

Bescherm uw VVE tegen een datalek

Handleiding voor VVE-besturen, met informatie en tips over oorzaken, gevolgen en het voorkomen van datalekken



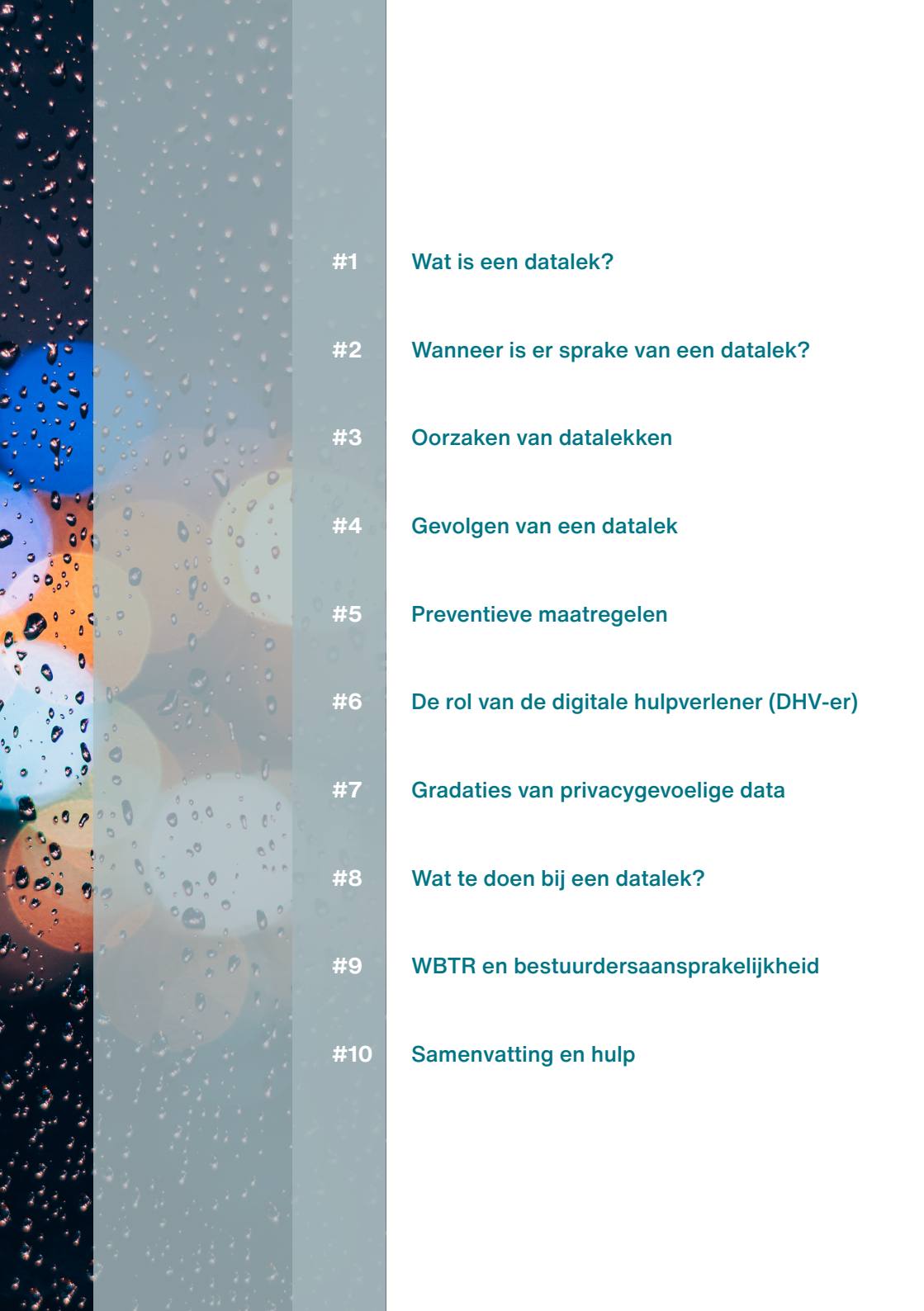
Bescherm uw VVE tegen een datalek

Informatie en tips over oorzaken, gevolgen en het voorkomen van datalekken

Inleiding

Als VVE-bestuurder bent u verantwoordelijk voor de veiligheid van persoonsgegevens die binnen de vereniging worden verwerkt. In een tijd waarin cyberaanvallen en menselijke fouten steeds vaker leiden tot datalekken, is het cruciaal om te weten wat een datalek precies is, hoe u dit kunt voorkomen en niet in de laatste plaats wat u moet bij een datalek of het vermoeden daarvan.

