EHBO St. Martinus Heeze

Secretariaat: Geldropseweg 61 5591 EB Heeze.
Tel. 040-2265376
E-mail: secretariaat@ehboheeze.nl
Web-site: www.ehboheeze.nl
Bank: Rabobank Dommelstreek.
Rek.nr: NL08 RABO 0120 3049 37
KvK: 40236476

Procedure melden datalek

gebaseerd op de Wet Algemene Verordening Gegevensbeheer (AVG)

Inleiding:
Dit protocol beschrijft de verschillende stappen die binnen EHBO-vereniging St. Martinus Heeze genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De meldplicht datalekken is een verplichting vanwege de Algemene Verordening Gegevens (AVG). Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in de AVG). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking. Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van inlognamen/wachtwoord aan anderen);
- calamiteit (brand, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;
- maar ook het onrechtmatige verwerking van gegevens.

Een datalek moet onverwijld (binnen 72 uur) nadat de verantwoordelijke[1] (1) er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (AP) gemeld worden.
Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van EHBO-vereniging St. Martinus Heeze zijn dit over het algemeen leden. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.
Een bewerker[2] is verplicht om een datalek te melden bij de verantwoordelijke.

Melden:
Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de secretaris. De melding kan door ieder lid en iedere bewerker worden gedaan.

---

[1] Verantwoordelijke: Bestuur EHBO-vereniging St. Martinus Heeze. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten);

[2] Bewerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern). De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid vande verantwoordelijke. De bewerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

De melding kan ook door een externe persoon worden gedaan bij een bestuurslid van EHBO-vereniging St. Martinus Heeze. De melding moet direct en telefonisch worden gedaan bij de secretaris en schriftelijk worden vastgelegd.
Deze meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.
De secretaris legt vast:

- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens vallen onder de melding;
- om welk aantal en/of gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen;
- de contactpersoon voor de melding.

Eerste analyse:
De secretaris en de voorzitter beoordelen of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de secretaris.
Is dit wel het geval, dan voert de secretaris de volgende acties uit:

1. telefonisch informeren voorzitter/secretaris;
2. telefonisch informeren bestuursleden;
3. direct bijeenroepen bestuur.

Bestuur:
Het bestuur wordt met een hoge prioriteit bijeengeroepen door de secretaris. De bijeenkomst wordt voorgezeten door de voorzitter. Het bestuur bespreekt en legt vast:

- de gegevens die door de secretaris zijn vastgelegd bij het aannemen van de melding.;
- de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- hetgeen gemeld gaat worden bij het AP door de secretaris (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):
  - de mogelijke gevolgen voor de betrokkenen;
  - de maatregelen die EHBO-vereniging St. Martinus Heeze neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
  - de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
  - contactgegevens voor betrokkenen;
- de wijze van afhandeling intern, inclusief communicatie naar melder;
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit EHBO-vereniging St. Martinus Heeze zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met een juridisch adviseur;
- hetgeen intern gecommuniceerd wordt, op welk moment;

- hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;
- of naast het AP ook andere stakeholders geïnformeerd worden;
- of er individuen, bedrijven geïnformeerd worden;
- op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;
- of eventuele schade is gedekt door de verzekeringspolis.

Vervolg:
De voorzitter accordeert de uit te voeren activiteiten, zoals door het bestuur vastgesteld, of stelt de uit te voeren activiteiten bij. De door de voorzitter vastgestelde activiteiten worden uitgevoerd.

Melding bij het Autoriteit Persoonsgegevens (AP):
De secretaris meldt binnen 72 uur volgens de aangewezen methode het datalek bij het AP (webformulier AP). In ieder geval zal gemeld moeten worden:

- aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- beschrijving van de te verwachten gevolgen;
- getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- contactgegevens voor betrokkene.

Ontvangstbevestiging Autoriteit Persoonsgegevens (AP):
Is er een melding gedaan, dan ontvangt EHBO-vereniging St. Martinus Heeze een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door het AP, zal het AP contact opnemen met EHBO-vereniging St. Martinus Heeze om de herkomst van de melding te verifiëren.

Afwezigheid secretaris
Bij afwezigheid van de secretaris wordt diens rol ingevuld door de voorzitter. Als deze ook afwezig is, wordt diens rol ingevuld door de penningmeester.

Dit document heet “Procedure melden datalek EHBO-vereniging St. Martinus Heeze” en is vastgesteld in een extra algemene ledenvergadering van EHBO vereniging St. Martinus Heeze op maandag xx oktober 2018.

Heeze, xx oktober 2018.

De voorzitter: De secretaris:

F. van Noort J. Petrillo.