# Willing & Able
# Technical and Organizational Measures

1. **Measures of pseudonymization and encryption of personal data**

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

4. **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. **Measures for user identification and authorisation**

Authentication with username / password

Regular checks of authorisations

Password guideline

Limitation of the number of administrators

Management of rights by system administrator

Differentiation between authorisations

## 6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TLS 1.2 or 1.3)
Use of company internal / restricted drives

## 7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

## 8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

## 9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

## 10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator
Regular training of IT staff

## 11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

## 12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

### 13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

### 14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

### 15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

### 16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure
Legal basis for processing exists for all activities
Documented privacy policy

### 17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests

Secure data erasure and data carrier destruction (certified data erasure and destruction).

18. **For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

Secure data erasure and data carrier destruction (certified data erasure and destruction).
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller