



# **Data Processing Agreement**

and

# **Technical and Organisational Measures (TOMs)**

Encodian Solutions Ltd

**Version: 2.3**

**Last Updated: December 2025**

# Encodian – Data Processing Agreement

## BACKGROUND

- (A) The Customer (defined below) and Encodian (defined below) have entered into a services agreement (**Master Agreement**) that may require Encodian to process Personal Data on behalf of the Customer.
- (B) This Personal Data Processing Agreement (**DPA**) sets out the additional terms, requirements and conditions on which Encodian will process Personal Data when providing services under the Master Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the assimilated EU law version of the General Data Protection Regulation ((*EU*) 2016/679) for contracts between Controllers and Processors and the General Data Protection Regulation ((*EU*) 2016/679).

## AGREED TERMS

### 1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA and in the Background section above.

#### 1.1 Definitions:

**Applicable Laws:** as applicable, Domestic Law or the EU Law.

**Business Purposes:** the Services to be provided by Encodian to the Customer as described in the Master Agreement and any other purpose specifically identified in Part 2 of Annex A.

**Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach and processing** have the meanings given in the Data Protection Legislation.

**Customer:** the organisation purchasing the Services from Encodian and a party to the Master Agreement.

**Customer Personal Data:** any Personal Data which Encodian processes in connection with this DPA in the capacity of a Processor as set out in paragraph 1.2, Part 1 of Annex A.

**Data Protection Legislation:**

(a) the UK Data Protection Act 2018 (**DPA 2018**);

(b) the UK GDPR;

(c) the EU GDPR; and

(d) all other UK, EU and EEA member state laws relating to the processing of Personal Data and privacy.

**Domestic Law:** the law of the UK or a part of the UK.

**EEA:** the European Economic Area.

**Encodian:** Encodian Solutions Ltd, incorporated and registered in England and Wales under company number 10200243, whose registered office is at 20 Wenlock Road, London, N1 7GU.

**Encodian Personal Data:** any Personal Data which Encodian processes in connection with this DPA in the capacity of a Controller as set out in paragraph 1.1, Part 1 of Annex A.

**Encodian Personnel:** all directors, officers, employees, agents, consultants and contractors of Encodian engaged in the performance of its obligations under the Master Agreement or this DPA.

**EU GDPR:** the General Data Protection Regulation ((EU) 2016/679).

**EU Law:** the law of the European Union or any member state of the European Union.

**Records:** has the meaning given in clause 12.1.

**Regulator:** as applicable to the processing, the Commissioner, concerned EEA supervisory authorities and such other regulators with authority to enforce the Data Protection Legislation applicable to the processing.

**Sub-Processor:** has the meaning given to it in clause 8.1.

**UK GDPR:** has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

- 1.2 This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this DPA.
- 1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.
- 1.4 A reference to writing or written includes email.
- 1.5 In the case of conflict or ambiguity between:
  - (a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail; and

- (b) any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail.

## **2. Personal Data types and processing purposes**

- 2.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation.
- 2.2 The Customer and Encodian agree and acknowledge that for the purpose of the Data Protection Legislation:
  - (a) Encodian is the Controller of the Encodian Personal Data;
  - (b) the Customer is the Controller and Encodian is the Processor of the Customer Personal Data;
  - (c) the Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Encodian; and
  - (d) in respect of the Customer Personal Data, Part 2 of Annex A describes the subject matter, duration, nature and purpose of the processing and the Customer Personal Data categories and Data Subject types in respect of which Encodian may process the Customer Personal Data to fulfil the Business Purposes.
- 2.3 Should the determination in clause 2.2 change, then the parties shall work together in good faith to make any change which is necessary to this DPA or the Annexes.

