Hockeyvereniging Bleiswijk

Protocol melden datalekken

Sinds 2016 bestaat er een meldplicht voor datalekken. Deze meldplicht is in de nieuwe Algemene Verordening Gegevensbescherming (AVG) overgenomen en uitgebreid. Organisaties moeten ieder datalek documenteren en/of onder omstandigheden melden bij de Autoriteit Persoonsgegevens en de betrokken personen.

Er is sprake van een datalek (in AVG terminologie: een inbreuk in verband met persoonsgegevens) als het gaat om verlies of andere onrechtmatige verwerking van persoonsgegevens, zonder dat dit de bedoeling is.

Er is sprake van verlies, als:
• Niemand binnen HVB nog (toegang tot) de originele persoonsgegevens heeft; en
• Er geen complete en actuele reservekopie van de persoonsgegevens meer is.

Een onrechtmatige verwerking kan bestaan uit:
• onrechtmatige aantasting van persoonsgegevens (bij versleuteling);
• onbevoegde kennisneming van/inzage in de persoonsgegevens;
• onrechtmatige wijziging van de persoonsgegevens;
• onrechtmatige verstrekking van persoonsgegevens.

Er zijn veel oorzaken te noemen van een datalek. Denk bijvoorbeeld aan:
• moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
• technisch falen (ICT-storingen);
• menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username en/of wachtwoord aan collega's en externen);
• calamiteit (brand datacentrum, wateroverlast)
• verloren USB stick of laptop;
• verzenden van e-mail met zichtbaar de e-mailadressen van alle geadresseerden;
• andere onrechtmatige verwerkingen van gegevens.

Niet elk datalek hoeft gemeld te worden. In het geval van een (vermoeden van) een datalek moet er zorgvuldig gehandeld worden. Met behulp van dit protocol kan bepaald worden of er sprake is van een datalek en zo ja, of dit gemeld moet worden. Snel handelen is hierbij belangrijk, want een melding moet binnen 72 uur gedaan worden.

Om het proces omtrent datalekken vlot en efficiënt te laten verlopen, worden alle (mogelijke) datalekken behandeld door het Meldpunt Datalekken Hockeyvereniging Bleiswijk (MDH). De leden van het MDH zijn:
• Penningmeester: Sjoerd Bosch penningmeester@hvbleiswijk.nl
• Voorzitter: Martijn Kruijt voorzitter@!hvbleiswijk.nl

Iedereen die een datalek ontdekt of vermoedt dat er een datalek heeft plaatsgevonden, meldt dit direct bij het MDH.

Procedure

1. Een mogelijk datalek kan door HVB, één van haar leden of andere betrokkenen worden ontdekt.
2. HVB één van haar leden of andere betrokkenen dienen bij een mogelijk datalek dit direct te melden bij het MDH.
3. Het MDH zal direct de melding in behandeling nemen en beoordelen.

4. In het geval het datalek één of meer specifieke leden of andere betrokkenen raakt, worden deze binnen 36 uur ingelicht.
5. In het geval er een datalek wordt geconstateerd wordt binnen 72 uur de Autoriteit Persoonsgegevens ingelicht.
6. Het MDH zal, na onderzoek te hebben gedaan, direct maatregelen treffen tegen het datalek.
7. Het MDH zal een volledige documentatie maken van het voorgevallen datalek.

Verantwoordelijkheden

Elke vrijwilliger en/of lid van HVB dient op de hoogte te zijn van het protocol.
Dit protocol wordt opgenomen op de website van de website van HVB
https://www.hvbleiswijk.nl/site/Default.asp onder het kopje clubinfo statuten en reglementen.

Protocol Datalekken

STAP 1: Is er een inbreuk op de beveiliging?

Er is geen inbreuk op de beveiliging als er slechts sprake is van een dreiging of een tekortkoming in de beveiliging van de gegevens. Er moet zich daadwerkelijk een incident hebben voorgedaan.

• Vul vraag 1 en 6 van de Vragenlijst Beveiligingsincident in.
• Ga door naar stap 2 als er een inbreuk op de beveiliging is geweest.

STAP 2: Zijn er persoonsgegevens gelekt?

Er is alleen sprake van een datalek als er persoonsgegevens worden gelekt, dat wil zeggen gegevens waarmee natuurlijke personen direct of indirect kunnen worden geïdentificeerd. NB: dit is een ruim begrip waar bijv. ook IP adressen onder vallen. Ogenschijnlijk anonieme data kunnen alsnog vaak tot identificatie van personen leiden.

