DATA PROCESSING AGREEMENT

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the terms of the Agreement.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

"Affiliate"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"Agreement"	means the master services agreement between the Controller and the Processor for the provision of the Services;
"CCPA"	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
"Controller"	means You;
"Data Protection Law"	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Irish Data Protection Act 2018, the EU GDPR, UK GDPR, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the UK Data Protection Act 2018, the FDPA, the CCPA and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011;
"Data Subject"	shall have the same meaning as in Data Protection Law;
"DPA"	means this data processing agreement together with Exhibits A and B;
"EEA"	means the European Economic Area;
"EU GDPR"	means 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, (General Data Protection Regulation);
"FDPA"	means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) and as amended from time to time;
"Personal Data"	shall have the same meaning as in Data Protection Law;

"Processor"	means Us, including as applicable any "Service Provider" as that term is defined in the CCPA;
"Restricted Transfer"	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
"Security Policy"	means the Technical and Organisational Measures document published at https://www.essentialskillz.com/docs, as amended from time to time;
"Services"	means all services and software applications provided to the Controller by the Processor under and as described in the Agreement;
"Sub-processor"	means any person or entity engaged by the Processor or its Affiliate engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;
"Supervisory Authority"	means a governmental or government chartered regulatory body having binding legal authority over a party;
"UK GDPR"	means the EU GDPR 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 2018;

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Your Data on behalf of the Controller. Your Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as may be updated from time to time.

3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process them except on the instructions from the Controller unless he or she is required to do so by any Data Protection Law.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.

4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.7 The technical and organisational measures detailed in Exhibit B shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that

the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

4.8 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.

4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

4.10 The Processor may not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement.

5. Controller Obligations

5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law; (ii) has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-processors, to execute their rights or perform their obligations under this DPA; and
(iii) All Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

5.2 The Controller shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5.3 The Controller acknowledges and agrees that some instructions from the Controller, including assisting the Processor with audits, inspections, DPIAs or providing other assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees for providing such assistance in advance and shall be entitled to charge the Controller for its reasonable costs and expenses in providing any such assistance

6. Sub-processors

6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.

6.2 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3 The Controller authorises the Processor to use the Sub-processors already engaged by the Processor as at the date of the Agreement and the Processor shall make available to the Controller a list of Sub-processors authorised to process the Personal Data which shall include the identities of Sub-processors authorised to process the Personal Data. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-processors before authorising any new or replacement Sub-processor(s) to process Personal Data.

6.4 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, the Controller may terminate the Agreement with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the Term of the Agreement following the effective date of termination with respect to such terminated Services.

6.5 All Sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall prior to the relevant Sub-processor carrying out any processing activities in respect of the Personal Data; (i) appoint each

Subprocessor under a written contract containing materially the same obligations to those of the Processor in this DPA enforceable by the Processor; and (ii) ensure each such Subprocessor complies with all such obligations.

6.6 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-processors are located in a country or territory recognized by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection.

7. Data Subject Access

7.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

7.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

8. Audit

8.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

8.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which will be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

8.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

9. Personal Data Breach

9.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 48 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("**Personal Data Breach**").

9.2 The Processor shall take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Personal Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

10. Compliance, Cooperation and Response

10.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

10.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

10.3 The Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.

10.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

10.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

11. Liability

11.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

11.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

11.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

11.4 The Controller shall not be entitled to recover more than once in respect of the same loss. **12. Term and Termination**

12.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

12.2 The Processor shall at the choice of the Controller, upon receipt of a written request received within 30 days of the end of the provision of the Services, delete or return Personal Data to the Controller. The Processor may contact the Controller to notify them that the Agreement is coming to the end and offer to delete or return Personal Data to the Controller. If the Controller does not: (i) reply to this notice within 30 days; or (ii) request return or deletion of Personal Data within 30 days of the end of the provision of the Services, the Processor shall in any event delete all Personal Data in its systems 30 days after the effective date of termination of the Agreement, subject to the provisions of clause 13.3 below.

