2018

Veluwse Wens Ambulance

Reglement datalekken

STICHTING VELUWSE WENS AMBULANCE

DECEMBER 2018

Inhoudsopgave

1. Inleiding

Dit reglement biedt een handleiding voor de melding, beoordeling en afhandeling van datalekken. Dit document beschrijft de procedure die binnen Stichting Veluwse Wens Ambulance wordt gevolgd bij een datalek en is gebaseerd op de regels van de Algemene verordening gegevensbescherming (AVG). Ter informatie zijn hoofdstukken opgenomen waarin wordt uitgelegd wat een datalek inhoudt, wanneer een melding aan de Autoriteit Persoonsgegevens en/of de betrokkene verplicht is en wat het datalekkenregister inhoudt.

Gebruikte termen in dit document:

- **Persoonsgegeven:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent alle informatie die herleidbaar is naar een individu.
- **Verwerking van persoonsgegevens:** Iedere handeling met persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens.
- **Betrokkene:** de persoon van wie de persoonsgegevens zijn.
- **Datalek:** een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de verwerkte gegevens.
- **Datalekkenregister:** het document waarin de datalekken worden geregistreerd.

2. Datalekken

2.1 Wat zijn datalekken?

De AVG spreekt niet van een datalek, maar van een inbreuk in verband met persoonsgegevens. De benaming komt wel op hetzelfde neer. Er is sprake van een datalek als er een inbreuk is op de beveiliging en die inbreuk leidt daadwerkelijk tot de vernietiging, het verlies, de wijziging, de verstrekking of toegankelijkheid van de verwerkte persoonsgegevens. Het komt er op neer dat persoonsgegevens komen waar zij niet horen.

Het moet dus gaan om:

1. een inbreuk op de beveiliging
2. met daadwerkelijke gevolgen voor de persoonsgegevens.

1. Een inbreuk op de beveiliging kan ten eerste optreden door het tekortschieten van de beveiliging. Het tekortschieten van de beveiliging kan komen doordat bepaalde bestanden niet goed zijn beveiligd of als er menselijke fouten zijn gemaakt. Als er slordig met persoonsgegevens wordt omgegaan, kan er namelijk ook worden gesproken van het tekortschieten van de beveiliging. Een inbreuk op de beveiliging kan ten tweede optreden doordat beveiligingsmaatregelen worden omzeild. In dat geval is de beveiliging niet tekortgeschoten, maar worden de beveiligingsmaatregelen op de een of andere manier omzeild. Een voorbeeld hiervan is als een hacker door de beveiliging van Synctool weet te komen, terwijl Synctool goed is beveiligd.

2. Daadwerkelijke gevolgen voor de persoonsgegevens kunnen zijn dat persoonsgegevens verloren zijn gegaan, vernietigd, gewijzigd, ongeoorloofd verstrekt of er ongeoorloofde toegang tot is.

Voorbeelden van datalekken:

- Laptop met persoonsgegevens wordt gestolen
- Usb-stick met persoonsgegevens raakt kwijt
- E-mail met persoonsgegevens wordt naar de verkeerde ontvanger gestuurd
- Een onbevoegde logt in op Synctool en bekijkt de documenten met persoonsgegevens
- Een onbevoegde hackt Synctool, waardoor jullie zelf niet bij de documenten kunnen
- Het verliezen van documenten met persoonsgegevens

3. Meldpunt datalek

Bij Stichting Veluwse Wens Ambulance is er één centrale plek waar datalekken worden beoordeeld en afgehandeld. Meldingen van een datalek kunnen door vrijwilligers worden ingediend bij het meldpunt datalek:

Kirsten Schutrops
Bestuurslid & vrijwilligersmanager
E-mail: vwm@veluwsewensambulance.nl
Telefoon: 0613784483

Meldingen aan het meldpunt datalek kunnen telefonisch of in persoon geschieden. Op deze manier zorgen we ervoor dat het datalek direct kan worden opgepakt. Voor overige vragen/ opmerkingen en in het geval er geen dringende vragen zijn, kan het meldpunt ook worden bereikt via het e-mailadres dat hierboven staat vermeld.

4. De procedure bij een datalek

Er zijn vier rollen die moeten worden onderscheiden om een datalek succesvol af te handelen:

1. **Ontdekker**: degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt datalek**: een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder:** degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens en/of de betrokkenen. Bij Stichting Veluwse Wens Ambulance is dit het meldpunt datalek.
4. **Technicus (ICT coördinator):** degene die de oorzaak van het datalek kan vinden en kan repareren.

4.1 Welke stappen moeten er worden ondernomen na de ontdekking van een mogelijk datalek?

1. Onmiddellijk nadat een vrijwilliger ontdekt of ter ore komt dat sprake kan zijn van verlies of onrechtmatige verwerking van persoonsgegevens binnen Stichting Veluwse Wens Ambulance, meldt hij dat aan het meldpunt datalek. Vermeld wat er is gebeurd en op welke datum en tijdstip het incident heeft plaatsgevonden. Vermeld ook wat je tot nu toe hebt gedaan om het datalek zo veel mogelijk te beperken.

