risr/

data processing addendum

date issued: [25th April 2023]

info@risr.global visit risr.global

data processing agreement

(REVISED 25th April 2023)

This Data Processing Addendum, including its Schedules and Appendices ("DPA") forms part of the Master Services Agreement or other written or electronic agreement between risr/ and Customer for the purchase of risr/ Services (the "Services") (the "Agreement") to reflect the parties' agreement regarding the Processing of Personal Data.

By signing the Agreement, the Customer enters into this DPA on behalf of itself and to the extent required under applicable Data Protection Laws in the name and on behalf of its Affiliates (if any), if and to the extent risr/ processes Personal Data for which such Affiliates qualify as the Controller for the purposes of this DPA only, and except where indicated otherwise, the term "Controller" shall include the Customer and Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA will follow the term of the Agreement. We may update these terms from time to time and we will provide you with thirty (30) days' notice of any update via email. Upon receiving such notice, you will have seven (7) days to respond with whether you agree to the update. If you do not agree with the update, we will negotiate in good faith and acting reasonably to come to agreement on the terms. If no agreement is reached by thirty (30) days after notifying us that you disagree with the terms, you may terminate this DPA in accordance with clause 8(IV) of the Agreement

In the course of providing the Services to Customer pursuant to the Agreement, risr/ may Process Personal Data on behalf of Controller and the parties agree to comply with the following provisions with respect to any Personal Data each acting reasonably and in good faith. For the purposes of this DPA, risr/ is the Processor and Customer is the Controller.

HOW TO EXECUTE THIS DPA:

This DPA consists of:

The main body of the DPA, Annex 1, 2, 3 & 4 and Appendices 1, 2 & 3.

This DPA and the Standard Contractual Clauses has been pre-signed on behalf of risr/, acting as the Processor. To complete this DPA, Customer must complete the information in the signature boxes and return the completed DPA to risr/ by email to: dpa@risr.global. Upon receipt of the validly completed DPA by risr/ at the aforementioned email address,this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the risr/ entity that is a party to the Agreement is party to this DPA.

1. DEFINITIONS

"Controller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
"Customer"	means the entity that executed the Agreement.
"Customer Data""risr/"	Means what is defined in the Agreement as "Customer Data".
"Processor"	means the FRY entity trading as risr/ which is a party to this DPA, as specified in the section"How this DPA applies" above, being either FRY-IT Ltd, FRY-IT Canada Ltd, FRY-IT Assessment Solutions Ireland Ltd, or FRY-IT PTY Ltd as further specified in section 12 of the Agreement.
"Data Protection Laws"	local, national or international laws and regulations which relate to the protection or Processing of Personal Data, including but not limited to: (a) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); European Union ("**EU**") member state data protection laws; and the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (the "**EU Data Protection Laws**"); (b) the UK Data Protection Act 2018 (and regulations made thereunder) and UK GDPR (the "**UK Data Protection Laws**"); and (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003; the Canada Personal Information Protection and Electronic Documents Act (PIPEDA); the Swiss Federal Act on Data Protection; the Australian Privacy Act 1988; and any other relevant, EU, local, state, provincial, or national data protection laws, in each case as amended, supplemented or replaced from time to time, and in each case to the extent that they apply to the Processing of Personal Data by a Party.
" Data Subject"	means the identified or identifiable natural person whom the Personal Data relates to.
"GDPR"	Means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 94/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.
"Instructions"	means the written, documented instructions issued by Controller to Processor, and directing the Processor to perform a specific or general action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available)

" Personal Data"	means any information, which directly or indirectly relates to a Data Subject and which Processor Processes on behalf of the Controller under this DPA.
" Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Services. For the avoidance of doubt, a Personal Data Breach will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls all networked systems.
" Processing"	means any operation or set of operations, which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means (processing other than by automated means only includes any operation or set of operations which is performed on Personal Data which form part of a filing system or are intended to form part of a filing system).
" Standard Contractual Clauses"	means the standard contractual clauses for Processors approved by the ICO, in the form set out at Annex 3, as may be amended, superseded, or replaced.
" Sub-Processor"	means any third party, which Processor engages to Process Personal Data on behalf of the Controller (including, but not limited to, Processor's subcontractors).
" Supervisory Authority"	means an independent public authority which is established by an EU member state pursuant to the GDPR or, for the United Kingdom, the Information Commissioner's Office ("ICO").

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that with respect to the Processing of Personal Data, Customer is the Controller, risr/ is the Processor, and that risr/ will engage Sub-Processors pursuant to the requirements set forth in section 7 "Sub-Processors" below.

2.2 **Details of the Processing.** The subject-matter of Processing of Personal Data by risr/ is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and the purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 (Details of Processing) to this DPA.

3. CUSTOMER RESPONSIBILITIES

3.1 **Compliance with Laws.** Within the scope of the Agreement and in its use of the Services, Customer will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to risr/. In particular but without prejudice to the generality of the foregoing Customer acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality and legality of Customer Data and the means by which Customer acquired such Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of Personal Data, including obtaining any necessary consents and authorisations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to transfer or provide access to the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws and complying with all laws (including Data Protection Laws) applicable to any emails or other content created sent or managed

through the Services including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You agree to inform us without undue delay if you are not able to comply with the responsibilities under this section 3.1 or applicable Data Protection Laws.

3.2 **Controller Instructions.** The parties agree that the Agreement (including this DPA) together with your use of the Services in accordance with the Agreement constitute your complete and final Instructions to us in relation to the Processing of Personal Data and additional instructions outside the scope of the Instruction shall require prior written agreement between us and you.

4. risr/ OBLIGATIONS

4.1 **Compliance with Instructions**. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

4.2 **Conflict of Laws.** If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will: (i) promptly notify you of that legal requirement to the extent permitted by applicable law; and (ii) where necessary cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Services until such time as you issue new lawful Instructions regarding the Processing.

4.3 **Confidentiality.** We will ensure that any personnel whom we authorise to Process Personal Data on our behalf are subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to such Personal Data.

4.4 **Personal Data Breaches.** We will notify you without undue delay if we become aware of any Personal Data Breach and we will provide timely information relating to such Personal Data Breach as it becomes known to us or reasonably requested by yourselves. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

4.5 **Deletion or Return of Personal Data.** We will delete or return all Customer Data including Personal Data (including copies thereof) processed pursuant to this DPA, on termination or expiration of Agreement in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent we are required by applicable law to retain some or all of the Customer Data or to Customer Data it has archived on backup systems which data we will securely isolate and protect from any further Processing and delete in accordance with our retention and deletion practices. You may retrieve your Customer Data in accordance with terms set out in the Agreement.

5. DATA SUBJECT REQUESTS

5.1 The Services provide you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use to assist in connection with your obligations under Data Protection Laws,including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

5.2 Processor shall forward any request to the Controller from a Data Subject, the Supervisory Authority or any other third party, who is requesting receipt of information regarding Personal Data, that Processor Processes under this DPA. Processor, or anyone working under Processor's supervision, shall not disclose Personal Data, or information about the Processing of Personal Data, without the Controller's express instruction or as provided in this DPA, unless required by the Data Protection Laws.

5.3 Unless prohibited by law, Processor shall inform the Controller of any inquiries from the Supervisory Authority concerning the Processing of Personal Data under this DPA. Processor is not entitled to represent the Controller or act on their behalf in relation to the Supervisory Authority.

6. SECURITY

6.1 Processor shall implement and maintain appropriate technical and organisational measures in order to protect Personal Data from Personal Data Breaches and to ensure a level of security appropriate to the risk with regard to the state of 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, as further described under Annex 2 to this DPA.

6.2 Processor shall assist and without delay (not to exceed 36 hours) notify the Controller about any unintentional or unauthorized access to Personal Data as well as any other Personal Data Breach

6.3 Upon the Customer's request, risr/ shall provide Customer with reasonable cooperation and assistance needed to fulfil the Customer's obligations under the Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to risr/.

6.4 Processor shall document the technical and organizational security measures Processor is using in order to fulfil the security requirements according to the Data Protection Laws and this DPA. Upon the Controller's written request, the documentation shall be made available without undue delay.

7. SUB-PROCESSORS

7.1 The Customer hereby agrees that as the Processor, we may engage Sub-Processors to Process Personal Data on the Customer's behalf. We have currently appointed, as Sub-Processors, the third parties listed in Annex 4 to this DPA.

7.2 Where we engage Sub-Processors, we will put in place each time a written contract between Processor and Sub-Processor and impose data protection terms on each Sub-Processor that provides at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the
Standard Contractual Clauses), to the extent applicable to the nature of the services provided by eachSub-Processor.

7.3 Upon Customer's request, risr/ shall provide such specified information regarding Processing by Sub-Processors, which the Customer reasonably may request according to Data Protection Laws.

7.4 If risr/'s Sub-Processor fails to fulfil its data protection obligations, risr/ shall remain responsible towardsthe Customer for the performance or non-performance of risr/'s Sub-Processor's data protection obligations and shall be responsible for any acts or omissions of such Sub-Processor that cause risr/ to breach any of its obligations under this DPA.

7.5 risr/ agrees to notify the Customer of any changes to its Sub-Processors listed in Annex 4 to this DPA and give the Customer the opportunity to object to the engagement of any new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days after updating Annex 4 to this DPA. Ifthe Customer does not notify risr/ of any such objection, the parties agree to discuss, in good faith, the Customers concerns, with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, risr/ will, at its sole discretion either not appoint the new Sub-Processor or permit the Customer to suspend or terminate the affected Services in accordance with the termination provisions of the Agreement, without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

8. DATA TRANSFERS

8.1 The Controller hereby acknowledges and agrees that the Processor may access and process Personal Data ona global basis, as necessary to provide the Services in accordance with the Agreement and in particular that Personal Data will be transferred to and processed by Processor in jurisdictions outside of the United Kingdom where risr/ and its Sub-Processors have operations. The Processor will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

9. ADDITIONAL PROVISIONS FOR EUROPEAN DATA

9.1 **Scope of Section 9**. This section shall apply only with respect to European Data.

9.2 Transfer Mechanisms for Data Transfers.

a) The Processor shall not transfer any European Data to any country or recipient not recognised as providing an adequate level of protection for Personal Data (within the meaning of the applicableEuropean Data Protection Laws), unless it first takes all such measures as are necessary to ensurethe transfer is in compliance with applicable European Data Protection Laws. Such measures mayinclude, but not limited to, transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognised by the relevant authorities or courts as providing an adequate level of protection for Personal Data to a recipient that has achieved binding corporate rules authorisation in accordance with European Data Protection Lawsor to a recipient that has executed appropriate standard contractual clauses in each case is adopted or approved in accordance with applicable European Data Protection Laws.

b) The Controller acknowledges that in connection with the performance of the Services the Processor may be a recipient of European Data in the United States. The parties hereby acknowledge and agree the following:

i) **Standard Contractual Clauses**. The Processor agrees to abide by and process European Data in compliance with the Standard Contractual Clauses.

c) The parties agrees that:

i) solely for the purposes of the descriptions in the Standard Contractual Clauses, risr/, will be deemed the '**data importer**" and Customer will be deemed the 'data exporter" (notwithstanding that you may yourself be located outside Europe and/or being acting as a processor on behalf of third party controllers); and

ii) If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

9.3 **Demonstration of Compliance**. risr/ agrees to make all information reasonably necessary to demonstrate compliance with this DPA available to the Customer and allow for and contribute to audits including inspections by the Customer in order to assess compliance with this DPA. The Customer acknowledges and agrees that it will exercise its audit rights under this DPA by instructing risr/ to comply with the audit measures described in this subsection 9.3. The Customer acknowledges that the Services are hosted by our data centrepartners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon request, risr/ will supply (on a confidential basis) a summary copy of its penetration testing report(s) to the Customer so that Customer can verify compliance with this DPA. Furthermore, risr/ agrees, upon written request from Customer, to provide written responses (on a confidential basis) to all reasonable requests for information to demonstrate risr/'s compliance with this DPA, provided that Customer does not exercise this right more than once per calendar year.

