moeilijker. Enige terughoudendheid is vereist. Bij deze diensten heb je namelijk geen 1-op-1 verwerkersovereenkomst en moet je zelf onderzoeken of de dienst voldoet aan de Europese eisen. Leg contact en/of bekijk de voorwaarden van de aanbieder. Geef altijd aan dat je vereniging domicilie heeft in Nederland. In aanloop naar de AVG zorgen diverse niet-Europese partijen (denk aan Microsoft), dat zij hun diensten/opslag binnen de EU regelen. Een goede ontwikkeling. Wees er echter op bedacht dat niet alle partijen dit (tijdig) op orde hebben. Zo heeft in november 2017 (na vele toezeggingen) MailChimp dit nog niet geregeld. Veel Nederlandse organisaties maken gebruik van hun nieuwsbriefdienst. Wellicht moet je nadenken over een anders oplossing?!

Stappenplan

Als je wilt dat de verenigingsdata netjes binnen de EU blijven, hoe pak je dan aan? Hier een aantal handige stappen:

- Werk voor dit onderdeel nauw samen met de ICT-afdeling of ICT-partij. Zeker externe partijen krijgen deze vragen steeds vaker en hebben waarschijnlijk al wat antwoorden klaarliggen;
- Begin met een beschrijving van alle software die je vereniging gebruikt, het zogenaamde softwarelandschap;
- Geef in het landschap aan met welke softwareleveranciers je een verwerkingsovereenkomst hebt. Als het goed is staat in de verwerkersovereenkomst dat jullie data alleen binnen de EU opgeslagen mogen worden;
- Vraag bij de overgebleven softwareleveranciers na waar de persoonsgegevens opgeslagen worden. Vaak heeft een softwareleverancier daarover al informatie staan op de website;
- Zorg dat je de informatie bewaart waar de persoonsgegevens zijn opgeslagen. Dit geldt in het bijzonder voor leveranciers waarvan bekend is dat ze een niet-Europese achtergrond hebben;
- Ben je er ook van bewust dat er sprake kan zijn van een keten van leveranciers. Zorg dat de eigen leverancier garant staat voor de gegevensbescherming door de partners en derden.

Goed om te weten: De Stichting AVG voor Verenigingen heeft contacten met AVG-ICT-specialisten die je kunnen helpen met het maken van een softwarelandschap en het controleren van de locaties van de data.

Verplichte (nieuwe) verwerkersovereenkomst met derden zoals drukkerij en hostingpartij

De AVG verplicht je om verwerkersovereenkomsten met derden/partners te sluiten. Dit komt bij verenigingen in veel situaties voor, bijvoorbeeld bij het inschakelen van een drukkerij, hostingpartij of digitale nieuwsbriefverzender. Als vereniging mag je persoonsgegevens nooit doorgeven aan een andere partij als je met die partij geen verwerkersovereenkomst hebt.

Ook oude bewerkersovereenkomsten herzien

Ga dus na met welke verwerkers jouw vereniging allemaal samenwerkt en sluit (nieuwe) overeenkomsten af die voldoen aan de AVG. Binnen de overeenkomst moeten onder meer afspraken worden gemaakt over de beveiliging van de gegevens en het verwijderen van de gegevens aan het einde van de opdracht. Let op. Oude bewerkersovereenkomsten moeten herzien worden, omdat de AVG andere eisen stelt.

Binnen het AVG-programma hebben we een standaard verwerkersovereenkomst ter download opgenomen. Uiteraard kun je ook zelf afspraken vastleggen binnen eigen documentatie/contracten. Hierin moet je in ieder geval de volgende afspraken vastleggen:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens;
- de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

Deze en meer punten kaarten we aan in een extra checklist waarmee je kunt vaststellen of je verwerkersovereenkomst voldoende is ‘dichtgetimmerd’. De Stichting AVG kan je ook helpen door je overeenkomsten (contracten) met externe verwerkers te controleren.

Gegevens van ex-leden moet je vernietigen!

Onder de AVG gelden dezelfde regels omtrent de bewaartermijn als nu. Het uitgangspunt blijft dat je persoonsgegevens niet langer mag bewaren dan noodzakelijk voor het doel van de verwerking.

Verscheuren en weggooien is niet voldoende

Persoonsgegevens moeten zowel digitaal (bijvoorbeeld een regel wissen in Excel) als fysiek vernietigd worden (het aanmeldingsformulier) als er geen overeenkomst meer is. Bij de vernietiging van papieren documenten is versnipperen de juiste wijze, verscheuren en weggooien is niet voldoende.

