Security & privacy:

Do's & don'ts

Wanneer je events organiseert en je bezoekers vraagt zich te registreren, ben je officieel persoonsgegevens aan het verwerken. Vanaf dat moment heb je wettelijk gezien bepaalde verantwoordelijkheden omtrent veiligheid en privacy. We leggen uit waar je rekening mee moet houden als eventmanager, en geven je vijf tips om een datalek te voorkomen.

Als eventmanager verzamel, verwerk en gebruik je doorlopend gegevens van bezoekers. Ga maar na: hoeveel registratielijsten heb je op je computer staan? Hoe goed zijn die gegevens beveiligd? Deel je de lijsten met leveranciers, bureaus, registratie- of softwarepartners? Stem je beleid goed af met alle partijen: de meeste datalekken worden immers veroorzaakt door menselijke fouten. Vanaf 2018 is een Europese verordening van toepassing die bestuurders (directie) van een bedrijf aansprakelijk kan stellen voor dergelijke lekken. Met andere woorden: als er iets met de data gebeurt, is dat niet alleen vervelend voor je klanten, maar hangt de organisatie ook een (hoge) boete boven het hoofd.

OPSLAG: BINNEN OF BUITEN DE EU?

Het is belangrijk om te weten waar de registratiegegevens worden opgeslagen: binnen of buiten de EU? De EU heeft strenge privacyregels waardoor de privacy van jouw data gewaarborgd blijft. De VS daarentegen hanteert minder strenge regels, waardoor de Amerikaanse

overheid op eenvoudige wijze toegang tot je data heeft. Dit is niet altijd gewenst.

DATALEK = REPUTATIESCHADE

Sinds 1 januari 2016 hebben bedrijven in Nederland een meldplicht voor datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten maken bij de Autoriteit Persoonsgegevens zodra zich een (ernstig) datalek voordoet. Een datalek betekent dat gegevens van jou en je klanten op straat komen te liggen, doordat er iets mis is gegaan met de beveiliging. Je hebt dus geen controle meer over wie de data in handen krijgt. Soms moet het lek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Dit kan jou als organisatie (of de klant van je eventbureau) ernstige reputatieschade opleveren!

BEPERK HET AANTAL PERSOONSGEGEVENS

Je hebt altijd bepaalde gegevens van je bezoeker nodig; voornaam, achternaam en e-mailadres zijn standaard. Let erop dat je je beperkt tot de gegevens die écht noodzakelijk zijn. Vermijd het verzamelen van paspoort-, creditcard- en medische gegevens: deze zijn zeer gevoelig en vereisen een verhoogd beveiligingsniveau. Hoe dan ook, beveiligd je persoonsgegevens altijd goed. Doe dit met onderstaande tips:

5 TIPS OM JE DATA VEILIG TE BEWAREN

1. Beveilig lijsten met een (sterk) wachtwoord

Wanneer je de eventgegevens in Excel bewaart, beveilig het document dan met een wachtwoord. Met name wanneer je ze gaat mailen naar een leverancier. Verstuur het wachtwoord apart, per SMS. Zo weet je zeker dat alleen jij en de leverancier bij de gegevens kunnen.

2. Werk met veilige eventsoftware (partners)

Wanneer je met eventsoftware of -registratiepartners werkt, vraag dan naar het beveiligingsbeleid dat zij hanteren. Worden de registratiegegevens versleuteld verstuurd tussen website en server? Waar en hoe wordt de data opgeslagen? Verdiep je in het beleid van de betreffende partij, zodat je weet of je jouw data aan hen kunt toevertrouwen!

3. Vermijd gebruik van gratis software

Gratis software is nooit écht gratis. Bij producten voor commercieel gebruik, waarbij niet betaald wordt voor de service, moet je je afvragen hoe het verdienmodel eruit ziet. De kans is aanwezig dat deze bedrijven jouw data doorverkopen aan derden. Immers, klantgegevens zijn een hoop geld waard! Overweeg goed of je jouw zakelijke database wilt delen met een gratis service.

> **"Zonder goede bewustwording kun je niet voldoen aan privacywetgeving. Zorg daarom altijd dat je weet waarom je welke persoonsgegevens verwerkt."**
>
> Juridisch adviesbureau ICTRecht

4. Sla je wachtwoorden niet op in de browser

Wanneer je software gebruikt waarin jouw eventdata is opgeslagen, sla dan de inloggegevens niet op in de browser. Stel dat je iemand je computer weet te bemachtigen, dan kan deze persoon met één klik bij de meest waardevolle data. Ja, het kan vervelend zijn om het wachtwoord steeds opnieuw in te typen, maar het wachtwoord is er niet voor niets!

5. Sluit een verwerkersovereenkomst met je leverancier(s)

Vanaf 25 mei 2018 zal de Algemene Verordening Gegevensbescherming van toepassing zijn. Volgens deze nieuwe verordening ben je verplicht om met iedere 'verwerker van persoonsgegevens' (bijvoorbeeld een extern marketingbureau of een webontwikkelaar) een verwerkersovereenkomst af te sluiten wanneer je persoonsgegevens door hen laat verwerken. Hierin wordt vastgelegd op welke manier bepaalde gegevens verwerkt worden en wat de consequenties zijn in geval van incidenten.

CONCLUSIE

Als eventmanager draag je een belangrijke verantwoordelijkheid voor de gegevens van jouw relaties. Door allerlei richtlijnen wordt het steeds belangrijker dat je hier zorgvuldig mee omspringt. Verdiep je dus tijdig in je leveranciers en partners en beveilig je eigen gegevens goed, zodat je je nergens zorgen over hoeft te maken.

Rutger Bremer is managing director van Momice. Zijn bedrijf ontwikkelt alles-in-1-software voor eventprofessionals. Reageren? Stuur een mail naar rutger@momice.com.