SNiC: ResilIT Privacy Policy

ResilIT Committee

October 2019

This is the privacy policy you, the Attendee, agree to when registering your ticket for the SNiC conference (except for to Section 1.3 which applies to all Attendees), organized by the SNiC foundation (hereafter the Organization).

1 Personal details

1.1 Account information

These are the personal information required to register as an Attendee to the SNiC conference ResilIT. The personal information we save is the full name, study association, study programme, diet preferences and e-mail address.

1.2 Sharing personal information with third parties

The Organization will only share your personal information with third parties when the Organization is legally obliged to do so by the local authorities. At the conference, the Attendee can choose to share their personal information with the companies and third parties present at the conference (Sec. 2). The Organization takes no responsibility for the Attendee's choice to share their personal information with the companies and third parties present at the conference. If the Attendee chooses to opt-in for the speed-dating option with one of the companies present at the conference, their personal information may be shared by the Organization with the chosen company. At the conference, the Attendee can choose to acquire a badge with a scannable QR code. This badge can be scanned by sponsors present at the conference. The Organization will keep a record of whose badges are scanned by which company. By acquiring this badge, the Attendee agrees to share their personal information with the third parties who have scanned the Attendee's badge.

1.3 Photos

This section applies to all Attendees of the conference, regardless of registering their ticket on the website. By attending the conference, the Attendee assigns

any neighbouring rights and/or copyright and/or portrait rights without restriction to the organisation. The photos can be made public on the Organization's present and future websites.

2 GDPR

The Organization is committed to processing personal information in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal personal information shall be:

1. **processed lawfully, fairly and in a transparent manner in relation to individuals;**
2. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;**
3. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**
4. **accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**
5. **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are pro-cessed; personal data may be stored for longer periods insofar as the per-sonal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and free-doms of individuals; and**
6. **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

2.1 General provisions

1. **This policy applies to all personal data processed by the Organization.**
2. **The Responsible Person shall take responsibility for the Organization's ongoing compliance with this policy.**

3. **This policy shall be reviewed at least annually.**

4. **The Organization shall register with the Information Commissioner's Office as an organisation that processes personal data.**

2.2 Lawful, fair and transparent processing

1. **To ensure its processing of data is lawful, fair and transparent, the Organization shall maintain a Register of Systems.**

2. **The Register of Systems shall be reviewed at least annually.**

3. **Individuals have the right to access their personal data and any such requests made to the Organization shall be dealt with in a timely manner.**

2.3 Lawful purposes

1. **All data processed by the Organization must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).**

2. **The Organization shall note the appropriate lawful basis in the Register of Systems.**

3. **Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.**

4. **Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organization's systems.**

2.4 Data minimisation

1. **The Organization shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**

2.5 Accuracy

1. **The Organization shall take reasonable steps to ensure personal data is accurate.**

2. **Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.**

2.6 Archiving / removal

1. **To ensure that personal data is kept for no longer than necessary, the Organization shall put in place an archiving policy for each area in which personal data is processed and review this process annually.**

2. **The archiving policy shall consider what data should/must be retained, for how long, and why.**

2.7 Security

1. **The Organization shall ensure that personal data is stored securely using modern software that is kept up-to-date.**

2. **Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.**

3. **When personal data is deleted this should be done safely such that the data is irrecoverable.**

4. **Appropriate back-up and disaster recovery solutions shall be in place.**

2.8 Breach

1. **In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organization shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).**

3 Cookie notice

The Organization's website only uses functional cookies. Therefore, no authorization by the user is required for its use.