10. GENERAL

10.1 **Liability.** Notwithstanding anything to the contrary stipulated in the Agreement, in the event that Processor, anyone working under Processor´s supervision or Processor's Sub-Processors, Process Personal

Data in breach of this DPA, the Data Protection Laws or contrary to lawful instructions given bythe Controller, Processor shall, subject to the limitations set forth at section 11, Liability, of the Agreement, indemnify and hold the Controller harmless from and against any damage under any legal theory, including any administrative fines and compensations that the Controller has paid to Data Subjects.

10.2 **Term and Termination.** Upon termination or expiration of the Agreement, Processor shall, upon instructions given by the Controller, delete or return the Personal Data that the Controller has transferred to Processor Services and delete any existing copies, unless storage of the Personal Data is required by EU law or applicable EU member state law, and send a confirmation to the Controller of the deletion. Processor shall ensure that each of Processor's Sub-Processors does the same.

10.3 **Changes and Additions**. If the data protection laws are changed during the term of this DPA or if the supervisory authority issues guidelines decisions or regulations concerning the application of the data protection laws that result in the DPA no longer meeting the requirements for a data processing agreement the parties should make the necessary changes in writing to this DPA to meet such new or additional requirements. The party that first becomes aware of the required changes will notify the other party of this fact as soon as reasonably practicable and the parties will have 30 days from the date of notification to reach agreement on the changes to the DPA, or otherwise no later than prescribed by the data protection laws including guidelines decisions or regulations of the supervisory authority. The changes and additions to this DPA must be made in writing and duly signed by both parties in order to be binding.

10.4 This DPA supersedes and replaces all prior data processing agreements between the parties and supersedes any deviating provisions of the Agreement concerning the subject matter of this DPA, notwithstanding anything to the contrary in the Agreement.

10.5 **Governing Law.** Each party agrees to the applicable governing law as set out in section 12 of the Agreement without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts.

The parties' authorised signatories have duly executed this Data Processing Addendum:

Customer:

Signature:
Name:
Title:
Date:

FRY-IT LTD (trading as risr/):

Signature:
Name:
Title:
Date:

FRY-IT Canada Ltd (trading as risr/)

Signature:
Name:
Title:
Date

FRY-IT PTY LTD (trading as risr/):

Signature:
Name:
Title:
Date:

FRY-IT Assessment Solutions Ireland Ltd (trading as risr/)

Signature:
Name:
Title:
Date:

ANNEX 1: DETAILS OF PROCESSING

In this Appendix 1, all capitalised words shall have the same meaning as defined in the DPA, unless otherwise expressly stated.

Nature and Purpose of Processing	risr/ will Process Personal Data as necessary to perform the risr/ Services pursuant to the Agreement, as further specified in the Documentation and as further instructed by Customer in its use of the risr/ Services
Duration of Processing	risr/ will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing between the parties.
Categories of Data Subjects	Customer may submit Personal Data to the risr/ Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: - Prospects, customers, business partners andvendors of Customer - Employees or contact persons of Customer'sprospects, customer, business partners and vendors. - Employees, agents, advisors, contractors ofCustomer - Users authorised by Customer to use the risr/Services
Types of Personal Data	Customer may submit Personal Data to the risr/ Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Personal Data: - Name - telephone number - email - title - location details, user, and account information - personal life data
Special Categories of data (if appropriate)	The parties do not anticipate the transfer of special categories of data
Processing Operation	e.g., viewing
Location of processing operations	Please refer to location specified in the applicable Order Form

ANNEX 2 – SECURITY

This Annex forms part of the DPA

We currently observe the Security Measures described in this Annex 2. All capitalised terms not otherwise definedherein shall have the meanings as set forth in the DPA.

A) **Access Control**

i) Preventing Unauthorised Services Access.

Outsourced processing: We hosts our services with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the services in accordance with our DPA. We rely on contractual agreements, privacy policies and vendor compliance programmes in order to protect data processed orstored by these vendors.

Physical and environmental security: We host our services infrastructure with multi-tenant, outsourced infrastructureproviders. The physical and environmental security controls are audited for SOC Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer services. Customers who interact with theservices via the user interface must authenticate before accessing non-public customer data.