In deze handleiding delen we uitleg en praktische handvatten en preventietips die u direct kunt toepassen om de risico's op datalekken te minimaliseren. Ook leest u informatie over de Digitale Hulpverlener (DHV-er), een rol die vergelijkbaar is met de Bedrijfshulpverlener en hoe een DHV-er uw VVE kan helpen.

- 
- #1 Wat is een datalek?
 - #2 Wanneer is er sprake van een datalek?
 - #3 Oorzaken van datalekken
 - #4 Gevolgen van een datalek
 - #5 Preventieve maatregelen
 - #6 De rol van de digitale hulpverlener (DHV-er)
 - #7 Gradaties van privacygevoelige data
 - #8 Wat te doen bij een datalek?
 - #9 WBTR en bestuurdersaansprakelijkheid
 - #10 Samenvatting en hulp

#1 Wat is een datalek?

Een datalek ontstaat wanneer persoonsgegevens of andere privacygevoelige gegevens per ongeluk of opzettelijk in verkeerde handen vallen. Dit kan gebeuren door technische fouten, cybercrime zoals social engineering, maar ook door menselijke vergissingen zoals verlies van een usb-stick of laptop of het gebruik van een verkeerd e-mailadres.

Een datalek kan ernstige gevolgen hebben voor de betrokkenen, zoals identiteitsdiefstal, financiële schade of reputatieverlies. Voor u en uw medebestuurders kan dit leiden tot verlies van vertrouwen, juridische gevolgen en financiële schade.

Preventietips:

- **Begrijp de risico's:** zorg dat alle bestuursleden weten wat een datalek is en welke gevolgen het kan hebben.
- **Maak duidelijke afspraken:** leg vast wie verantwoordelijk is voor het beheer van persoonsgegevens en wat de procedures zijn bij een vermoeden van een datalek.
- **Gebruik een veilige opslag:** bewaar gevoelige informatie op beveiligde servers en maak gebruik van encryptie om gegevens te beschermen.



#2 Wanneer is er sprake van een datalek?

Een datalek is niet altijd direct zichtbaar. Soms merkt u pas dat er gegevens gelekt zijn als deze al in handen van derden zijn. Het is daarom belangrijk om te weten wanneer u van een datalek kunt spreken en hoe u dit herkent.

Preventietips:

- **Monitor toegang tot gegevens:** gebruik logboeken en toegangsmeldingen om te zien wie toegang heeft gehad tot welke gegevens.
- **Voer regelmatig controles uit:** controleer regelmatig de veiligheid van de systemen en de procedures rondom gegevensbeheer.
- **Herken verdachte activiteiten:** leer bestuursleden om verdachte e-mails en andere vormen van phishing te herkennen.



#3 Oorzaken van datalekken

Datalekken kunnen door verschillende oorzaken ontstaan, van menselijke fouten tot technische tekortkomingen. Het begrijpen van de oorzaken helpt bij het voorkomen van toekomstige lekken.

Preventietips:

- **Zorg voor goede beveiliging:** gebruik sterke wachtwoorden, tweefactorauthenticatie en regelmatige software-updates om systemen te beveiligen.
- **Bewustwording en training:** geef trainingen aan bestuursleden over veilige omgang met gegevens en de risico's van datalekken.
- **Veilige apparatuur:** zorg ervoor dat laptops, usb-sticks en andere apparaten die gevoelige informatie bevatten, altijd beveiligd zijn met wachtwoorden en encryptie.



#4 Gevolgen van een datalek

De gevolgen van een datalek kunnen groot zijn, niet alleen voor de betrokkenen, maar ook voor het bestuur van de VVE. Naast mogelijke boetes en juridische consequenties, kan een datalek leiden tot vertrouwensverlies bij de leden.

