Data Processing Agreement

and

Technical and Organisational Measures (TOMs)

Encodian Solutions Ltd

Title: Data Processing Agreement and Technical and Organisational Measures (TOMs)
Issue Number: V2.1
Issue Date: 27/07/2023
Owner: Operations Manager
Approver: Operations Director
Reference: DOC13
Classification: Public

Encodian – Data Processing Agreement

PARTIES

(1) **ENCODIAN SOLUTIONS LIMITED** incorporated and registered in England and Wales with company number 10200243 whose registered office is at Blythe Valley Innovation Centre Central Boulevard, Blythe Valley Business Park, Solihull, England, B90 8AJ United Kingdom (**Encodian**).

(2) **THE CUSTOMER** Encodian's customer as referred to in the Master Agreement (**Customer**).

BACKGROUND

(A) The Customer and Encodian have entered into a services agreement (**Master Agreement**) that involves Encodian processing personal data on behalf of the Customer.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which Encodian will process personal data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) UK GDPR for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Business Purposes: the services described in the Master Agreement and any other purpose specifically identified in Part 2 of Annex A.

Commissioner: either the EU Commissioner or the UK Commissioner, as relevant.

controller, processor, data subject, personal data, personal data breach and **processing** shall have the meaning given to them in the UK GDPR.

Customer Personal Data: means any personal data which Encodian processes in connection with this Agreement, in the capacity of a processor on behalf of the Customer as set out in paragraph 1.2, Part 1 of Annex A.

Data Losses: any reasonably foreseeable damages or costs incurred by the Customer or any penalties or fines imposed on the Customer by the Commissioner or any equivalent regulator in a jurisdiction other than the UK, such damages, costs, penalties or fines being incurred or imposed as a direct result of Encodian failing to comply with the Data Protection Legislation and/or its obligations under this Agreement.

Data Protection Legislation: all applicable laws and regulations relating to the processing, protection, or privacy of personal data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, the UK GDPR and the EU GDPR.

EEA: means the European Economic Area.

Encodian Personal Data: any personal data which the supplier processes in connection with this Agreement, in the capacity of a controller as set out in paragraph 1.1, Part 1 of Annex A.

EU Commissioner: the relevant supervisory authority of a European Union Member State (Article 4(22) EU GDPR).

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

Records: has the meaning given to it in clause 12.

Term: this Agreement's term as defined in clause 10.

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

UK GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018.

1.2 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.3 A reference to writing or written includes email.

1.4 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail; and

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

2. Personal data types and processing purposes

2.1 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 relation to the Customer Personal Data, Part 2 of Annex A describes the subject matter, duration, nature and purpose of the processing and the personal data categories and data subject types in respect of which Encodian may process the Customer Personal Data to fulfil the Business Purposes.

2.2 Should the determination in clause 2.1(a) or clause 2.1(b) change, then each party shall work together in good faith to make any changes which are necessary to clause 1, clause 2, and/or the Annexes.

2.3 The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Encodian Personal Data and the Customer Personal Data to Encodian and lawful collection of the same by Encodian for the duration and purposes of this Agreement.

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. Encodian will not process the Customer Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. Encodian must notify promptly the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 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.

3.3 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 Agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) 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 the domestic or EU law prohibits the giving of such notice.

3.4 Encodian will reasonably assist the Customer 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 Commissioner under the Data Protection Legislation.

4. Encodian's employees

4.1 Encodian will ensure that all of its employees:

(a) are informed of the confidential nature of the Customer Personal Data and are bound by written 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 Agreement.

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 Customer Personal Data including, but not limited to, the security measures set out in Annex B.

5.2 Encodian must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security 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 un-useability of part or all of the Customer Personal Data. Encodian will restore as soon as possible such Customer Personal Data at its own expense;

(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) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with Encodian's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) 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

(e) 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 domestic or EU law.

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 Commissioner, other in-scope regulators, 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 and time costs associated with the performance of Encodian's obligations under clauses 6.1 to 6.3 inclusive unless the matter arose from Encodian's negligence, wilful default or breach of this Agreement, 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 an 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 personal data

7.1 Encodian may transfer 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 subcontractor shall at their own expense comply with all data protection laws and regulations relating to their activities under this agreement in the jurisdictions in which they operate, as such laws and regulations may change from time to time.