## **3. Encodian's obligations**

- 3.1 Encodian will only process the Customer Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions, unless Encodian is required by any Applicable Laws to otherwise process that Customer Personal Data. Where Encodian is relying on any Applicable Laws as the basis for processing Customer Personal Data, Encodian shall notify the Customer of this before performing the processing required by any Applicable Laws, unless those Applicable Laws prohibit Encodian from so notifying the Customer on important grounds of public interest.
- 3.2 Encodian will not process the Customer Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation.

Encodian shall inform the Customer, if in the opinion of Encodian, the instructions of the Customer infringe the Data Protection Legislation.

- 3.3 Encodian must comply promptly with any Customer written instructions requiring Encodian to amend, transfer, delete or otherwise process the Customer Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.4 Encodian will maintain the confidentiality of the Customer Personal Data and will not disclose the Customer Personal Data to third parties unless the Customer or this DPA specifically authorises the disclosure, or as required by any Applicable Laws, a UK or EU member state court or the Regulator. If any Applicable Laws, an UK or EU member state court or the Regulator requires Encodian to process or disclose the Customer Personal Data to a third party, Encodian must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless any Applicable Laws prohibit the giving of such notice.
- 3.5 Encodian will reasonably assist the Customer, at the Customer's cost, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Encodian's processing and the information available to Encodian, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Regulator under the Data Protection Legislation.
- 3.6 Encodian must notify the Customer of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Encodian's performance of the Master Agreement or this DPA.

#### **4. Encodian Personnel**

Encodian will ensure that the Encodian Personnel:

- (a) are informed of the confidential nature of the Customer Personal Data and are bound by appropriate statutory, common law or contractual confidentiality obligations and use restrictions in respect of the Customer Personal Data;
- (b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Customer Personal Data and how it applies to their particular duties; and
- (c) are aware both of Encodian's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

## 5. Security

- 5.1 Encodian must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Customer Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of the Customer Personal Data. These measures are set out in Annex B.
- 5.2 The Customer acknowledges and agrees that it has reviewed the technical and organisational measures set out in Annex B and confirms that they are appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures.

## 6. Personal Data Breach

- 6.1 Encodian will promptly, and in any event within 48 hours, notify the Customer in writing if it becomes aware of:
- (a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Customer Personal Data. Encodian will restore such Customer Personal Data at its own expense as soon as possible;
  - (b) any accidental, unauthorised or unlawful processing of the Customer Personal Data; or
  - (c) any Personal Data Breach.
- 6.2 Where Encodian becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:
- (a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Customer Personal Data and approximate number of both Data Subjects and the Customer Personal Data records concerned;
  - (b) the likely consequences; and
  - (c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.
- 6.3 Immediately after the Customer has been notified pursuant to clause 6.1, following any accidental, unauthorised or unlawful Customer Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, Encodian will reasonably co-operate with the Customer in the Customer's handling of the matter, including but not limited to:

- (a) assisting with any investigation;
  - (b) facilitating interviews with Encodian Personnel, former Encodian Personnel (where possible) and others involved in the matter including, but not limited to, its officers and directors;
  - (c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and
  - (d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Customer Personal Data processing.
- 6.4 Encodian will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Customer Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by any Applicable Laws.
- 6.5 Encodian agrees that the Customer has the sole right to determine whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Regulator, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice. The Customer shall not offer any remedy to affected Data Subjects without the prior written approval of Encodian, such approval not to be unreasonably withheld or delayed.
- 6.6 The Customer will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 (inclusive), unless the matter arose from Encodian's negligence, wilful default or breach of this DPA, in which case Encodian will cover all of its expenses and time costs.
- 6.7 Encodian will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that Encodian caused such incident and/or Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.5.
- 7. Cross-border transfers of Customer Personal Data**
- 7.1 Encodian (and any Sub-Processor) may transfer or otherwise process the Customer Personal Data outside of the UK or the EEA provided that Encodian shall ensure that all such transfers are effected in accordance with the Data Protection Legislation.