Een datalek (of cyberincident) kan dit uitlopen op een aanzienlijke kostenpost voor uw VVE, ter indicatie:

- Herstelwerkzaamheden na een hack, datalek of attack: € 7.000
- Boete van Autoriteit Persoonsgegevens: tot € 820.000
- Inhuren juridisch expert voor hulp bij aangifte datalek: € 240 per uur
- Forensisch onderzoek naar opsporen hack, lek of attack*: € 4.000 per dag
- Kosten van een gestolen of verloren bestand: € 185 per bestand
- Inhuren ICT-expert voor repareren datalek: € 120 per uur

**Als na een datalek persoonlijke dan wel privacygevoelige gegevens op straat komen te liggen, moet u vanwege de privacywetgeving (AGV) aantonen dat u er alles aan heeft gedaan om dit te voorkomen. Ook bent u verplicht een rechercheur in te schakelen die de oorzaak onderzoekt.*

Preventietips:

- **Voer een risicoanalyse uit:** evalueer regelmatig de risico's die uw VVE loopt met betrekking tot datalekken en pas uw beveiligingsmaatregelen hierop aan.
- **Maak een noodplan:** zorg voor een duidelijk stappenplan waarin staat wat er moet gebeuren bij een datalek, inclusief wie er verantwoordelijk is voor welke acties.
- **Communiceer proactief:** zorg ervoor dat de leden van de VVE op de hoogte zijn van de stappen die genomen worden om hun gegevens te beschermen.

#5 Preventieve maatregelen

Het voorkomen van datalekken vraagt om een proactieve benadering. Door preventieve maatregelen te nemen, kunt u de kans op datalekken aanzienlijk verkleinen.

Preventietips:

- **Implementeer sterke wachtwoorden:** gebruik een wachtwoordmanager om sterke, unieke wachtwoorden te genereren en deze veilig op te slaan.
- **Beveilig fysieke documenten:** bewaar geprinte documenten in afsluitbare kasten en zorg dat deze niet onbeheerd worden achtergelaten.
- **Gebruik versleuteling:** versleutel gevoelige gegevens, zowel bij opslag als tijdens verzending, om te voorkomen dat deze door onbevoegden kunnen worden gelezen.



MFA staat voor “Multi-Factor Authentication” of “Meervoudige Authenticatie.”

Het is een beveiligingsmaatregel die wordt gebruikt om de toegang tot online accounts en systemen te versterken. In plaats van alleen een wachtwoord te gebruiken, vereist MFA dat een gebruiker meerdere identificatiemethoden doorloopt om te bewijzen dat ze geautoriseerd zijn.

Wanneer MFA is ingeschakeld, moet een gebruiker tijdens het inlogproces meerdere van deze factoren verstrekken. Dit maakt het veel moeilijker voor kwaadwillende personen om toegang te krijgen tot accounts, zelfs als ze het wachtwoord kennen. MFA is een belangrijke stap om de online beveiliging te verbeteren en wordt sterk aanbevolen voor het beschermen van gevoelige informatie.



#6 De digitale hulpverlener (DHV-er)

De digitale hulpverlener (DHV-er) is vergelijkbaar met die van een bedrijfshulpverlener. De DHV-er zorgt ervoor dat digitale risico's worden geminimaliseerd en dat er snel en effectief, maar vooral juist wordt gehandeld bij cyberincidenten.



Dat doen ze door het signaleren van veiligheidsrisico's, melden incidenten en ondersteunen bestuurders met advies en geruststelling. Hun rol is essentieel voor het creëren van een veiligere digitale omgeving en draagt bij aan een gedeelde verantwoordelijkheid binnen de VVE.

DHV'ers hoeven zeker geen cyberexperts te zijn, maar zijn wel essentieel voor het herkennen van risico's en het ondersteunen van bestuurders in geval van incidenten. Hun rol als ambassadeurs voor digitaal veilig werken en als toegankelijke vraagbaak verlaagt de drempel voor het melden van incidenten aanzienlijk.

