Protocol Meldplicht Datalekken

oktober 2018

Schietsportvereniging Filadelfia

INLEIDING

De Koninklijke Nederlandse Schietsport Associatie (KNSA) en de bij haar aangesloten schietsportverenigingen (Verenigingen) hebben in het kader van de Algemene Verordening Gegevensbescherming (AVG) de verplichting om een datalek bij de AP en onder bepaalde omstandigheden bij de betrokken te melden.

Het Protocol Meldplicht Datalekken is onderdeel van het *Protocol Omgang met en bescherming van persoonsgegevens binnen de schietsportverenigingen*. Het doel is om de Verenigingen inzicht te verschaffen in de wijze waarop aan de meldplicht kan worden voldoen, zodat de KNSA en de Verenigingen handelen in overeenstemming met de AVG.

WAT HOUDT DE MELDPLICHT IN?

De meldplicht houdt in dat vanaf het moment dat de Vereniging kennis krijgt van een (beveiligings-)incident dat mogelijk een datalek betreft, dit zo snel mogelijk moet worden gemeld. Op grond van de AVG moet er onverwijld en binnen 72 uur een melding bij de Autoriteit Persoonsgegevens (AP) plaatsvinden. Indien de melding na de termijn van 72 uur plaatsvindt, dan moet deze vergezeld gaan van een motivering.

Een datalek moet worden gemeld aan de AP als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

WANNEER IS SPRAKE VAN EEN DATALEK?

De AVG definieert een "inbreuk in verband met persoonsgegevens" als:

> *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;*

Er is sprake van een datalek wanneer de inbreuk waarschijnlijk een hoog risico voor de betrokkene inhoudt. Hieronder valt een beveiligingsincident waarbij sprake is van verlies of onrechtmatige verwerking van persoonsgegevens. Indien redelijkerwijs niet kan worden uitgesloten dat tijdens het incident persoonsgegevens zijn betrokken, moet worden uitgegaan van een datalek. Een beveiligingsincident betekent dat inbreuk heeft plaatsgevonden op de beschermingsmaatregelen die de verwerkings-verantwoordelijke heeft genomen of had moeten nemen om persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking te beveiligen.

Er is bijvoorbeeld sprake van een datalek als een beveiligingsincident heeft plaatsgevonden waarbij persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uit te sluiten valt.

Als er alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden bij aan de AP. Beveiligingslekken dienen echter wel te worden gemeld bij de KNSA.

Wanneer persoonsgegevens tijdelijk niet beschikbaar zijn, is onder bepaalde omstandigheden ook een datalek dat moet worden gemeld. Een omstandigheid is bijvoorbeeld een DDOS aanval. Een DDOS aanval heeft mogelijk tot gevolg dat er tijdelijk geen operaties uitgevoerd kunnen worden.

INTERNE PROCEDURE: ROLLEN EN VERANTWOORDELIJKHEDEN

Wanneer de Vereniging kennis krijgt van een datalek moet eerst beoordeeld worden wie voor de verwerking daarvan verantwoordelijk is. Indien het gaat om de verwerking waarvoor de Vereniging verantwoordelijk is (zoals de interne verenigingscompetitie, aanwezigheidsregisters, de ledenadministratie, enzovoorts) dan is de Vereniging ervoor verantwoordelijk om daarvan een melding bij de AP te doen. Voorts dient de Vereniging melding te doen bij de KNSA.

Indien het gaat om verwerkingen waarvoor de KNSA verantwoordelijk is (zoals het bijhouden van wedstrijdgegevens in verband met de KNSA-ranking of de ledenadministratie zoals die wordt gevoerd in de "Mijn KNSA online omgeving") doet de Vereniging van een datalek melding aan de KNSA en zal de KNSA zo nodig een melding bij de AP doen. Bij twijfel dient het bestuur van de Vereniging contact op te nemen met de KNSA, om te kunnen beoordelen wie de melding aan de AP zal doen.

MELDEN AAN DE AUTORITEIT PERSOONSGEGEVENS

Artikel 33 van de AVG bepaalt wanneer en op welke manier een datalek aan de AP moet worden gemeld. De belangrijkste vereisten zijn de volgende:

1. Een melding aan de AP moet plaatsvinden bij elk incident met betrekking tot persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico voor de betrokkene(n) inhoudt.