- 7.2 Subject to clause 8.1, Encodian shall and shall ensure that any Sub-Processor shall at their own expense comply with all data protection laws and regulations relating to their activities under this DPA in the jurisdictions in which it and they operate, as such laws and regulations may change from time to time.
- 7.3 Encodian shall notify the Customer in case of any conflict between the laws and regulations in the jurisdictions in which it and any of its Sub-Processors operate and the Data Protection Legislation.
- 7.4 The Customer acknowledges and agrees that it is the responsibility of the Customer to select and configure the data processing of location of Customer Personal Data processed by the Sub-Processor Microsoft Limited.

## **8. Sub-Processors**

- 8.1 The Customer provides its prior, general authorisation for Encodian to appoint any third party or subcontractor (**Sub-Processor**) to process the Customer Personal Data if:
- (a) the Sub-Processor is listed in Part 3 of Annex A or the Customer is provided with an opportunity to object to the appointment of each new Sub-Processor;
  - (b) Encodian enters into a written contract with the Sub-Processor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts;
  - (c) Encodian maintains control over all of the Customer Personal Data it entrusts to the Sub-Processor; and
  - (d) Encodian remains responsible for the acts or omissions of any Sub-Processor as if they were the acts or omissions of Encodian.
- 8.2 Where the Customer objects to the appointment of any Sub-Processor pursuant to clause 8.1(a), Encodian may terminate the Master Agreement with immediate effect by giving written notice to the Customer.

## **9. Complaints, Data Subject requests and third-party rights**

- 9.1 Encodian must, at the Customer's cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

- (a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and
  - (b) information or assessment notices served on the Customer by the Regulator under the Data Protection Legislation.
- 9.2 Encodian must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Customer Personal Data or to either party's compliance with the Data Protection Legislation.
- 9.3 Encodian must notify the Customer immediately if it receives a request from a Data Subject for access to their Customer Personal Data or to exercise any of their other rights under the Data Protection Legislation.
- 9.4 Encodian will give the Customer, at the Customer's cost, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.
- 9.5 Encodian must not disclose the Customer Personal Data to any Data Subject or to a third party other than in accordance with the Customer's written instructions, or as required by any Applicable Laws.

## **10. Term and termination**

- 10.1 This DPA will remain in full force and effect so long as:
  - (a) the Master Agreement remains in effect; or
  - (b) Encodian retains any of the Customer Personal Data related to the Master Agreement in its possession or control.
- 10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Customer Personal Data will remain in full force and effect.

## **11. Data return and destruction**

- 11.1 At the Customer's request, Encodian will give the Customer, or a third party nominated in writing by the Customer, a copy of or access to all or part of the Customer Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

- 11.2 On termination of the Master Agreement for any reason or expiry of its term, Encodian will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Customer Personal Data related to this DPA in its possession or control.
- 11.3 If any law, regulation, or government or regulatory body requires Encodian to retain any documents, materials or Customer Personal Data that Encodian would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Customer Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.
- 11.4 Encodian will certify in writing to the Customer that it has deleted or destroyed the Customer Personal Data within five days after it completes the deletion or destruction.
- 11.5 For the purposes of this clause 11, Encodian shall be deemed to have deleted or destroyed the Customer Personal Data when such Customer Personal Data has been, to the extent technically and legally possible, put beyond further use of Encodian.

## **12. Records**

- 12.1 Encodian will keep detailed, accurate and up-to-date written records regarding any processing of the Customer Personal Data, including but not limited to, the access, control and security of the Customer Personal Data, Sub-Processors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in clause 5.1 (**Records**).
- 12.2 Encodian will ensure that the Records are sufficient to enable the Customer to verify Encodian's compliance with its obligations under this DPA and the Data Protection Legislation and Encodian will provide the Customer with copies of the Records upon request.
- 12.3 The Customer and Encodian must review the information listed in the Annexes to this DPA whenever requested by the Customer to confirm its current accuracy and update it when required to reflect current practices.