Bewaartermijn, wet nog in beweging

Hoe lang mag of moet je persoonsgegevens bewaren? Op dit punt is de wetgeving nog in beweging. Hoe het precies zit met de gegevens van ex-leden, is namelijk nog niet duidelijk. Financieel heb je een bewaarplicht van 7 jaar, maar voor een nieuwsbrief? Ons advies is te bepalen hoe lang je de persoonsgegevens bewaart. Als dat niet mogelijk is, bepaal je in elk geval de criteria voor het vaststellen van de bewaartermijn. Je legt de bewaartermijn of de criteria vast in het privacybeleid. Ons advies is ook om de nodige persoonsgegevens in de financiële administratie te behouden, en verder de gegevens overal vernietigen na het verlopen van de bewaartermijn. De Stichting AVG volgt de ontwikkelingen op de voet en zodra er meer over duidelijk is over de concrete invulling omtrent bewaartermijnen informeren wij deelnemers aan ons programma.

Toestemming & controleplicht bij gegevens minderjarigen (<16)

Als je persoonsgegevens verwerkt van personen jonger dan 16 jaar, dan moet je daarvoor schriftelijk een akkoord hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Zwart op wit! Volgens de AVG geldt namelijk de controleplicht, dit wordt ook expliciet vermeld in de nieuwe privacywet. Als vereniging moet je dus kunnen aantonen dat die toestemming ook daadwerkelijk is verleend. Een handtekening op papier.

Maar mag je überhaupt geboortedata vastleggen?

Als het lidmaatschap leeftijdsafhankelijk is dan heb je bij inschrijving dus ook een geboortedatum nodig. Is het lidmaatschap niet leeftijdgebonden, dan is hiervoor de geboortedatum dus niet relevant en mag je die niet opnemen.. Let er ook op dat er altijd een duidelijk doel van de gegevensverwerking beschreven is als je een geboortedatum gaat opslaan en verwerken.

Bewustwording: maak gebruik van geheimhoudingsverklaringen!

Je neemt als vereniging je verantwoordelijkheid door je te houden aan de wettelijke privacyregels en bewustwording te creëren binnen de gehele organisatie. Om bewustwording om te zetten in harde procedures en verantwoordelijkheden kan je geheimhoudingsverklaringen inzetten. Niet verplicht, zeker wel aan te raden!

De vereniging bepaalt wie er geautoriseerd is om persoonsgegevens in te zien, te bewerken ofwel te verwerken. Vaak worden alleen de secretaresse (of secretaris) en de bestuursleden geautoriseerd. Dat verschilt per vereniging. Om goed vast te leggen wat een geautoriseerde medewerker van de vereniging wel of niet mag doen is het verstandig dit goed te beschrijven in een geheimhoudingsverklaring (vaak onderdeel van de arbeidsovereenkomst). Je kunt risico's beperken door goed vast te leggen welke medewerkers geautoriseerd moeten zijn voor hun werk voor de vereniging (en andere dus niet). Kortom: Laat medewerkers/vrijwilligers die inzicht hebben in persoonsgegevens een geheimhoudingsverklaring tekenen!

Tip: Het is bovendien een mooi moment om weer een goede afweging te maken wie momenteel toegang heeft tot (welke) persoonsgegevens.

Moet onze vereniging een (D)PIA houden?

Zodra de AVG geldt (25 mei 2018) moeten sommige organisaties verplicht een Data Protection Impact Assessment (DPIA) uitvoeren. De DPIA is een instrument om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen en om vervolgens maatregelen te nemen om de risico's zo klein mogelijk te maken. Wat is voor verenigingen van toepassing? Een DPIA geldt enkel voor speciale gegevensverwerkingen, met name wanneer er een hoog privacyrisico is.

De AVG geeft aan dat dat in ieder geval geldt als jouw organisatie:

- systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling (beoordelen van mensen op basis van persoonskenmerken);
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).
- op grote schaal bijzondere persoonsgegevens verwerkt;

(Kleine) verenigingen komen veelal niet bij deze voorbeelden in de buurt. Heb je twijfels, neem contact op met je koepelorganisatie. Heb je een vraag vanuit een koepelorganisatie en ben je partner van onze stichting, dan kan je een beroep doen op onze specialisten.

Je mag gegevens van een lid alleen gebruiken met de juiste ‘doelbinding’. Wat betekent dat?

Welke gegevens verwerkt jouw vereniging, met welk doel en heb je ze daar ook voor gekregen? We praten over ‘doelbinding’. Het is belangrijk dat je persoonsgegevens alleen verwerkt voor de doeleinden waarvoor je deze hebt verkregen. En, je mag ook niet meer gegevens verlangen dan nodig zijn voor het doel.