Klik hier voor meer informatie op de website van ESET over de DHV-er voor uw VVE.

Preventietips:

- **Stel een DHV-er aan:** kies een bestuurslid of huur een externe expert in die verantwoordelijk is voor digitale veiligheid binnen de VVE.
- **Regelmatige training:** zorg ervoor dat de DHV-er up-to-date blijft met de laatste ontwikkelingen op het gebied van digitale veiligheid en datalekken, ESET ondersteund hierbij.
- **Samenwerking met experts:** werk samen met cybersecurity-experts van ESET, voor specialistische ondersteuning en van Aon over risico-advies.

#7 Gradaties van privacygevoelige data

Niet alle gegevens zijn even gevoelig, maar bepaalde soorten informatie vereisen extra zorg en bescherming. VVE's verwerken vaak verschillende soorten privacygevoelige data, variërend van minder kritieke gegevens tot zeer gevoelige informatie die ernstige gevolgen kan hebben als deze in verkeerde handen valt. Het is belangrijk dat u weet welke gradaties van gegevens uw VVE beheert en welke maatregelen u moet nemen om deze te beschermen.

Het beheer van privacygevoelige gegevens:

1. **Persoonlijke gegevens:** Dit omvat informatie zoals namen, adressen, telefoonnummers en e-mailadressen van de VVE-leden. Hoewel deze gegevens vaak als minder kritisch worden beschouwd, kunnen ze in combinatie met andere informatie waardevol zijn voor kwaadwillende.
2. **Financiële gegevens:**
 - a. Bankgegevens en automatische incasso's: deze informatie kan direct worden misbruikt voor frauduleuze activiteiten, zoals het doen van ongeoorloofde afschrijvingen.
 - b. Geboortedata en paspoortgegevens: deze gegevens kunnen worden gebruikt voor identiteitsfraude, wat grote financiële en persoonlijke schade kan veroorzaken.
3. **Vastgoedinformatie:** Aankoopgegevens, contracten, waardebepalingen, transacties en belangrijke gegevens van uw verzekering: hoewel deze informatie vaak niet direct naar een persoon leidt, kan het inzicht bieden in de financiële status van de VVE, bewoners/huiseigenaren en leveranciers en daarom gevoelige gevolgen hebben bij openbaarmaking.



Preventietips:

- **Classificeer gegevens:** maak een inventarisatie van de gegevens die uw VVE beheert en categoriseer deze op basis van gevoeligheid. Geef hierbij extra aandacht aan financiële en identificatiegegevens.
- **Extra beveiliging voor kritieke gegevens:** versleutel zeer gevoelige gegevens, zoals bankgegevens en paspoortnummers, zowel bij opslag als tijdens verzending.
- **Minimale gegevensverwerking:** verzamel en bewaar alleen die gegevens die strikt noodzakelijk zijn voor de operationele behoeften van de VVE. Vermijd het bewaren van overbodige persoonlijke informatie.
- **Beperk toegang:** zorg ervoor dat alleen bevoegde personen toegang hebben tot de meest gevoelige gegevens. Maak gebruik van rollen en rechten in uw digitale systemen om de toegang tot kritieke informatie te beperken.

Bedrijven of organisaties, dus ook uw VVE die over privacygevoelige gegevens beschikken, zijn wettelijk verplicht om deze koste wat het kost te beschermen.

De AVG maakt onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens (de letterlijke term in de AVG is: 'bijzondere categorieën van persoonsgegevens').

Bijzondere persoonsgegevens zijn gegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Daarom krijgen deze extra bescherming in de AVG.

Gekoppelde (gevoelige) informatie: is direct en elk persoonlijk detail kan worden gebruikt om een persoon te identificeren. Enkele voorbeelden van gekoppelde informatie zijn: voor- en achternaam, thuisadres, e-mailadres, burgerservicenummer, paspoortnummer, rijbewijsnummer, geboortedatum, telefoonnummer en eigendomsbewijzen.