## **13. Audit**

- 13.1 Encodian will permit the Customer and/or its third-party representatives to conduct reasonable audits of Encodian's compliance with its obligations under

this DPA, on reasonable written notice at a frequency of not more than once per year.

- 13.2 The frequency restrictions set out in clause 13.1 shall not apply where the Customer is directly required by the Regulator to audit Encodian's compliance with its obligations under this DPA or if there has been, or the Customer reasonably suspects that there has been, a Personal Data Breach.

## 14. Warranties

14.1 Encodian warrants and represents that:

- (a) the Encodian Personnel are reliable and trustworthy and have received the required training on the Data Protection Legislation;
- (b) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and
- (c) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Customer Personal Data and the loss or damage to, the Customer Personal Data, and ensure a level of security appropriate to:
  - (i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;
  - (ii) the nature of the Personal Data protected; and
  - (iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The Customer warrants and represents that Encodian's expected use of the Customer Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

## 15. Limitation of liability

15.1 Nothing in this DPA will exclude, limit or restrict Encodian's liability for:

- (a) death or personal injury caused by its negligence;
- (b) fraud or fraudulent misrepresentation; or
- (c) any other liability which may not be limited or excluded by law.

15.2 Subject to clause 15.1, Encodian shall not be liable to the Customer for any of the following losses or damages, in each case arising out of or in connection with this DPA (including without limitation as a result of breach of contract, negligence or any other tort, under statute or otherwise), and regardless of whether Encodian

knew or had reason to know of the possibility of the loss, injury or damage in question:

- (a) any loss (whether direct or indirect) of revenue or profits;
- (b) any loss (whether direct or indirect) of anticipated savings;
- (c) any loss (whether direct or indirect) of goodwill or injury to reputation;
- (d) any loss (whether direct or indirect) of business opportunity;
- (e) any loss (whether direct or indirect) of or corruption to data, software or information; and/or
- (f) indirect or consequential loss or damage.

15.3 Subject to clauses 15.1 and clause 15.2 the total aggregate liability of Encodian (including, but not limited to, its respective partners, officers, employees, contractors, sub-contractors, Sub-Processors and agents) under or in connection with this DPA whether in contract, tort (including, but not limited to, negligence) or otherwise shall be limited to £50,000 (fifty thousand pounds sterling).

## 16. Notice

16.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and sent by email to the following addresses (or an address substituted in writing by the party to be served):

For the Customer: the email address provided by the Customer to Encodian.

For Encodian: [admin@encodian.com](mailto:admin@encodian.com).

16.2 Any notice shall be deemed to have been received at the time of transmission unless the transmission under clause 16.1 would occur outside business hours in the place of receipt. In such circumstances transmission shall be deferred until business hours resume. In this clause 16.2, business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

16.3 Clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This DPA has been entered into on the date the Master Agreement is executed.

# ANNEX A Personal Data Processing Purposes and Details

## Part 1: Role of the parties

### 1.1 Where Encodian acts as a Controller:

- (a) when processing Encodian Personal Data contained within correspondence between the Customer's staff, Encodian Personnel and/or documents relating to the establishment, management, audit, operation, and communication (on which Encodian may wish to rely on to establish its rights and liabilities under the Master Agreement) in respect of the Master Agreement for the provision of the contracted services; and
- (b) when processing Encodian Personal Data of the Customer's staff for marketing purposes.

### 1.2 Where Encodian acts a Processor:

Save as set out in paragraph 1.1 of this Annex A, when processing the Personal Data of Data Subjects whose Personal Data is collected and/or processed through the services provisioned under the Master Agreement.

## Part 2: Particulars of processing

### 2.1 Subject matter of processing

The performance of Encodian's duties under the Master Agreement.

### 2.2 Duration of processing

For the term of the Master Agreement and for such time afterwards as required for the parties to exercise their rights and obligations under clause 11.