2. Het datalek wordt door de verwerkingsverantwoordelijke [Vereniging] en/of [KNSA] aan de AP gemeld.

3. De melding vindt binnen 72 uur plaats. Indien de melding niet binnen 72 uur plaatsvindt, moet de vertraging worden gemotiveerd.

4. Indien het datalek door een verwerker wordt geconstateerd, informeert hij de verwerkingsverantwoordelijke zonder onredelijke vertraging nadat hij van het datalek heeft kennisgenomen.

5. De melding aan de AP bevat ten minste de volgende onderdelen:

    a. de aard van de datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b. de naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen;

c. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

d. de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

MELDEN AAN DE BETROKKENE(N)

Het is belangrijk dat betrokkenen snel en adequaat over het datalek worden geïnformeerd. Dit biedt de betrokkenen de mogelijkheid om maatregelen te nemen om eventuele schade te voorkomen of te beperken. Tevens verkleint dit de kans op reputatieschade, financiële schade en/of andere schade van de schietsport in het algemeen en van de KNSA en de Vereniging in het bijzonder.

De aard van de datalek en de gevolgen daarvan spelen een belangrijke rol in het besluit of en zo ja op welke manier moet worden gemeld. De melding kan schriftelijk (e-mail of per post) en/of telefonisch plaatsvinden.

Artikel 34 van de AVG bepaalt wanneer en op welke manier een datalek aan de betrokkene moet worden gemeld. De belangrijkste vereisten zijn de volgende:

1. Wanneer het datalek "waarschijnlijk een hoog risico inhoudt" voor de betrokkene, deelt de Vereniging de betrokkene de inbreuk in verband met persoonsgegevens mee.

2. De melding aan de betrokkene dient "onverwijld" plaats te vinden.

3. De melding aan de betrokkene is opgesteld in eenvoudige en duidelijke taal.

4. De melding aan de betrokkene bevat ten minste de onderdelen zoals vermeld in § 4 ("Melden aan de Autoriteit Persoonsgegevens") nummer 5 b – d.

In de volgende gevallen is het *niet* nodig om de betrokkene te informeren:

1. Er zijn passende technische en organisatorische maatregelen genomen (bijvoorbeeld encryptie of hashing);

2. De verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om te zorgen dat het risico zich waarschijnlijk niet meer zal voordoen.

3. Het melden aan betrokkene vergt onevenredig veel inspanning; in dat geval kan worden volstaan met een openbare mededeling.

CYBERCRIME, RANSOMWARE

Ingeval van een cybercrime (waaronder een hack) wordt door de Voorzitter en/of de Secretaris de verzekering geïnformeerd. Tevens wordt dan de afweging gemaakt of aangifte bij politie moet plaatsvinden.

Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'. Betalen blijkt echter niet (altijd) tot ontsluiting van de computer te leiden. Wanneer er sprake is van ransomware, zal dit te allen tijde gemeld worden aan de AP.

INFORMEREN VAN DERDEN

In geval van (grootschalige) datalekken kan de Voorzitter en/of de Secretaris contact opnemen met de pers om ze te informeren. Het is belangrijk om de volgende aspecten in overweging te nemen:

(i) De Vereniging is transparant;

(ii) De Vereniging biedt excuses aan en legt uit dat er wordt gewerkt aan een betere beveiliging;

(iii) De Vereniging geeft in heldere taal aan welke stappen de betrokkenen zelf kunnen nemen om de schade te beperken;

(iv) De Vereniging biedt de gedupeerden, waar nodig, iets extra's aan. Bijvoorbeeld een rechtstreeks nummer waar ze terecht kunnen met vragen.

BOETE

Bij overtreding van de meldplicht datalekken kan de AP een (hoge) boete opleggen. De kans op een boete is groter bij niet melden dan bij wel melden.

EVALUEREN

Na het afsluiten van het proces van afhandeling van het datalek zal de FG een evaluatie moment initiëren. Doel is om het proces te evalueren en verbeteracties te adresseren. Van deze evaluatie wordt een verslag gemaakt en door de FG bewaard.

* * *