Authorisation: Customer Data is stored in multi-tenant storage systems accessible to customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of our services is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and authorisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application programming interface API access: Public service API's may be accessed using an API key or through authorisation.

ii) Preventing Unauthorised Service Use

We implement industry standard access controls and detection capabilities for the internal networks that support its services.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the service infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacksagainst publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for codingbest practises and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognised penetration testing service providers for fourannual penetration tests. The intent of the penetrating penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Bug bounty: A bug bounty programme invites and incentivises independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty programme in an effort to widen the available opportunitiesto engage with the security community and improve the service defences against

sophisticated attacks.

iii) Limitations of Privilege & Authorisation Requirements

Service access: A subset of our employees have access to the services and to customer data for our controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All risr/ employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by applicable law(s). All risr/ employees are required toconduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

B) Transmission Control

In transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces andfor free on every customer site hosted on the risr/ services. Our HTTPS implementation uses industry standard algorithms and certificates.

At rest: We store user passwords following policies that follow industry standard practises for security. We haveimplemented technologies to ensure that stored data is encrypted at rest.

C) Input Control

Detection: We designed our infrastructure to log extensive information about the system behaviour, traffic received,system authentication and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Responsive and tracking: We maintain a record of known security incidents that includes description, dates and timesof relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize service and customer damage or unauthorised disclosure. Notification to you will be in accordance with the terms of the Agreement.

D) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and failover protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standardmethods.

Our services are designed to ensure redundancy and seamless failover. The server instances that support the services are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining andupdating the service applications and backend while limiting downtime.

ANNEX 3 – STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/4/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer, as defined in the risr/ Master Services Agreement (the "data exporter")

And

risr/, as defined in Section 12 of the risr/ Master Services Agreement (the "data importer") each a "party, together the "parties",

HAVE AGREED on the following Standard Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection and fundamental rights and freedoms of individuals for the transfer by the data exporterto the data importer of the personal data specified in Annex 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'Personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;
(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 the processing on his behalf after the transfer in accordance with his instructions and the termsof the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issues under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act2018;
(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of thedata importer who agrees to receive from the data importer or from any other sub-processor 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 Clauses and the terms of thewritten subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms ofindividuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;
(f) 'technical and organisational security measures' means those measures aimed at protecting personal dataagainst accidental loss, alternation, 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 inAnnex 1 which forms an integral part of the Clauses.

Clause 3

Third-Party beneficiary clauses

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, Clause7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceasedto 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 sub-processor this Clause, Clause 5(a) to (e) & (g), Clause 6, Clause7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or cease 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 sub-processor shall be limited to its own processingoperations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the datasubject 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 carriedout in accordance with the relevant provisions over the applicable data protection law (and, where applicablehas been notified to the Commissioner) and does not violate the applicable data law;

(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 accordancewith the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisationalsecurity measures specified in Appendix 2 to this contract;

(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 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 thirdcountry not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) andClause 8(3) to the Commissioner 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 Clauses, with the exception of Appendix 2,and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer

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 Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the dataexporter 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 Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case thedata 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 Appendix 2 beforeprocessing 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 enforcementauthority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of 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;

(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 Commissioner with regard to theprocessing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activitiescovered by the 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 Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub- processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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 sub-processing, it has previously informed the data exporter and obtained its priorwritten consent;

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

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the dataexporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligationsreferred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation fromthe 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 sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually

disappeared or ceased to existin 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 or 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 sub-processor 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 sub-processor 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 orcease to exist in law or have become insolvent, that sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the 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 sub-processor shall be limited to its ownprocessing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the datasubject:
    a. to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;
    b. to refer the dispute to the UK courts.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or proceduralrights 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 Commissioner if it so requests or if suchdeposit is required under the applicable data protection law.
2. The parties agree that the Commissioner has the right to conduct an audit of the data importer and of any sub-processor, which has the same scope and is subject to the same conditions at would apply to an audit ofthe 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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 Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England and Wales.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business relatedissues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub- processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 orby operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified bythe data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after termination

1. The parties agree that on the termination of the provision of data-processing services, the data importer andthe sub-processor 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 thatit has done so, unless legislation imposed upon the data importer prevents it from returning or destroying allor 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 sub-processor warrant that upon request of the data exporter and/or of theCommissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

Date of the Standard Contractual Clauses:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.Data Exporter
The data exporter is the legal entity specified as "Customer" in the DPA.