Een voorbeeld:
De vereniging heeft bij het inschrijven van een nieuw lid zijn of haar naw-gegevens gekregen. Je mag deze naw-gegevens van het nieuwe lid dus alleen gebruiken voor de uitvoering van de lidmaatschapsovereenkomst en niet voor andere doeleinden. Er moet dus 1) een overeenkomst (hetzij een schriftelijke of elektronische instemming) zijn met 2) een bepaald doel en de daarvoor 3) relevante persoonsgegevens. De betrokkene heeft jou zijn/haar persoonsgegevens aangereikt met een specifiek doel (lid worden) en de persoonsgegevens mogen dan ook alleen daarvoor gebruikt worden.

Een ander herkenbaar voorbeeld is het inschrijven voor de digitale nieuwsbrief. De afspraak is dan: je krijgt mijn e-mailadres voor toesturen van de (wekelijkse) nieuwsbrief. Je mag deze persoon niet zomaar in een aparte mail uitnodigen voor bijeenkomsten, want dat heb je niet samen afgesproken!

Inventariseer en registreer
Inventariseer en registreer wat bij jouw vereniging van toepassing is. Voor verenigingen hebben wij al uitgezocht welke soorten overeenkomsten er meestal gelden (denk ook aan een vrijwilligersovereenkomst) en hebben we al het doel en het type persoonsgegevens genoteerd. In het AVG-programma hebben we uitgebreide lijst opgenomen van doelbindingen die je alleen maar hoeft aan te vinken.


AVG

Checklist inventarisatie doelbinding

Voor verenigingen hebben wij al uitgezocht welke soorten overeenkomsten er zijn en hebben we al doel en persoonsgegevens genoteerd. Je hoeft dus alleen maar aan te vinken welke zaken voor jou van toepassing zijn. Staat jouw overeenkomst er niet bij voeg deze dan toe.

[ ] Doordat een persoon met diens persoonsgegevens of een organisatie met diens (contact-)persoonsgegevens zich aangemeld heeft als lid
[ ] Naam, adres, woonplaats;
[ ] e-mail;
[ ] Geboortedatum;
[ ] Kleding- en/of schoenmaten;
[ ] Bankgegevens voor automatische incasso;
[ ] Anders, nl.

[ ] Doordat een persoon zich aangemeld heeft als vrijwilliger
[ ] Naam, adres, woonplaats, e-mail, geboortedatum;
[ ] Bankgegevens declaratie/vergoedingen;
[ ] Anders, nl.

Aandachtspunt bij een lidmaatschapsovereenkomst
Zorg dat in je lidmaatschapsovereenkomst/formulier duidelijk vermeld dat de ingevulde gegevens gebruikt gaan worden conform de privacy policy. In de privacy policy kun je al de doelbindingen het

beste beschrijven. Je kunt de privacy policy bijvoegen of een duidelijke verwijzing (of link naar de website) opnemen. Let op dat een minderjarige (< 16jaar) schriftelijke toestemming nodig heeft van ouder, verzorger, wettelijke vertegenwoordiger om de overeenkomst aan te gaan. Vergeet ook niet om met vrijwilligers een aparte overeenkomst aan te gaan.

Tip: hou je vereniging eens extra tegen het licht
Je bent nu met veel gegevens bezig. Je raakt aan de kern van je vereniging. Zijn de statuten nog actueel? En het huishoudelijk reglement? Belangrijke vragen. Door aan de slag te gaan met de AVG zie je dat je meer inzichten krijgt. Zijn aanpassingen nodig? Bespreek dit eens in het bestuur.

Wist je dat je moet inventariseren welke persoonsgegevens je vastlegt?

Vanuit de AVG moet elke vereniging inventariseren welke persoonsgegevens worden verwerkt. En je moet daar een overzicht van kunnen overhandigen. Je hebt voor je vereniging persoonsgegevens nodig anders kun je geen ledenbestand opbouwen. Kernbegrip is 'verwerken'. Hiermee bedoelen we alle handelingen die je met de persoonsgegevens uitvoert. Je maakt een algemeen Excel-ledenbestand en een financieel Excel-bestand, je kopieert gegevens op papier, je maakt een adressenlijstje voor je nieuwsbrief, enz. Zodra je persoonsgegevens verwerkt val je onder de AVG en moet je dus aan deze regelgeving voldoen.

Ga na welke persoonsgegevens er binnen de vereniging gebruikt worden
Het is een hele klus om te inventariseren welke gegevens je allemaal verwerkt. Denk aan:

- Computerapplicaties controleren waarin velden zijn opgenomen met persoonsgegevens
- Controleer ook persoonsgegevens die je als vereniging hebt ondergebracht bij derde partijen, b.v. een salarisadministratiekantoor of nieuwsbrief-verzender
- Elektronische documenten (Excel-lijstjes, Word-documenten, etc.) met persoonsgegevens
- Papieren documenten (denk ook aan kopieën van een paspoort of rijbewijs)

Binnen ons AVG-programma hebben we een handige checklist waarbij je na kunt lopen en aanvinken welke persoonsgegevens je allemaal verwerkt.