2. Zorg ervoor dat de gevolgen zo veel mogelijk worden beperkt indien dat mogelijk is.

   Heb je bijvoorbeeld een e-mail met persoonsgegevens naar de verkeerde ontvanger verstuurd? Mail dan direct de persoon waar je onbedoeld een e-mail naar toe hebt gestuurd met de mededeling dat de e-mail niet voor hem of haar was bedoeld en de vraag of hij of zij de e-mail

met inhoud zo snel mogelijk kan verwijderen zonder de inhoud te lezen. Vraag ook of deze persoon een bevestiging kan sturen van de verwijdering van de e-mail.

Het is de vrijwilliger niet toegestaan om het datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkenen te melden. Alleen het meldpunt datalek is hiertoe bevoegd.

4.2 Welke stappen neemt het meldpunt datalek als er een datalek is ontdekt?

1. Het meldpunt datalek neemt de melding in ontvangst en stelt de volgende vragen:
    - Wat is de naam van de melder?
    - Wat is er gebeurd?
    - Wanneer is het gebeurd?
    - Wanneer is het ontdekt?
    - Hoe zijn de gevolgen zo veel mogelijk beperkt?
    - In welke systemen staan deze gegevens?

2. Het meldpunt datalek onderzoekt of er daadwerkelijk sprake is van een datalek. Het meldpunt stelt vast of er sprake is van een datalek.
    - Als een USB-stick kwijt is geraakt, maar er stonden geen persoonsgegevens op, dan heb je wel een beveiligingsincident, maar geen datalek.
    - Een laptop met persoonsgegevens wordt gestolen, maar de laptop is beveiligd door encryptie, dan heb je een beveiligingsincident, maar geen datalek.

3. Indien er is vastgesteld dat er sprake is van een datalek, wordt de technicus gevraagd te achterhalen wat de oorzaak van het datalek is en moet de technicus de oorzaak verhelpen. De technicus wordt natuurlijk alleen ingeschakeld als er sprake is van een technisch incident. De technicus moet vastleggen welke technische en organisatorische maatregelen zijn genomen of zullen worden genomen om de inbreuk te verhelpen en verdere inbreuk te voorkomen.

   Als er een e-mail naar de verkeerde ontvanger is verstuurd, dan kan de technicus daar natuurlijk niks aan verhelpen.

4. Het meldpunt datalek maakt een afweging of dit datalek moet worden gemeld bij de Autoriteit Persoonsgegevens. Indien een melding nodig is, draagt het meldpunt datalek zorg voor de melding aan de Autoriteit Persoonsgegevens.

   De melding dient binnen 72 uur na vaststelling van het datalek te gebeuren via het formulier op: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

5. Daarnaast maakt het meldpunt datalek een afweging of dit datalek moet worden medegedeeld aan de betrokkenen. Indien een mededeling nodig is, draagt het meldpunt datalek zorg voor de mededeling aan de betrokkenen.

   De mededeling dient zo snel mogelijk te gebeuren. Gebruik hiervoor het format mededeling datalek aan betrokkene.

6. Leg het datalek vast in het datalekkenregister. Elk datalek/ incident dient te worden geregistreerd, onafhankelijk van de vraag of het datalek moet worden gemeld. Voor de volledigheid worden incidenten ook vastgelegd, zodat we daarvan kunnen leren.

5. De melding

5.1 Dient het datalek te worden gemeld aan de AP?

Hieronder wordt uitgelegd wanneer een datalek dient te worden gemeld bij de Autoriteit Persoonsgegevens (AP). Deze uitleg helpt je bij het maken van die beslissing.

Ieder datalek dient te worden gemeld aan AP, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene.

Er hoeft dus geen melding te worden gedaan aan de AP als het niet waarschijnlijk is dat het datalek een risico meebrengt voor de betrokkenen. Kijk voor deze afweging naar:

- de aard van de persoonsgegevens. Zijn er gewone persoonsgegevens of bijzondere persoonsgegevens gelekt?
- hoe gemakkelijk kan de identiteit van de betrokkene worden afgeleid van de persoonsgegevens die zijn gelekt?
- de omstandigheden van het datalek. Zijn er kwaadaardige bedoelingen geweest bij het datalek?

Door bij jezelf bovenstaande na te gaan, kan je een afweging maken of het datalek een risico vormt voor de betrokkene.

5.2 Dient het datalek te worden medegedeeld aan de betrokkene?

Een datalek dient te worden medegedeeld aan de betrokkene als het datalek waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van de betrokkene.

Er is sprake van een hoog risico als de te verwachten negatieve gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Denk bij negatieve gevolgen aan: betrokkene verliest de controle over zijn persoonsgegevens, discriminatie, identiteitsdiefstal, financiële verliezen of reputatieschade.