Data Importer

Data importer: risr/

Categories of data: Please see Annex 1 of the DPA, which describes the categories of data.

Special categories of data (if appropriate): The parties do not anticipate the transfer of special categories of data.

Purposes of Processing: risr/ shall process personal data as necessary to provide the Services to data exporter in accordance with the Agreement.

Processing Operations: Please see Annex 1 of the DPA, which describes the processing operations.

DATA EXPORTER

Name:

Authorised Signature:

DATA IMPORTER

Name:

Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses') and must be completed and signed byboth parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5© (or document/legislation attached):

Please see Annex 2 of the DPA, which describes the technical and organisational security measures implemented by risr/.

DATA EXPORTER

Name:

Authorised Signature:

DATA IMPORTER

Name:

Authorised Signature:

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the "Clauses").

This Appendix sets out the parties' interpretation of their respective obligations under specific terms of the Clauses. Where a party complies with the interpretations set out in this Appendix, the party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Agreement in place between Customer and risr/and to which these Clauses are incorporated, and "Agreement" shall have the meaning given to it in the DPA.

Clause 4(h) and 8: Disclosure of these Clauses

a. Data exporter agrees that these Clauses constitute data importer's Confidential Information as defined in theAgreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a) and 5(b): Suspension of data transfers and termination

a. The parties acknowledge that data importer may process the personal data only on behalf of the dataexporter and in compliance with its instructions and provided by the data exporter and the Clauses.
b. The parties acknowledge that if data importer cannot provide such compliance in accordance with Clause 5(a) and Clause 5(b) for whatever reason, the data importer 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, or the affected parts of the Services in accordance with the terms of the Agreement.
c. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts ofthe Services, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
d. If required the parties shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards and other measures, if any, may be reasonably required to ensure the data importer'scompliance with the Clauses and applicable data protection law.
e. If after the Cure Period, the data importer has not or cannot cure the non-compliance than the data exportermay suspend and/or terminate the affected part of the Services in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination). The data exporter shall not be required to provide such notice in an instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5 (f): Audit

a. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing dataimporter to comply with the audit measures described in the Section 9.3 of the DPA.

Clause 5(j): Disclosure of sub-processor agreements

a. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.
b. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose thesub-processor agreement to data exporter.
c. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide

all information itreasonably requires in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

a. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability withrespect to any data subject rights under these Clauses.

Clause 11: Onward sub-processing

a. The parties acknowledge that the data exporter provides a general consent to data importer pursuant to Clause 11 of these Clauses to engage onward sub-processors. Such consent is conditional on data importer'scompliance with the requirements set out in Section 7.5 of the DPA.

Clause 12: Obligation after termination of the Services

a. Data importer agrees that the data exporter will fulfil its obligation to return or destroy all the personal data upon the termination of the provision of the Services by complying with the requirements set out in Section
10.2 of the DPA.

DATA EXPORTER

Name:

Authorised Signature:

DATA IMPORTER

Name:

Authorised Signature:

ANNEX 4 LIST OF SUB-PROCESSORS

SUB-PROCESSOR	PURPOSE	LOCATION
Amazon Web Services, Inc	Standard Hosting, Video & Infrastructure	Canada, EU (Ireland & Germany), UK & Australia
FRY-IT Ltd (trading as risr/)	Standard Services & Support	UK
FRY-IT Assessment Solutions Ireland Ltd (trading as risr/)	Standard Services & Support	EU
FRY-IT Canada Ltd (trading as risr/)	Standard Services & Support	Canada
FRY-IT PTY LTD (trading as risr/)	Standard Services & Support	Australia
Examity	Optional Proctoring Services	Canada, EU (Germany), India, USA
ProctorExam	Optional Proctoring Services	Canada, EU (Germany,Netherlands, Belgium, Ireland), India, USA
TurnitIn	Optional Plagiarism Software services	Dependent upon customer direct agreement with TurnitIn