### 2.3 Nature of processing

The processing of Customer Personal Data to enable Encodian to comply with its duties under the Master Agreement.

### 2.4 Business Purposes

To enable Encodian to perform its duties under the Master Agreement.

### 2.5 Personal Data categories

Identity data, image data, contact details and such other Personal Data categories as relevant.

### 2.6 Data Subject types

Clients or customers of the Customer and/or such clients' or customers' staff and such other Data Subjects whose Personal Data is processed by Encodian in connection with the performance of its duties under the Master Agreement.

**Part 3: Approved Sub-Processors:**

Name	Purpose	Data	Location	Legal Basis for Transfer
Microsoft Limited	Encodian services and products are hosted in Microsoft Azure	Any data submitted by the Customer for processing through Encodian products	Subject to clause 7.4, United States, United Kingdom, Switzerland, Germany, Australia, Canada	Article 45 adequacy decision or Standard Contractual Clauses, as applicable
Zendesk, Inc.	Customers may submit information via Zendesk for the purpose of assisting with support requests	Any data submitted by the customer via Zendesk for the purpose of assisting with support requests	Germany	Article 45 adequacy decision

## ANNEX B Technical and Organisational Measures (TOMs)

This document describes the technical and organisational measures implemented by Encodian (and in some cases its Sub-processors) to protect the confidentiality and integrity of personally identifiable information processed via Encodian's products and services pursuant to Article 32 of the UK General Data Protection Regulation as given in s. 3(1) (as supplemented by s. 205(4)) of the Data Protection Act 2018 (UK GDPR) and the General Data Protection Regulation ((EU) 2016/679) (EU GDPR).

### Confidentiality

#### Physical Access Control

Measures suitable for preventing unauthorised persons from gaining entry to data processing systems with which personal data are processed or used.

Technical Measures	Organisational Measure
Alarm System	Visitors' book / Visitors' protocol
Automatic access control system	Key Regulation / List
Manual locking system	Front desk / Reception / Gatekeeper
Safety Locks	Obligation to wear identity badges
Doorbell system with camera	Employee / visitor badges
Video surveillance of the entrances	Visitors accompanied by employees
	Diligent selection of security personnel
	Diligent selection of cleaning services
For Data Centres / Server Rooms	
Access only via personalized transponders / chip cards	Logged access restricted to the most necessary group of persons

## Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorised persons.

Technical Measures	Organisational Measure
Login via username + password	Established role and access rights concepts in IT systems according to need-to-know principle
Hardware and software firewalls for clients and server systems	Creation of user profiles
Access with additional use of two-factor authentication	Central password assignment
Mobile Device Management	Password Security Policy
Anti-Virus-Software Servers	Deletion / Disposal Policy
Anti-Virus-Software Clients	Clear Desk Policy
Anti-Virus-Software for mobile devices	General Data Protection and / or Security Policy
Encryption of data carriers in laptops / notebooks	Mobile Device Policy
Encryption of smartphones	
BIOS protection (separate password)	
Automated patch and vulnerability management on server and endpoint	
Automatic desktop lock	
Encapsulation of sensitive systems through separate network areas (logical segmentation)	
Multiple hardware and software firewall shielding of the customer servers (DMZ)	

Technical Measures	Organisational Measure
File shredder min. recommended security level 3 (cross cut)	Regulation, creation and implementation of authorisation concepts and a regular review of the authorisations
External document shredder (DIN 32757)	Limitation of the number of administrators to the minimum and regular review of the authorisations
Physical destruction of data carriers	Lockable containers at the workplaces
Encryption of data carriers	Password policy including a minimum length and a regular change of passwords
Logging of accesses to applications, specifically when entering, changing, and deleting data	
Secured interfaces (USB, Firewire, Network etc.)	
Logging of the login attempts	
Anti-virus software centrally managed with KPI and regular updates	