Koppelbare (niet-gevoelige) informatie: is indirect en kan an-sich een persoon niet identificeren. In combinatie met andere informatie kan het wel gebruikt worden om een persoon te identificeren, op te sporen of te lokaliseren. Enkele voorbeelden van koppelbare informatie zijn: voor- of achternaam, straat, huisnummer, postcode, plaats, land, geslacht en ras.

#8 Wat te doen bij een datalek?

Wanneer een datalek plaatsvindt (of het vermoeden daarvan), is het belangrijk om snel en adequaat te handelen. De wet verplicht u om ernstige datalekken te melden bij de autoriteit persoonsgegevens (AP) en om de betrokkenen te informeren.

Preventietips:

- **Stappenplan voor datalekken:** zorg voor een duidelijk plan waarin staat wat er moet gebeuren bij een datalek, inclusief contactpersonen en te nemen acties.
- **Snelle melding bij de AP:** meld een datalek binnen 72 uur na ontdekking bij de autoriteit persoonsgegevens via hun website.
- **Communicatie naar betrokkenen:** informeer de betrokkenen op een transparante manier over het datalek en de maatregelen die worden genomen om de schade te beperken.



#9 WBTR en bestuurdersaansprakelijkheid

Iedere bestuurder, commissaris of toezichthouder loopt een bepaald risico om persoonlijk aansprakelijk te worden gesteld voor financiële schade als gevolg van fouten, verzuim of nalatigheden bij het uitoefenen van de functie. Het ingaan van de Wet Bestuur en Toezicht Rechtspersonen (WBTR) op 1 juli 2021 j.l. heeft gevolgen voor bestuurders van (onder andere) verenigingen en stichtingen.

Waar bestuurders van verenigingen en stichtingen voorheen maar beperkt aansprakelijk waren in privé, zijn zij vanaf nu op dezelfde manier aan te spreken als bestuurders in het MKB. Dit heeft gevolgen voor de statuten van verenigingen en stichtingen, maar dus ook voor de bestuurders zelf.

Advies over uw situatie

Controleer of de verzekerde limiet van uw **bestuurdersaansprakelijkheidsverzekering** is afgestemd op uw huidige situatie en pas deze in overleg met uw Aon contactpersoon aan.



Hoofdstuk 10: Samenvatting en hulp

Datalekken vormen een serieus risico voor uw VVE. Door preventieve maatregelen te nemen, zoals sterke wachtwoorden, veilige omgang met gegevens, en de aanstelling van een digitale hulpverlener, kunt u de kans op een datalek aanzienlijk verkleinen. Mochten er toch gegevens lekken, dan is het essentieel om snel en correct te handelen volgens de wettelijke voorschriften.

Handige linkjes:

- [eBook "Gegevensbescherming voor Dummies"](#): download de handige gids voor iedereen die meer wil leren over gegevensbescherming,
- [Digitale Hulpverlener](#): neem contact op met de cybersecurity specialisten van ESET voor meer informatie over de Digitale Hulp Verlener (DHV-er),
- [Autoriteit Persoonsgegevens](#): informatie over persoonsgegevens op de website van de Autoriteit Persoonsgegevens,
- [WBTR](#): informatie over de Wet Bestuur en Toezicht Rechtspersonen,
- [ESET](#): informatie over datalekken.



Vragen?

Heeft u een vraag over de cyberverzekering of CyberHulp via Aon?

Vul dan het [CyberHulp contactformulier](#) in, dan nemen onze adviseurs contact met u op. Dat kan via telefoon, mail of videochat.

We helpen u graag!

Team Vastgoed en VVE



Over Aon

Aon plc (NYSE: AON) draagt bij aan een betere besluitvorming – om zo het leven van mensen overal ter wereld te beschermen en te verbeteren. Aan de hand van bruikbare analytische inzichten, wereldwijd geïntegreerde expertise op het gebied van menselijk en risicokapitaal én lokaal relevante oplossingen geven onze collega's cliënten in meer dan 120 landen de duidelijkheid en het vertrouwen om betere beslissingen op menselijk en risicogebied te nemen, zodat zij hun bedrijf kunnen beschermen en kunnen laten groeien.

Volg Aon op LinkedIn, X, Facebook en Instagram. Blijf op de hoogte via onze Newsroom en nieuwsbrief.