INNOSPOT GmbH

Schedule C – Technical and Organizational Measures

Confidentiality (Art. 32(1) lit. b of the GDPR)

- **Premise access control**
  We prevent unauthorized access to company premises and buildings through technical and organizational measures for access control, in particular for the legitimization of authorized persons.

  INNOSPOT office / internal:
  - The premise is secured through a fence and digital key system (according to standards of a critical infrastructure)
  - Every door to the office rooms is secured by a digital key system with mandatory data updates every 14 days
  - Key assignment only to authorized people via handover documentation
  - Visitors are always accompanied by an INNOSPOT employee

  INNOSPOT Software:
  - There are no servers in the INNOSPOT office. All servers are located in the Amazon Web Services datacenter in Frankfurt am Main. Please find more information in the Amazon Web Services Documents:
    - https://aws.amazon.com/compliance/data-center/data-centers/
    - https://aws.amazon.com/compliance/data-center/controls/

- **System access control**
  We prevent the intrusion of unauthorized persons into the data processing systems through technical and organizational measures regarding user identification and authentication:

  INNOSPOT office / internal:
  - Router with Firewall and WPA2 secured WiFi
  - All systems are password protected
  - Manual for ”Desktop Lock”

  INNOSPOT Software:
  - Connection to systems only possible via SSH certificate (private/public key)
  - Systems placed within a demilitarized zone (DMZ)
  - VPN Connection
  - IP-Restriction to systems
  - API-Request Authentication
  - Administration of user profiles and access rights to systems

- **Admission control**
  We prevent unauthorized activities in data processing systems outside the granted authorizations through a demand-oriented design of the authorization concept and access rights as well as their monitoring and logging:

  - Task-oriented authorizations through Administrator (e.g. people have only access to the data they need to have access to)
  - Limitation of Administrators with full access permissions
  - Privacy compliant password rules
  - Regular evaluations of granted authorizations

  - Deletion of users (e.g. employees after they have left the company)
  - Document shredder (Level 3, crosscut)

- **Separation control**
  Data collected for different purposes will be processed separately:

  - Separation of production and test systems
  - Physical separation of systems, databases and data storages on Amazon Web Services
  - Limitation of purpose of the systems

- **Pseudonymization** (Art. 32(1) lit. a of the GDPR; Art. 25(1) of the GDPR)
  We process personal data in such a way that the data can no longer be assigned to a specific data subject without the use of additional information which is kept separately and is subject to appropriate technical and organizational measures.

Integrity (Art. 32(1) lit. b of the GDPR)

- **Transfer control**
  We ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transfer. Measures during transport, transfer and transmission or storage on data carriers (manual or electronic) as well as during subsequent verification are:

  - Encryption of connections via TSL (SFTP and HTTPS)
  - Tunnel connection (VPN)

- **Input control**
  The traceability and documentation of data management and maintenance is guaranteed through measures for retrospectively examining whether and by whom data have been entered, modified or deleted (e.g. through logging of data modifications, visits and accesses).

Availability (Art. 32(1) lit. b, c of the GDPR)

- **Availability control**
  Data is protected against accidental destruction or loss through measures for data backup (physical / logical):

  - Automatic backup procedures
  - Backup & Recovery concept
  - For the server infrastructure see https://aws.amazon.com/compliance/data-center/controls/

- **Timely restorability / resilience** (Art. 32(1) lit. c of the GDPR)
  We ensure the ‘resilience’ of our processing systems and services through the implemented resilience measures via the high-available cloud infrastructure of Amazon Web Services, redundancy and backups.

Regular Testing, Assessing and Evaluating (Art. 32(1) lit. d of the GDPR)

- **Data protection management**
  We have a strong culture of security awareness within our organization and a dedicated person with day-to-day responsibility for information security and data protection. We make sure this person has the appropriate resources and authority to do his/her job effectively.

  Measures concerning data protection management include:
  - the co-ordination between key people in our organization (e.g. the security manager knows about commissioning and disposing of any IT equipment)
  - the access check to premises or equipment given to anyone outside our organization (e.g. for computer maintenance) and the additional security considerations this will generate
  - periodic checks to ensure that our security measures remain appropriate and up to date.

- **Incident response management**
  We have a procedure in place to detect/identify, report, manage and cure incidents that adversely affect our information security or, more specifically, the rights and freedom of natural persons.

- **Data protection by design/by default** (Art. 25 of the GDPR)
  We are following the data protection by design/by default obligation according to Art. 25 of the GDPR whenever we establish a new or evaluate an existing processing activity. This includes for example the implementation of the principle of data economy ("Datensparsamkeit") and the pseudonymization of data in our systems.

- **Employee training and commitment**
  We ensure that anyone acting under our authority with access to personal data does not process that data unless we have instructed them to do so and that our staff understands the importance of protecting personal data. We provide appropriate initial and refresher training, including:
  - our responsibilities as a data controller under the GDPR
  - staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority
  - the proper procedures to identify callers
  - the dangers of people trying to obtain personal data by deception (e.g. enabling staff to recognize 'phishing' attacks), or by persuading your staff to alter information when they should not do so
  - any restrictions we place on the personal use of our systems by staff (e.g. to avoid virus infection or spam)

  All employees authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- **Job control**
  We ensure the GDPR compliance of processors through technical and organizational measures, including a formalized order management, strict selection of service providers and a clear contract design to avoid unambiguous wording of the contract.