• Vul vraag 7 van de Vragenlijst Beveiligingsincident in.

STAP 3: Van wie zijn er gegevens gelekt?

De plicht om datalekken te documenteren en te melden ligt bij de verwerkingsverantwoordelijke. HVB is verwerkingsverantwoordelijke en is sommige gevallen verwerker.

• Bepaal met behulp van de verwerkingsregisters welke verantwoordelijkheid HVB heeft voor de gelekte gegevens (verwerkingsverantwoordelijke of verwerker).
• Zijn er gegevens gelekt waarvan HVB verwerker is? Meld het lek dan direct aan de betreffende verwerkingsverantwoordelijke. Hier kan eventueel een ingevulde Vragenlijst Beveiligingsincident voor gebruikt worden.
• Zijn er gegevens gelekt waarvan HVB verwerkingsverantwoordelijke is? Ga dan door naar stap 4.

STAP 4: Kan worden uitgesloten dat er onrechtmatig persoonsgegevens zijn verwerkt?

Soms kan worden uitgesloten dat de persoonsgegevens onrechtmatig zijn verwerkt. Er is sprake van onrechtmatige verwerking als de persoonsgegevens zijn gestolen, als ze door een onbevoegde zijn gelezen, gekopieerd of gewijzigd, of als de gegevens zijn verwijderd of vernietigd zonder dat dit de bedoeling is.

• Bepaal of de onrechtmatige verwerking van persoonsgegevens uitgesloten kan worden. Bijvoorbeeld door logs waaruit blijkt dat er geen persoonsgegevens toegankelijk zijn geweest door een onbevoegde.
• Kan onrechtmatige verwerking worden uitgesloten? Dan is er geen sprake van een datalek.
• Kan onrechtmatige verwerking niet worden uitgesloten? Er is sprake van een datalek. Ga door naar stap 5.

STAP 5: Melding bij de Autoriteit Persoonsgegevens

Een datalek moet aan de Autoriteit Persoonsgegevens (AP) gemeld worden, tenzij het datalek waarschijnlijk geen risico inhoudt voor de rechten en vrijheden (de privacy) van natuurlijke personen.

- Vul vraag 2, 3, 8 & 10 van de Vragenlijst Beveiligingsincident in.
- Bepaal aan de hand van alle tot nu toe ingevulde vragen of het datalek een risico inhoudt voor de rechten en vrijheden van de betrokken personen.
- Indien het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen, meld dan het datalek aan de Autoriteit Persoonsgegevens via het meldloket datalekken.

STAP 6: Melding aan de betrokken personen

Soms moet een datalek ook gemeld worden aan de betrokken personen. Dit is het geval als het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De Autoriteit Persoonsgegevens kan ook aan organisaties opleggen om een datalek te melden aan de betrokkenen.

- Neem contact op met de Autoriteit Persoonsgegevens om te controleren of het datalek aan de betrokken personen gemeld moet worden.
- Als het datalek aan de betrokken personen gemeld moet worden, dan moet de melding ten minste het volgende bevatten:
    - de naam en contactgegevens van het contactpunt binnen HVB waar de betrokkenen meer informatie kunnen verkrijgen over het datalek;
    - de waarschijnlijke gevolgen van het datalek;
    - de maatregelen die HVB heeft voorgesteld of genomen om het datalek aan te pakken, waaronder maatregelen om de nadelige gevolgen te beperken.

STAP 7: Intern documenteren

Ieder datalek moet intern gedocumenteerd worden, ook als het datalek niet gemeld hoeft te worden.

- Vul alle resterende vragen van de Vragenlijst Beveiligingsincident in.

Protocol Datalekken HVB

Hockeyvereniging Bleiswijk

Bijlage: Vragenlijst Beveiligingsincident

Deze vragenlijst is gebaseerd op het meldformulier datalekken van de Autoriteit Persoonsgegevens.
Gegevens van de organisatie (de VERWERKINGSVERANTWOORDELIJKE):

Naam organisatie: ……
Adres: ……
Postcode en plaats: ……
Actief in de sector: ……

De contactperso(o)n(en) bij VERWERKINGSVERANTWOORDELIJKE voor de meldplicht datalekken:

Naam: ……
Functie: ……
E-mailadres: ……
Telefoonnummer(s): ……
VERWERKER zal bij een Beveiligingsincident de volgende vragen beantwoorden:

