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;
"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 GDPR 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, B and C;
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
"Personal Data"	shall have the same meaning as in Data Protection Law;
"Processor"	means Us;
"Security Policy"	means the Processor's security document set out in Exhibit B of this DPA;
"Standard Contractual Clauses"	means the EU model clauses for Personal Data transfer from controllers to processors c2010-593 - Decision 2010/87EU, set out in Exhibit C of this DPA;
"Sub-Processor"	means any person or entity engaged by the Processor or its Affiliate to process Personal Data in the provision of the Services to the Controller.

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.

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 Where Personal Data relating to an EU or UK Data Subject is transferred outside of the EEA it shall be processed in accordance with the provisions of the Standard Contractual Clauses,

unless the processing takes place: (i) in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) by an organisation located in a country which has other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

4.10 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.

5. Controller Obligations

5.1 The Controller represents and warrants that it shall comply with this DPA and its obligations under Data Protection Law.

5.2 The Controller represents and warrants that it 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.

5.3 All Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

5.4 The Controller is responsible for compliance with Data Protection Law, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement.

5.5 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.

5.6 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. 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.

5.7 The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, the Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. The Processor shall be entitled to charge the Controller for its 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 and their country of location. During the term of this DPA, the Processor shall provide the Controller with prior notification, via email, of any changes to the list of Sub-processor(s) 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 Sub-Processor 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 Sub-Processor complies with all such obligations.

6.6 The Controller agrees that the Sub-Processors may transfer Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement to countries outside the European Economic Area (EEA). The Processor confirms that such Sub-Processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

7. Audit

7.1 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.

7.2 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.

7.3 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.

8. Data Breach

8.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("Data Breach").

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

9. Compliance, Cooperation and Response

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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 parties agree that amendments are required, but the Processor is unable to accommodate the 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.

9.6 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA and Data Protection Law.

10. Liability

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

10.2 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.

10.3 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.

10.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

11. Term and Termination

11.1 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.

11.2 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 shall in any event 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.

12. General

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

12.2 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.

12.3 Subject to any provision of the Standard Contractual Clauses 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

Overview of data processing activities to be performed by the Processor

1. **Controller**

The Controller transfers Personal Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The Controller is the customer named in the Order Form, ("**You**").

2. **Processor**

The Processor received data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The Processor is RiskWize Limited T/A EssentialSkillz, ("**Us**").

3. **Data Subjects**

The Personal Data transferred includes but is not limited to the following categories of Data Subjects:

- Employees, freelancers and contractors of the Controller.
- Users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement.
- Clients of the Controller and individuals with whom those end users communicate with by email and/or other messaging media.
- Employees of clients of the Controller.
- Suppliers and service providers of the Controller.
- Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.
-

4. **Categories of Data**

The Personal Data transferred includes but is not limited to the following categories of data:

- 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.

5. **Special categories of Data**

The sensitive data transferred includes, but is not limited to the following categories of data:

- Data concerning health, where this is provided by the end-user in response to a risk assessment.

6. **Processing operations**

The Personal Data transferred will be subject to the following basic processing activities:

- Personal Data will be processed to the extent necessary to provide the Services in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller.
- 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. These operations relate to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Services and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.
- Virus, anti-spam and Malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data processed.
- URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement. This operation relates to attachments and links in emails and will relates to any Personal Data within those attachments or links which could include all categories of Personal Data.

Exhibit B

Technical and Organisational Security Measures

The Processor utilises third party data centres that maintain current ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organisational measures may be found in the Security Policy. It's acknowledged and agreed that the Security Policy and the technical and organisational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in the Security Policy in any material, detrimental way.

1. Technical Measures

Cloud Hosting

- Controller data is stored and processed on infrastructure which complies with the highest industry standards

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

Physical and Environmental security

- Facilities containing confidential information of the Controller are designed to protect information assets from unauthorized physical access
- Facilities containing confidential information of the Controller are designed to guard against environmental hazards such as heat, fire and water damage

Building Security

- Robust measures and protocols are in place to secure access to offices of the Processor
- Controls are in place to ensure that visitors are registered and identifiable
- Employees of the Processor are informed of duties and responsibilities in relation to such controls

Communication

- Communication with the application utilises industry-standard cryptographic protocols to protect information in transit over public networks
- Controller data at rest is protected by industry-standard encryption

Logging

- Security and event logs for product are maintained and monitored

Data Segregation

- Customer databases are segregated to ensure integrity

Product Access

- Product enables password complexity requirements (length, case, characters etc) to be configured by the Controller
- Passwords are stored in hashed form
- Single Sign On can be configured to authenticate users of the Controller

Backup

- Architecture is built to provide a highly available and durable service
- Redundancy is built-in at both the application and database tiers
- Copies of customer databases are stored across multiple availability zones and will automatically be recovered with minimal data loss

Firewalls

- Operate a deny-all policy
- Ports are only opened for specific purposes and for authorised users
- Multi-tier protection is utilised to filter attacks

Antivirus

- Office hardware and application servers are protected by appropriate antivirus software

Disposal

- 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

2. Organisational Measures

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

Employee Awareness and Training

- Employees of the Processor complete regular information security training across a number of areas including Data Protection, Cyber Security and Phishing Awareness
- Acceptable Use and Clean Desk/Screen policies are implemented and enforced

Business Continuity

- Operate Business resiliency, continuity and disaster recovery procedures which are designed to maintain service and/or recovery from foreseeable emergency situations or disasters
- Business Continuity and Disaster Recovery plans have been approved by management and are communicated to relevant employees of the Processor

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

Exhibit C

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

the Controller, (the data "exporter")

and

the Processor, (the data "importer")

each a "party"; together "the parties",

HAVE AGREED on the following Standard Contractual Clauses (the "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Exhibit A of the DPA.

Clause 1

Definitions

For the purposes of the Standard Contractual Clauses all terms used in capitals shall have the meaning given to them in the DPA unless defined otherwise below:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Standard Contractual Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Standard Contractual Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Exhibit A of the DPA which forms an integral part of the Standard Contractual Clauses.

1

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Standard Contractual Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Standard Contractual Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in the Security Policy;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Standard Contractual Clauses, with the exception of the Security Policy, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Standard Contractual Clauses, unless the Standard Contractual Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Standard Contractual Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Standard Contractual Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Standard Contractual Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in the Security Policy before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

2

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Standard Contractual Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Standard Contractual Clauses, or any existing contract for subprocessing, unless the Standard Contractual Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of the Security Policy which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Standard Contractual Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Standard Contractual Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by

operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Standard Contractual Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Standard Contractual Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Standard Contractual Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Standard Contractual Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Standard Contractual Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Standard Contractual Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Standard Contractual Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Standard Contractual Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Standard Contractual Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Standard Contractual Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Miscellaneous

1. These Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Standard Contractual Clauses are entered into.

2. Unless the Standard Contractual Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Standard Contractual Clauses are entered into, will amend the terms or the effects of the Standard Contractual Clauses, or limit any liability under the Standard Contractual Clauses, and no term of any such other agreement should be read or interpreted as having that effect.