## Authorisation Control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that

personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

## Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

Technical Measures	Organisational Measure
Separation of production and test environments	Control via authorisation concept
Physically separated storage on separate redundant systems (depending on the criticality of the systems)	Limitation of database access rights
Logical client separation (software based)	Data records contain attributes for specific purposes / data fields
Segmentation of the different network areas	

## Integrity

### Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures	Organisational Measure
E-mail encryption	Documentation of data recipients as well as the duration of the planned transfer and deletion periods
Logging of accesses and retrievals	Diligent selection of transport personnel and vehicles
Safe transport containers and	Comprehensive logging procedures

packaging	
Transmission of data via encrypted containers / data carriers or tunnel connections	Disposal service provider for professional file and data media destruction
Use of signature procedures	Regulation of the transfer through guidelines

## Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures	Organisational Measure
Technical logging of the entry, modification, and deletion of data	List of applications that can be used to enter, modify, or delete personal data
Manual or automated control of the logs	Traceability of data entry, modification and deletion through individual usernames (not user groups)
	Assignment of rights to enter, modify, and delete data based on an authorisation concept
	Clear responsibility for deletions

## Availability and Resilience

### Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss.

Please note that some of these measures are handed off to Microsoft as our hosting provider.

Technical Measures	Organisational Measure
Fire and smoke detection systems	Backup and recovery concept
Monitoring of temperature and humidity in server rooms	Control of the backup process
Air-conditioning in server rooms	Regular review of data recovery and logging of the results
Interruption-free and redundant power supply	Outsourced storage of data backups
Redundant data connection	
Redundant server system	
Separate partitions for operating systems and data	
Alarm signal in case of unauthorised access to server room	

## Procedures for Regular Review, Assessment and Evaluation

### Data Protection Management

Measures to ensure that the requirements of the U K GDPR and EU GDPR have been verifiably implemented.

Technical Measures	Organisational Measure
Use of software solutions for data protection management	Regular data protection audits
External audit / revision	Internal audit / revision
Security certifications: (e.g. ISO27001)	Regular awareness-raising of employees (at least annually)
Internal Data Protection Officer (DPO)	Internal Information Security Officer (ISO)

Central documentation of all procedures and regulations regarding data protection with access for employees depending on need/ authorisation (e.g. wiki, intranet ...)	Data protection impact assessment (DPIA will be carried out if required)
Formalised process for handling requests regarding data subject rights	Implementation of a data protection management system

## Incident Response Management

Measures to ensure that the data subject is informed after a malfunction or data breach in case the data of the data subject was affected.

Technical Measures	Organisational Measure
Monitoring of data access	Existence of an escalation management
	Involvement of DPO and ISO in security incidents and data breaches

## Data Protection by Default

Measures pursuant to Article 25 UK GDPR and EU GDPR that comply with the principles of data protection by design and by default.

Technical Measures	Organisational Measure
Personal Data is not further processed than necessary regarding the purpose of processing	Automated software support

Simple exercise of the right of withdrawal by the data subject due to technical measures, procedures and data protection regulations including accessibility for employees according to need / authorisation (e.g. wiki, intranet ...)	Manual deletion in accordance with legal requirements
--	---

## Order Control (Outsourcing, Sub-Processors and Order Processing)

Measures to ensure that personal data is only processed on the instructions from the controller in case the processing is to be carried out on behalf of the controller.

Technical Measures	Organisational Measure
Prior examination of the contractor and their security measures as well as it's documentation	Obligation of the contractor's employees to maintain data secrecy
Selection of the contractor according to due diligence criteria (especially with regard to data protection and data security)	Agreement on effective control rights of the controller
Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses	Regulation on the use of further Sub-Processors
No processing except on documented instructions from the controller (data processing agreement – Art. 28 UK GDPR and EU GDPR)	Ensuring the return and/or destruction of data after termination of the contract

In case of long-term processing: Regular audits of the processor and its level of data protection	
---	--