1. Geef een omschrijving van het Beveiligingsincident:
……..
(bijvoorbeeld “gestolen laptop met klantgegevens” of “een hack op systeem [X]” of “inloggegevens verstuurd naar ontvanger Y ipv X”)

2. De persoonsgegevens van hoeveel personen zijn getroffen door het Beveiligingsincident?
……..
(geef een minimum en maximum aantal aan)

3. Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.
……..
(bijvoorbeeld sollicitanten of cliënten van VERWERKINGSVERANTWOORDELIJKE)
Is er sprake van één van deze specifieke groepen personen (omcirkel het antwoord):
Ouderen: JA / NEE
Kinderen: JA / NEE
Zieken of mensen met een verstandelijke beperking: JA / NEE

4. Datum en tijdstip van het incident:
……..
(kan een vast tijdstip zijn of een periode, als dit niet bekend is “onbekend” invullen)

5. Wanneer is het beveiligingsincident ontdekt?
……..

6. Wat is de aard van de inbreuk? Omcirkel de antwoorden en vul in waar nodig
Kan een onbevoegde de gegevens lezen: JA / NEE
Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: JA / NEE
Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bijv. hack in het systeem): JA / NEE
Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd (bijv. ransomware of brand datacenter): JA / NEE

Zijn de gegevens gestolen: JA / NEE
Overig: ……
(invullen, of als de aard niet bekend is: “onbekend” invullen)

7. Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:
Naam-, adres- en woonplaatsgegevens: JA / NEE
Telefoonnummer: JA / NEE
E-mailadres of andere adres voor elektronische communicatie: JA / NEE
Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer): JA / NEE, zo ja;
welke gegevens zijn het: ……(invullen)
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer): JA / NEE
Burgerservicenummer (BSN) of sofinummer: JA / NEE
Paspoortkopieën of kopieën van andere legitimatiebewijzen: JA / NEE
Geslacht: JA / NEE
Geboortedatum en/of leeftijd: JA / NEE
(Pas)foto: JA / NEE
Geboorteland: JA / NEE
Medische gegevens (waaronder ook medicijnen of medische hulpmiddelen): JA / NEE
Biometrische gegevens (bijv. vingerafdruk, DNA): JA / NEE,
zo ja; welke gegevens zijn het: …… (invullen)
Gegevens over schulden/kredieten: JA / NEE
Inkomensgegevens: JA / NEE
Gegevens over iemands betalingsverkeer: JA / NEE
Gegevens over wettelijke vertegenwoordiging (bewindvoerder/mentor): JA / NEE
Verslavingsgegevens: JA / NEE
School/werkprestaties: JA / NEE
Gegevens over relationele problemen: JA / NEE
Gegevens over (vermoeden van) mishandeling: JA / NEE
Religie: JA / NEE
Strafrechtelijke gegevens (ook bijv. straatverboden): JA / NEE
Politieke overtuiging: JA / NEE
Vakbondslidmaatschap: JA / NEE
Seksuele voorkeur/geaardheid: JA / NEE
Overige persoonsgegevens: …… (invullen)

8. Welke gevolgen kan de inbreuk hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:
Stigmatisering of uitsluiting: JA / NEE
Schade aan de gezondheid: JA / NEE
Kans op identiteitsfraude: JA / NEE
Kans op financiële schade (bijv. fraude met creditcardgegevens): JA / NEE
Blootstelling aan spam of phishing: JA / NEE
Andere gevolgen, namelijk: …….. (invullen)

9. Omschrijf welke technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
……..

10. Zijn de gelekte persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:
Zijn de gegevens versleuteld: JA /NEE,
zo ja; welke versleuteling: …… (invullen)
geldt deze versleuteling voor alle persoonsgegevens of voor een deel? Indien voor een deel, voor welk deel:
…… (invullen)
Zijn de gegevens gehasht: JA /NEE,
zo ja; op welke wijze: …… (invullen)
Kunnen de gegevens vanaf afstand worden gewist: JA /NEE,
zo ja; is dat gebeurd en wanneer is dat gebeurd: …… (invullen)
Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt: JA /NEE,
zo ja; op welke manier: …… (invullen)

11. Zijn er Persoonsgegevens van personen in andere EU-landen getroffen door het Beveiligingsincident? Zo ja, welke uit welke landen:

……..

12. Was er een andere organisatie betrokken bij de inbreuk? Zo ja, welke organisatie was dit en in welke hoedanigheid was deze organisatie betrokken bij de inbreuk?:

……..