#3 Privacy & sportvereniging: informatiebeveiliging

Vanaf 25 mei 2018 geldt er nieuwe, strengere regelgeving op het gebied van privacy, de zogeheten Algemene Verordening Gegevensbescherming (AVG). In deze reeks van nieuwsbrieven gaan we in op de belangrijkste verplichtingen voor sportverenigingen. Ditmaal behandelen we de verplichting tot het beveiligen van persoonsgegevens.

Inleiding
Iedere sportvereniging is zelfstandig verplicht om persoonsgegevens veilig te behandelen. Als gegevens bijvoorbeeld worden gestolen of ergens rondslingeren, kan dit vervelende gevolgen hebben voor betrokkenen. We bespreken enkele vaak door sportverenigingen gestelde vragen.

Welke beveiligingsplicht heeft een vereniging?
Een vereniging moet *passende maatregelen* treffen om te voorkomen dat persoonsgegevens worden blootgesteld aan onrechtmatige verwerking. Informatiebeveiliging is echter meer dan het beschermen tegen diefstal en virussen. De praktijk leert dat de meeste beveiligingsincidenten het gevolg zijn van niet-opzettelijke nalatigheid. Denk bijvoorbeeld aan het rondslingeren van USB-sticks met leden- en deelnemerslijsten, of een computercrash waarbij persoonsgegevens definitief verloren gaan. Je beschermt persoonsgegevens tegen iedere vorm van verlies van beschikbaarheid, integriteit dan wel vertrouwelijkheid.

Welke maatregelen moet de vereniging treffen?
Uiteindelijk draait informatiebeveiliging om een juiste combinatie van zowel *technische* als *organisatorische* maatregelen, waarbij uiteindelijk de zwakste schakel telt. Zo is een complex wachtwoord voor het inloggen op de online ledenadministratie zinloos als datzelfde wachtwoord op een notitieblok rondslingert in het clubhuis.

> **Voorbeelden van veelvoorkomende beveiligingsmaatregelen**
> Technisch:
> - het versleutelen van bestanden ("encryptie");
> - het regelmatig doen wijzigen van wachtwoorden;
> - het regelmatig maken van back-ups.
>
> Organisatorisch:
> - het invoeren van een geheimhoudingsplicht aan vrijwilligers/bestuurders;
> - het invoeren van een incidentprotocol voor beveiligingsincidenten;
> - het trainen van vrijwilligers/bestuurders om veiligheidsbewustzijn te creëren.

Welke maatregelen nodig zijn, hangt af van de risico's die met de verwerking van persoonsgegevens zijn verbonden. Bijzondere risicogebieden waar je als sportvereniging bijvoorbeeld vaak rekening mee houdt zijn:
- de vertrouwelijkheid en beschikbaarheid van de verenigingsadministratie, met name de ledenadministratie;
- communicatie met vertrouwenscontactpersonen; en
- gegevens van jeugdleden.

> **Tip**
> De Autoriteit Persoonsgegevens heeft de Beleidsregels beveiliging persoonsgegevens gepubliceerd. Het is aan te raden aan dit document te lezen, nu de autoriteit daarin uitgebreid aangeeft wat zij zoal van een organisatie verwacht.

Wat te doen als een vereniging geen kennis in huis heeft?
Het feit dat een doorsnee sportvereniging meestal weinig tot geen expertise in huis heeft op het gebied van IT/informatiebeveiliging, is geen excuus om het onderwerp links te laten liggen. Verenigingen, groot of klein, worden geacht datgene te doen wat redelijkerwijs van hen kan worden verlangd.

Onthoud daarbij dat de kwaliteit van beveiliging niet zozeer draait om geld, maar vooral om het verkrijgen van voldoende kennis en bewustzijn.

Moet de vereniging beveiligingsafspraken maken met leveranciers van (IT-)diensten?
Ja, dat is noodzakelijk als de leverancier toegang krijgt tot persoonsgegevens waarvoor de vereniging verantwoordelijk is. Denk bijvoorbeeld aan leveranciers van online verenigingsapplicaties. De afgesproken beveiligingsniveaus leg je meestal vast in een zogeheten verwerkersovereenkomst (ook wel "bewerkersovereenkomst" genoemd).

Mogen persoonsgegevens op privéapparatuur worden geplaatst?
Het is niet ongebruikelijk dat bestuurders/vrijwilligers bij de vervulling van verenigingstaken gebruikmaken van privéapparatuur. Dat is in principe mogelijk, maar de vereniging blijft verantwoordelijk voor het veilig verloop van dit gebruik. Overweeg in ieder geval het invoeren van de volgende regels:

- de gebruiker moet antivirussoftware installeren en deze regelmatig updaten;
- de gebruiker moet deugdelijke toegangscodes instellen;
- vermijd opslag op lokale harde schijven indien gebruik kan worden gemaakt van web-omgevingen (bijv. Google Apps, Office 365, online verenigingsadministratie etc.);
- zorg dat te allen tijde een deugdelijke back-up beschikbaar blijft van de gegevens die op de privéapparatuur worden verwerkt; en
- beëindigt iemand zijn of haar verenigingstaken, zorg er dan voor dat deze persoon niet langer toegang heeft tot de gegevens.

Wat moet de vereniging doen in geval van een datalek?
Leidt een beveiligingsincident tot de vernietiging, verlies, wijziging of ongeoorloofde verstrekking/toegang, dan is mogelijk sprake van een *datalek*. Tenzij het datalek waarschijnlijk geen nadelige gevolgen heeft voor de betrokken personen, moet het lek tijdig worden gemeld bij de Autoriteit Persoonsgegevens. Heeft het lek bovendien een hoog risico op nadelige gevolgen voor de personen wiens gegevens het betreft, dan moet het incident ook aan deze personen worden gemeld. Blijkt een datalek achteraf ten onrechte niet tijdig te zijn gemeld, dan kan dit leiden tot oplegging van een fikse boete.

Heeft de vereniging onvoldoende kennis of mankracht in huis om een incident af te handelen, vraag dan om hulp van een deskundige. CMS is ervaren in het adviseren van sportorganisaties en het afhandelen van beveiligingsincidenten.

In de volgende editie gaan we dieper in op de privacyverklaring en het vragen van toestemming aan een betrokkene.