Dataveiligheid Checklist:

Voldoet mijn nieuwe softwarekeuze aan mijn beveiligingseisen?

In een tijd waarin dataveiligheid essentieel is, wil je ook kunnen inschatten of jouw (nieuwe) software keuze voldoet aan je beveiligingsnormen. Vooral bij event software worden talloze personlijke gegevens verwerkt. Onze checklist helpt je hierbij. Start met afvinken en versterk jou beveiliging aanpask nu!

Maar eerst: Hoe 'streng' zijn jouw beveiligingseisen?

De ISO 27001 is dé internationale standaard voor beveiliging, inclusief AVG-naleving. Voor event organisaties is dit natuurlijk van groot belang. Toch streven sommigen naar extra veiligheid. Voor wie nog verder wil gaan in beveiliging, zijn er extra maatregelen naast deze certificatie. Bedenk zelf wat je behoeften zijn, check de software die je in gedachte hebt en doorloop de checklist.

Ondenk hoe aanmelder.nl zorgt voor goede beveiliging binnen onze event software? Stuur een email naar **sales@aanmelder.nl**, laat je vraag of opmerking achter en kom in contact met onze experts!

Certificering

☐ **Check 1:** Heeft de leverancier een ISO 27001 certificatie?

Check! Als je dit hebt afgevinkt, zijn er meer checks onderweg. Blauwe achtergrond? Dat kun je verwachten bij een ISO certificatie. Witte achtergrond? Die bieden extra opties voor geavanceerde informatiebeveiliging.

Tip: Wanneer mogelijk, kies voor een recente variant zoals de ISO 27001:2022 certificatie.

Compliance met GDPR/AVG

☐ **Check 2:** Voldoet de leverancier aan de AVG en bieden zij een DPA?

Veilige gegevens (zowel het invoeren als uploaden)

☐ **Check 3:** Wordt er binnen de software gebruikgemaakt van veilige methoden voor het inlezen van gegevens en vermeden van fysieke media, zoals versleutelde verbindingen (HTTPS) en versleutelde upload- en download mogelijkheden?

Dataopslag en Hosting

☐ **Check 4:** Is de opgeslagen data binnen de software versleuteld, zowel in rust als tijdens transport?

☐ **Check 5:** Controleer waar de data wordt gehost (bijvoorbeeld in de VS of in de EU). Geef eventueel voorkeur aan hosting in de EU vanwege strengere gegevensbescherming.

☐ **Check 6:** Vraag naar de wijze van versleuteling en de beheerprocedures van encryptiesleutels. Heeft de leverancier bijvoorbeeld deelnemer data extra encrypted waardoor data onbruikbaar wordt bij een eventueel datalek?

Toegangsbeheer en Authenticatie / logging en monitoring

- [ ] **Check 7:** Zijn er sterke wachtwoord beleidsregels geïmplementeerd en is multi-factor authentication (MFA) mogelijk?
- [ ] **Check 8:** Kan toegang op basis van rol op accountniveau beperkt worden?
- [ ] **Check 9:** Worden er Single sign-on (SSO) mogelijkheden geboden?
- [ ] **Check 10:** Is er uitgebreide logging en monitoring van toegangspogingen en data wijzigingen en worden er aanvullende monitoring tools gebruikt om verdachte activiteiten snel te detecteren?

Beveiliging van (e-mail) communicatie

- [ ] **Check 11:** Vermijd het e-mailen van gevoelige gegevens. Gebruik beveiligde portals of bestandsuitwisselingssystemen (tip voor intern gebruik, maar ook binnen de software).
- [ ] **Check 12:** Kies een software die gebruikmaakt van extra e-mail encryptie en phishing-bescherming.
- [ ] **Check 13:** Wordt er gebruikgemaakt van beveiligde netwerken (bijvoorbeeld door VPN's).
- [ ] **Check 14:** Zijn er firewalls en IDS /IPS systemen geïmplementeerd?

Incidentbeheer en Herstel

- [ ] **Check 15:** Is er een duidelijk Incident Response Plan (incl. duidelijke communicatieprocedure?)
- [ ] **Check 16:** Worden er regelmatig back-ups gemaakt van alle kritieke gegevens en zijn de procedures aanwezig om data snel te herstellen bij verlies?

Privacy en Gebruikersbescherming

- [ ] **Check 17:** Worden er alleen noodzakelijke gegevens verzameld en bewaard voor het doel waarvoor ze bestemd zijn?
- [ ] **Check 18:** Zijn er beleidsregels voor de bewaartermijn / tijdige verwijdering van deze gegevens?
- [ ] **Check 19:** Worden gevoelige gegevens waar mogelijk geanonimiseerd of gepseudonimiseerd?

Evaluatie, audits en tests voor continue verbetering

- [ ] **Check 20:** Worden er regelmatig interne beveiligings audits uitgevoerd om beveiligingsmaatregelen te evalueren?
- [ ] **Check 21:** Worden er regelmatig externe beveiligings audits uitgevoerd en worden de resultaten door de leverancier gebruikt om continu verbeteringen door te voeren?
- [ ] **Check 22:** Worden er regelmatig penetratietests uitgevoerd én worden de inzichten hiervan gebruikt ter verbetering?

En verder?

Binnen je eigen organisatie is het altijd goed om deze punten in gedachten te houden:

- [ ] **Tip 1:** Zorg voor regelmatige beveiligingstraining voor alle medewerkers.
- [ ] **Tip 2:** Stimuleer een cultuur van bewustzijn en verantwoordelijkheid omtrent gegevensbeveiliging.

Klaar?

Nu je alle checks doorlopen hebt, heb je een goed beeld van de mate van beveiliging bij jouw (gekozen) event software. Ben je benieuwd hoe aanmelder.nl zorgt voor goede beveiliging binnen onze event software? Stuur een email naar **sales@aanmelder.nl**, laat je vraag of opmerking achter en kom in contact met onze experts!

aanmelder.nl is een softwarepartner met een passie voor dataveiligheid voor evenement organisatoren. Zet vandaag nog de volgende stap in het versterken van je dataveiligheid!

aanmelder.nl