Aanwijzingen dat het om een hoog risico gaat:

- Gegevens over ras of etnische afkomst;
- Gegevens over politieke opvatting;
- Gegevens over religie of levensbeschouwelijke overtuiging;
- Gegevens over vakbondslidmaatschap;
- Genetische of biometrische gegevens van een individu;
- Gegevens over gezondheid;
- Gegevens over strafrechtelijke veroordeling, strafbare feiten of daarmee verband houdende veiligheidsmaatregelen hebben een vergelijkbare impact als bijzondere gegevens.
- Inloggegevens en wachtwoorden
- Identiteitsgegevens, bijvoorbeeld paspoort, BSN
- Financiële gegevens van de persoon
- Gegevens waarbij reputatieschade en schaamte kan ontstaan

Daarop zijn uitzonderingen. De mededeling aan de betrokkene is niet vereist wanneer:

- de gelekte persoonsgegevens op een passende wijze zijn beveiligd. Dus wanneer er technische en organisatorische beschermingsmaatregelen zijn genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het datalek betrekking heeft. De persoonsgegevens die zijn gelekt zijn dan onbegrijpelijk voor onbevoegden en misbruik is daardoor uit te sluiten. Hiervan is sprake als de persoonsgegevens zijn versleuteld of als er gebruik is gemaakt van encryptie.
- er achteraf maatregelen zijn genomen om ervoor te zorgen dat het hoge risico voor betrokkenen zich waarschijnlijk niet meer zal voordoen.
- de mededeling een onevenredige inspanning zou vergen. In dat geval komt er in plaats van de mededeling aan de betrokkenen een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

5.3 Welke informatie staat er in de melding of mededeling?

De AVG bepaalt wat er in de melding of de mededeling moet staan.

Melding aan de Autoriteit Persoonsgegevens:

- De aard van het datalek;
- Waar mogelijk de categorieën van betrokkenen en persoonsgegevensregisters in kwestie;
- Het aantal betrokkenen en persoonsgegevensregisters in kwestie (inschatting maken);
- De naam en de contactgegevens van de functionaris gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van het datalek;
- De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het datalek aan te pakken of de maatregelen om de eventuele nadelige gevolgen te beperken.

De melding aan de AP kan worden gedaan via de website:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Mededeling aan betrokkenen
De betrokkenen moeten dezelfde informatie krijgen als de Autoriteit Persoonsgegevens. Let op: De aard van de inbreuk dient in een duidelijke en eenvoudige taal te worden omschreven. Daarnaast moeten er aanbevelingen worden gegeven aan de betrokkene, zodat hij daarmee zelf ook actie kan ondernemen.

Voor de mededeling van een datalek aan betrokkenen heeft Stichting Veluwse Wens Ambulance het format *Mededeling datalek aan betrokkene*. Het format is opgesteld in lijn met de vereisten uit de AVG en kan worden gebruikt voor de mededeling.

5.4 Termijn van de melding en de mededeling

Indien er een datalek heeft plaatsgevonden en er is geconstateerd dat een melding aan de Autoriteit Persoonsgegevens verplicht is, dan moet dit datalek binnen 72 uur nadat het ter kennis is gekomen bij Stichting Veluwse Wens Ambulance worden gemeld aan de Autoriteit Persoonsgegevens.

Indien er een datalek heeft plaatsgevonden en er is geconstateerd dat een mededeling aan de betrokkenen verplicht is, dan moet dit datalek zo snel mogelijk aan de betrokkenen worden medegedeeld.

6. Het datalekkenregister

Welke informatie moet er in het datalekkenregister worden opgenomen?
Ieder datalek moet worden gedocumenteerd, ongeacht of het moet worden gemeld of niet. Bij de documentatie moeten de feiten omtrent het datalek worden vermeld. Daarnaast moeten ook de gevolgen van het datalek en de genomen corrigerende maatregelen worden vermeld. De Autoriteit Persoonsgegevens kan inzicht verlangen in het datalekkenregister, zodat zij kan controleren of er daadwerkelijk op de juiste manier wordt omgegaan met datalekken. Bij Stichting Veluwse Wens Ambulance registreren wij elk datalek en incident voor een volledig overzicht.

Bij Stichting Veluwse Wens Ambulance is naast dit Reglement datalekken ook een datalekkenregister beschikbaar waarin alle datalekken kunnen worden geregistreerd.

7. Afsluiten van het incident/ datalek

Als er een datalek heeft plaatsgevonden gaat het bestuur met elkaar om tafel gaat zitten om te evalueren wat er is gebeurd. Hoe hebben we het incident/ datalek afgehandeld? Hoe kan dit incident in de toekomst worden voorkomen? Wat kunnen we de volgende keer beter doen? Op deze manier willen we datalekken in de toekomst voorkomen.