Pas op met bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn gegevens van gevoelige aard, de verwerking ervan kan iemands privacy ernstig beïnvloeden. Denk aan gezondheidsgegevens of politieke voorkeur. Bijzondere persoonsgegevens mogen daarom alleen onder zeer strenge voorwaarden worden verwerkt.

Nog een aantal kernpunten

Bron: Webish, ict – security products, Cor Procee

UITGANGSPUNTEN VAN GEGEVENSVERZAMELING

- Verzamel niet meer dan nodig is
- Stel een correcte grondslag vast
- Ga zorgvuldig met gegevens om
- Registreer uitgevoerde handelingen

PERSOONSGEGEVENS

- Ieder stukje informatie, waarmee een persoon direct of indirect geïdentificeerd kan worden:

• Naam	• NAW	• IP adres
• Geslacht	• Leeftijd	• Geboortedatum
• Burgerlijke staat	• Talenkennis	• Telefoonnummer
• Emailadres	• BSN nummer	• Serienummer

- Hoe meer informatie aanwezig is, des te groter de kans dat dit iemand kan identificeren
- Geen onderscheid tussen persoonsgegevens privé of zakelijk

BIJZONDERE PERSOONSGEGEVENS

Specifieke categorieën informatie, waarmee een persoon direct of indirect geïdentificeerd kan worden:

- Ras / etnische achtergrond
- Politieke opvattingen
- Religieuze, of filosofische opvattingen
- Vakbond
- Biometrische data
- Medische status
- Gegevens over seksleven
- Seksuele voorkeur
- Veroordelingen / overtredingen / maatregelen
- Persoonsgegevens van kinderen*

VERWERKER

→ Je bent een Verwerker, wanneer je in opdracht van een verantwoordelijke persoonsgegevens verwerkt

VERWERKINGSVERANTWOORDELIJKE

→ Je bent een Verwerkingsverantwoordelijke, wanneer je organisatie eigenaar is van gegevens, of wanneer je organisatie zelf de doelen en de middelen van verwerking van persoonsgegevens vaststelt

VERWERKERSOVEREENKOMST

→ Altijd verplicht bij het uitbesteden van verwerkingen

→ Wat staat in een verwerkersovereenkomst:

• Algemene informatie over de verwerking.	• Verwerkingsinstructies
• Geheimhoudingsplicht	• Privacyrechten helpen naleven
• Beveiliging	• Subverwerkers
• Gegevens verwijderen	• Audits

TECHNISCHE MAATREGELEN

→ Encryptie, pseudonimiseren, anonimiseren

→ Goede sloten op belangrijke ruimtes

→ Netwerkbescherming: actieve firewall

→ Beveiligde cloudopslag met uitgebreide logging, of lokale server met afdoende beveiliging en logging

→ Emailbeveiliging en werken met filelinks

→ Gebruikmaken van certificaten

→ Op maat gemaakte cookiemelding

→ Op maat gemaakte privacyverklaring

ORGANISATORISCHE MAATREGELEN

- Duidelijke afspraken wie toegang heeft tot wat
- Inrichten van een verwerkingsregister
- Inrichten van incidentenregister
- Verwerkersovereenkomsten aangaan met partners
- NDA en intern privacybeleid

WAT IS EEN DATALEK?

- Hack
- Ransomware / virus
- USB stick kwijtgeraakt
- Laptop gestolen
- Scherm niet vergrendeld in toegankelijke ruimte
- Mail naar de verkeerde persoon gestuurd
- Wachtwoord bekend bij onbevoegde
- Dossierkast open laten staan
- Etc, etc, etc.....

TOESTEMMING

- Vastleggen welke toestemming iemand heeft gegeven
- Toestemming moet op verzoek bewezen worden als onderdeel van de verantwoordingsplicht
- Gestelde eisen aan toestemming:
  - Vrij – toestemming geven en intrekken
  - Specifiek – geen twijfel over doel en gegevens
  - Geïnformeerd – transparant en duidelijk
  - Ondubbelzinnig – actieve handeling van toestemming

INVENTARISEREN……..

- Welke persoonsgegeven worden verwerkt?
- Wat is de grondslag voor iedere verwerking?
- Wie heeft er toegang en op welke manier?
- Welke rechten van betrokkenen zijn vastgelegd?
- Ben je in staat hieraan te voldoen?
- Controleer voor welke gegevens toestemming vereist is
- Bezit je dit aantoonbaar? Zo nee, alsnog formaliseren
- Bepaal hoe datalekken geregistreerd moeten worden
- Zorg voor een verantwoordelijke voor gegevensbescherming