Data Security Checklist

Does my new software choice meet my security requirements?

In a time where data security is essential, you also want to assess whether your (new) software choice meets your security standards. This is especially important for event software, which processes numerous personal data. Our checklist can help you with this. Start checking off and strengthen your security adjustments now!

But first: How 'strict' are your security requirements?

ISO 27001 is the international standard for security, including GDPR compliance. This is naturally of great importance for event organisations. However, some strive for extra safety. For those who want to go further in security, there are additional measures beyond this certification. Consider what your needs are, check the software you have in mind, and go through the checklist.

Curious how aanmelder.nl ensures good security within our event software? Send an email to sales@aanmelder.nl, leave your question or comment, and get in touch with our experts!

Certification

- [ ] **Check 1:** Does the supplier have an ISO 27001 certification?

Check! If you've ticked this off, more checks are on the way. Blue background? This can be expected with an ISO certification. White background? They offer additional options for advanced information security.

Tip: When possible, opt for a recent version such as the ISO 27001:2022 certification.

Compliance with GDPR

- [ ] **Check 2:** Does the supplier comply with the GDPR and do they offer a Data Processing Agreement (DPA)?

Secure data (both input and upload)

- [ ] **Check 3:** Does the software use secure methods for data input and avoid physical media, such as encrypted connections (HTTPS) and encrypted upload and download capabilities?

Data storage and Hosting

- [ ] **Check 4:** Is the data stored within the software encrypted both at rest and in transit?
- [ ] **Check 5:** Verify where the data is hosted (for example, in the US or in the EU). Preferably opt for hosting in the EU due to stricter data protection regulations.
- [ ] **Check 6:** Ask about the encryption methods and key management procedures. For instance, does the supplier have additional encryption for participant data, rendering the data unusable in case of a data breach?

Access Control and Authentication / Logging and Monitoring

- [ ] **Check 7:** Are strong password policies implemented and is multi-factor authentication (MFA) enabled?
- [ ] **Check 8:** Can role-based access be restricted at the account level?
- [ ] **Check 9:** Are Single Sign-On (SSO) capabilities provided?
- [ ] **Check 10:** Is there comprehensive logging and monitoring of access attempts and data changes, and are additional monitoring tools used to quickly detect suspicious activities?

Security of (Email) Communication

- [ ] **Check 11:** Avoid emailing sensitive information. Use secure portals or file exchange systems (advice for internal use, but also within the software).
- [ ] **Check 12**: Choose software that uses additional email encryption and phishing protection.
- [ ] **Check 13:** Are secure networks used (for example, through VPNs)?
- [ ] **Check 14:** Are firewalls and IDS/IPS systems implemented?

Incident Management and Recovery

- [ ] **Check 15:** Is there a clear Incident Response Plan (including a clear communication procedure)?
- [ ] **Check 16:** Are regular backups made of all critical data, and are there procedures in place to quickly restore data in case of loss?

Privacy and User Protection

- [ ] **Check 17:** Is only necessary data collected and retained for the purpose for which it is intended?
- [ ] **Check 18:** Are there policies for data retention periods / timely deletion of this data?
- [ ] **Check 19:** Is sensitive data anonymised or pseudonymised where possible?

Evaluation, Audits and Tests for Continuous Improvemen

- [ ] **Check 20:** Are regular internal security audits conducted to evaluate security measures?
- [ ] **Check 21:** Are regular external security audits conducted and are the results used by the provider to continuously make improvements?
- [ ] **Check 22:** Are regular penetration tests conducted and are the findings used for improvement?

And furthermore?

Within your own organisation, it is always good to keep these points in mind:

- [ ] **Tip 1:** Ensure regular security training for all employees.
- [ ] **Tip 2:** Foster a culture of awareness and responsibility regarding data security.

Ready?

Now that you have gone through all the checks, you have a good overview of the level of security in your chosen event software. Curious about how aanmelder.nl ensures robust security within our event software? Send an email to **sales@aanmelder.nl**, leave your question or comment, and get in touch with our experts!

aanmelder.nl is a software partner with a passion for data security for event organisers. Take the next step in strengthening your data security today!

aanmelder.nl