12.3 The Processor will delete all copies of Personal Data in its systems 30 days after the effective date of termination of the Agreement unless: (i) applicable law or regulations require storage of the Personal Data after termination; (ii) partial Personal Data of the Controller is stored in backups, then such Personal Data shall be deleted from backups of the Controller's files/folders 5 weeks after the effective date of termination of the Agreement; (iii) the Controller explicitly request that the Processor keeps the Personal Data for a longer period to enable the Controller to retrieve Personal Data prior to deletion by the Processor.

13. General

13.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

13.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

13.3 Subject to any provision to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

12.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Controller:

means You.	
Address:	As set out for You in the Agreement.
Contact person's name, position and contact details:	As provided by You in your account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Role:	Data Exporter.
Name of Representative (if applicable):	Any EU or UK representative named in the Controller's privacy policy.

The Processor:

means Us: Riskwize Limited T/A EssentialSkillz	
Address:	The Hub, Galway Technology Park, Parkmore, Galway, H91 K2WP, Ireland
Contact person's name, position and contact details:	support@essentialskillz.com https://www.essentialskillz.com/contact-us

Activities relevant to the data transferred:	The provision of cloud computing solutions to the Controller under which the Processor processes Personal Data upon the instructions of the Controller in accordance with the terms of the Agreement.
	into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role:	Data Importer

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of data subjects:	Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Controller's prospects, customers, clients, business partners and vendors. Suppliers and service providers of the Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.

Categories of Personal Data:	The Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Controller. The Personal Data includes but is not limited to: ● Personal details, first name, surname, user names, passwords, email addresses, employee ID, structure location (department, team etc.), manager name and ID, IP address and digital signature of Users. ● Personal Data derived from the Users use of the Services such as records and business intelligence information. ● Personal Data within email and messaging content which identifies or may reasonably be used to identify data subjects. ● Metadata including sent, to, from, date, time, subject, which may include Personal Data. ● E-Learning course materials on risk assessment. ● Photographs uploaded via risk assessment. ● File attachments that may contain Personal Data. ● Survey, feedback and assessment responses relating to risk assessment. ● Information offered by users as part of support enquiries. ● Other data added by the Controller from time to time.
Sensitive Data:	Personal data transferred includes but is not limited to the following special categories of data: ● Data concerning health, where this is provided by the end-user in response to a risk assessment.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Processing operations include but are not limited to: provision of training courses, risk assessment questionnaires and learning management services to employees, contractors and users of the Services to monitor and evaluate risk assessment in the workplace in compliance with rules and regulations applicable to the Controller's business.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list accessed via https://www.essentialskillz.com/docs sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies	Where the EU GDPR applies, the Irish Data Protection Authority – The Data Protection Commission (DPC). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is Us.

The Data Importers: are the Sub-processors named in the Sub-processor list which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

The Sub-processor list includes the information about the processing and transfers of the Personal Data, for each Data Importer:

- categories of Data Subjects
- categories of Personal Data
- the nature of the processing
- the purposes of the processing

Personal Data is processed by each Sub-processor:

- on a continuous basis

- to the extent necessary to provide the Services in accordance with the Agreement and the Data Exporter's instructions.

- for the duration of the Agreement and subject to clause 14 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority of the Data Exporter shall be:

- Where the EU GDPR applies, the Irish Data Protection Authority – The Data Protection Commission (DPC);

- Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO).

- Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

Exhibit B

Technical and Organisational Security Measures(including Technical and Organisational Measure to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by the Processor(s) / Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Full details of the Processor's/Data Importer's technical and organisational security measures used to protect Personal Data is available in our Security Policy. We reserve the right to update or alter our organisational and technical measures. Changes will be reflected in the Security Policy.

Measure	**Description**
Measures of pseudonymisation and encryption of Personal Data	See subheadings 'Encryption', 'Encryption at rest', 'Encryption in transit' and 'Key Management' in the Security Policy.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See subheadings 'C-I-A triad' and 'Access control' in the Security Policy.