7.3 Encodian shall notify the Customer immediately in case of any conflict between the laws and regulations in the jurisdictions in which it and any of its subcontractors operate and the Data Protection Legislation.

8. Subcontractors

8.1 The Customer hereby provides its prior, general authorisation for Encodian to appoint a third party or subcontractor to process the Customer Personal Data if:

(a) the third party or subcontractor is listed in Part 3 of Annex A or the Customer is provided with an opportunity to object to the appointment of each new third party or subcontractor;

(b) Encodian enters into a written contract with the third party or subcontractor that contains terms substantially the same as those set out in this Agreement, and, upon the Customer's written request, provides the Customer with copies of such contracts;

(c) Encodian maintains control over all Customer Personal Data it entrusts to the relevant third party or subcontractor; and

(d) Encodian remains responsible for the acts and omissions of any such third party or subcontractor as if they were the acts and omissions of Encodian.

8.2 Where the Customer objects to the appointment of any new third party or subcontractor 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 no additional cost to the Customer, 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 Commissioner 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 domestic or EU law.

10. Term and termination

10.1 This Agreement 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 (**Term**).

10.2 Any provision of this Agreement 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.

10.3 If Encodian fails to comply with the terms of this Agreement the Customer may, without prejudice to any other right or remedy available to it, terminate the Master Agreement immediately on written notice to Encodian without further liability or obligation.

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 within 10 working days of such date, return and not retain, all or any of the Customer Personal Data related to this Agreement 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.

12. Records

12.1 Encodian will keep detailed, accurate and up-to-date written records regarding any processing of Customer Personal Data it carries out for the Customer, including but not limited to, the access, control and security of the Customer Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of Customer Personal Data to a third country and related safeguards, 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 Agreement 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 Agreement 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 its third-party representatives to audit Encodian's compliance with its obligations under this Agreement, on at least 10 working days' notice, during the Term. Encodian will give the Customer and its third-party representatives all necessary assistance to conduct such audits at the Customer's cost. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at Encodian's premises or on systems storing the Customer Personal Data;

(b) access to and meetings with any of Encodian personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to process the Customer Personal Data.

13.2 The notice requirements in clause 13.1 will not apply if the Customer reasonably believes that a personal data breach has occurred or is occurring, or Encodian is in material breach of any of its obligations under this Agreement or any of the Data Protection Legislation.

13.3 If a personal data breach occurs or is occurring, or Encodian becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, Encodian will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit as soon as possible and in any event within five working days.

13.4 At the Customer's written request and cost, Encodian will:

(a) conduct an information security audit;

(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit as soon as possible and in any event within five working days.

14. Warranties

14.1 Encodian warrants and represents that:

(a) it and anyone operating on its behalf will process the Customer Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(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 Customer 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 Agreement 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 loss or damage, in each case arising out of or in connection with this Agreement (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 Data Losses (whether direct or indirect);

(f) any loss (whether direct or indirect) of or corruption to data, software or information; or

(g) indirect or consequential loss or damage.

15.3 Subject to clauses 15.1 and 15.2 the aggregate liability of Encodian (including, but not limited to, its respective partners, officers, employees, contractors, directors, sub-contractors and agents) under or in connection with this Agreement 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 Agreement must be in writing and may be 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 of a director or other member of the Customer's management team.

For Encodian: *admin@encodian.com*.

16.2 Any notice by email shall be deemed to have been received at the time of transmission unless the transmission 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 Agreement 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's staff 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 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 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, 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 Subcontractors:

Name	Purpose	Data	Location*	Appropriate safeguards for transfers outside the UK
Microsoft Limited	Encodian services and products are hosted in Microsoft Azure	Examples of data could include: client name, email address, telephone number	United States, United Kingdom, Switzerland, Germany, Australia, Canada * data processing location is dependent on Encodian subscription level purchased.	Standard Contractual Clauses

ANNEX B Technical and Organisational Measures (TOMs)

This document describes the technical and organisational measures implemented by Encodian (and in some cases their sub-processors) to protect the confidentiality and integrity of personally identifiable information processed via Encodian's products and services in pursuant of 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 accompanies 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)	
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.

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	

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 packaging	Comprehensive logging procedures
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 unauthorized 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/ authorization (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 Art 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, Subcontractors 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 subcontractors
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	