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	See subheadings 'Business Continuity', 'Disaster recovery', 'Database backup' and 'Files backup' in the Security Policy.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	We conduct multiple internal audits. We obtain an external security and compliance audit once per calendar year. See subheadings 'Certifications', 'Monitoring and logging' and 'Due Diligence' in the Security Policy.
Measures for user identification and authorisation	See subheadings 'Access control' in the Security Policy.
Measures for the protection of data during transmission	See subheadings 'Encryption' and 'Encryption in transit' in the Security Policy.

Measures for the protection of data during storage	Personal Data is only retained internally, and on the third party data centre servers, which are covered by AWS certifications. See subheadings 'Encryption', 'Encryption at rest', 'Encryption in transit', 'Business Continuity' and 'Disaster Recovery' in the Security Policy.
Measures for ensuring physical security of locations at which Personal Data are processed	See subheading 'Building Security' in the Security Policy.
Measures for ensuring events logging	See subheadings 'Monitoring and logging' in the Security Policy.
Measures for ensuring system configuration, including default configuration	System configuration is applied and maintained by software tools that ensure the system configurations do not deviate from the specifications. Deviations will be fixed automatically and reported to our SOC.

Measures for internal IT and IT security governance and management	**Employee Awareness and Training** See subheadings 'Police and procedures' and 'Awareness Training' in the Security Policy. At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems. The Controller's Personal Data is stored in a way that logically separates it from other customer data. **Access** ● Access is granted on a need-to-know and least privilege basis ● Access controls manage electronic access to data and system functionality based on authority levels and job functions ● All access attempts are logged ● Access to Controller data is restricted to minimal designated employees of the Processor **Information Security Program** ● Management and dedicated staff are responsible for the development, implementation, and maintenance of the Processor's information security program ● Information risk assessments are reviewed by management ● Information Security system is built on the principles of Confidentiality, Integrity and

	Availability **Information Security Policy** ● Information Security policies are approved by management ● Policies and measures are regularly reviewed and updated ● Employees of the Processor are informed of duties and responsibilities in relation to such policies **Access Management** ● Access permissions are reviewed on a regular basis, and in the event of any changes in personnel or access requirements ● Access permission changes are reviewed and approved by senior management **Password Management** ● Policies are in place to manage and control password strength and usage ● All default admin passwords are changed. **Incident Management** ● Incident management procedures are implemented in order to investigate, respond to, mitigate and notify of events related to product technology and information assets **Change Management** ● Change management procedures are designed to test, approve and monitor all changes to product technology and information assets. **Application Development** ● Application code is proactively monitored for vulnerabilities during development ● Application updates/patches are applied by the Processor on a quarterly basis **External Audit/Testing** ● Application penetration test and vulnerability scan is performed by an independent third party on an annual basis **Supplier Management** ● Appropriate due diligence is exercised in the selection and approval of new suppliers ● Supplier information security requirements and controls are formally documented in a contractual agreement

Measures for certification/assurance of processes and products	See subheadings 'Certifications' in the Security Policy.

Measures for ensuring data minimisation	If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.
Measures for ensuring data quality	All of the data that we possess is provided by the Controller. We do not assess the quality of the data provided by the Controller. We provide reporting tools within our product to help the Controller understand and validate the data that is stored.
Measures for ensuring limited data retention	See the subheading 'Disposal' in the Security Policy. ● Devices and paperwork are disposed of in a secure manner ● Devices are securely wiped to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal ● Device disposal is managed centrally to ensure effective and complete erasure ● Hosting infrastructure components are decommissioned using industry-standard practices of sanitisation and disposal
Measures for ensuring accountability	We internally review our information security policies annually to ensure they are still relevant and are being followed. All employees that handle sensitive data must acknowledge the information security policies. These employees are re-trained on information security policies once per year. A disciplinary policy is in place for employees that do not adhere to information security policies. See subheadings 'Policy and procedures' and 'Awareness Training' in the Security Policy.
Measures for allowing data portability and ensuring erasure	The Services have built-in tools that allow the Controller to export and, by request, to permanently erase data. See subheadings 'Backup policy' and 'Disaster recovery' the Security Policy.

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).	The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. Personal Data will not be transferred by the Processor or their sub-processors outside of the UK, EEA or a country deemed adequate by the UK supervisory authority.