FaceUp

Data Processing Addendum

Data Processing Addendum

Last change: 14/02/2025

1. Initial Provisions

1.1. Agreement. This Data Processing Addendum (the "**DPA**") forms an integral part of the Terms of Service available at faceup.com/en/terms-of-service or Master Services Agreement executed separately by the Parties (hereinafter "**Agreement**") and is referenced in the Agreement.

1.2. Data Processing Agreement. By entering into the Agreement with the Provider You, the Customer, acknowledge that you have read and understood this DPA and agree to be bound by it.

2. Definitions

Other than the terms defined in the body of this DPA or in the Agreement, these terms have the following meaning:

"**CCPA**" means the California Consumer Privacy A
including as modified by the California Privacy Rig
amendments and implementing regulations that b
of this DPA. Terms "**business**", "**service provider**" a
it under the CCPA.

"**Data Breach**" means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by The Provider under this DPA.

"**Data Protection Legislation**" means, as applicable to a party and its Processing of Personal Data: (i) EU Data Protection Law (ii) UK Data Protection Law, (iii) CCPA and any national data protection laws made under the CCPA, (iv) any other law applicable for the provision of the Services.

"**EU Data Protection Laws**" mean Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**GDPR**") and the EU e-Privacy Directive (Directive 2002/58/EC). Terms "**Controller**", "**Processor**", "**Process**", "**Processing**", and "**Data Subject**" shall have the same meanings given to them under the GDPR.

"**Personal Data**" means any information that (i) is protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Legislation; and (ii) is Processed by the Provider on behalf of Customer in the course of providing the Services, as more particularly described in Annex A of this DPA.

"**Restricted Transfer**" means a transfer of Personal Data from the European union/EEA to any other country which is not subject based on adequacy regulations pursuant to Article 45 of Regulation (EU) 2016/679.

"**Sub-processor**" means any third party engaged by the Provider to assist in fulfilling its obligations with respect to providing the Services and that Processes Personal Data as Processor.

"**Standard Contractual Clauses**" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 (the "**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**").

"**UK Data Protection Law**" means: (i) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) or (ii); in each case, as may be amended or superseded from time to time.

3. Provider's Obligations

3.1. Roles. For the purposes of the GDPR and similar Data Protection Legislation, Customer (or third party on whose behalf Customer is authorized to instruct the Provider) is the Controller of Customer Data that are Personal Data, and the Provider shall Process Personal Data as a Processor (or sub-Processor, as applicable to Customer's use of the Services); and for the purposes of the CCPA (to the extent the CCPA is applicable), Customer is the business and the Provider is the service provider.

3.2. Permitted Purposes. The Provider shall Process Personal Data for the purposes described in Annex A and in accordance with Customer's documented lawful instructions ("**Permitted Purposes**"), except where otherwise required by laws that are compatible with applicable Data Protection Legislation. In particular and to the extent the CCPA is applicable, Customer's transfer of Personal Data to the Provider is not a sale, and the Provider provides no monetary or other valuable consideration to Customer in exchange for Personal Data. To the extent required by Data Protection Legislation, this Section 3.2 constitutes the certification from the Provider to the Processing instructions herein. The Provider is obliged at all times to Process Personal Data in compliance with Data Protection Legislation and fulfil all its obligations arising out of Data Protection Legislation.

3.3. Processing Instructions. The Provider shall immediately inform Customer if it becomes aware that Customer's Processing instructions infringe Data Protection Legislation. If the Provider is unable to Process Personal Data in accordance with the Customer's documented lawful instructions, the Provider is obliged to promptly notify Customer of its inability to comply.

3.4. Security Measures. The Provider shall implement and maintain reasonable and appropriate technical and organizational measures designed to protect all data, including Personal Data, from Data Breaches and preserve their security, integrity, and confidentiality. Such measures shall have regard to 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. At a minimum, these measures must include the measures identified in Annex C of this DPA.

3.5. Access and Confidentiality. The Provider shall ensure that any person it authorizes to Process the Personal Data (including Provider's staff, agents and Sub-processors) ("**Personnel**") are under appropriate obligations of confidentiality (whether a contractual or statutory duty), have received proper training, and are informed about the confidential nature

of the Personal Data and their obligations related to it and have access to Personal Data only on need-to-know basis. The Provider shall ensure that Personnel Processes the Personal Data only as necessary for the Permitted Purposes.

3.6. Data Returns and Deletion. Upon termination or expiration of the Agreement, the Provider must delete or return to the Customer all Personal Data in its possession or control except for one copy for archival and compliance purposes.

4. Audit Right

4.1. Right to conduct audits. The Customer shall have the right to conduct an audit to verify Provider's compliance with its obligations laid down in Art. 28 GDPR (if applicable) and in this DPA. The Provider shall allow the Customer to carry out the audit if (i) the Customer requests to carry out the audit via a written notice at least 30 (thirty) days in advance; (ii) the Customer will specify the agenda for such audit in such notice; (iii) the audit shall not take place more than once a year; (iv) all associated costs and expenses shall be borne by the Customer or reimbursed to the Provider on demand; and (v) the audit shall last no longer than the equivalent of 1 working day (8 hours) of Provider's representative. On the request of the Customer, the Provider will provide the Customer with the estimated cost that it expects to incur during such audit according to the extent specified in the agenda provided by the Customer.

4.2. Independent Auditor. In case the Customer requests the audit by an independent party – external licensed auditor, the Provider may object to an external licensed auditor appointed by the Customer to conduct the audit if the auditor is, in Provider's reasonable opinion, not suitably qualified or independent, a competitor of the Provider, or otherwise manifestly unsuitable. Any such objection will require the Customer to appoint another auditor.

5. Customer's Obligations

5.1. Customer's Processing of Personal Data. The Customer shall, in its use of the Services, Process Personal Data in accordance with Data Protection Legislation. The Customer shall have the sole responsibility for the accuracy, quality, and legality of Personal Data and how the Customer acquired Personal Data.

5.2. Customer's Compliance. The Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Legislation in respect of its Processing of Personal Data and any Processing instructions it issues to the Provider; (ii) it has provided notice and obtained (or shall obtain) all consents or any other necessary authorizations (as applicable) under Data Protection Legislation for the Provider to Process Personal Data for the Permitted Purposes; (iii) it shall be responsible for providing any notices required by Data Protection Legislation to its Permitted users and other relevant data subjects with respect to sharing their Personal Data with the Provider; (iv) it has fulfilled (or shall fulfil) all registration or notification obligations to which the Customer is subject to under the Data Protection Legislation; and (v) it is responsible for its own Processing of Personal Data, including integrity, security, maintenance, and appropriate protection of Personal Data under Customer's control.

5.3. Technical and Organizational Measures. The Customer is responsible for its secure use of the Services, including securing the user IDs and passwords, protecting the security of Personal Data when in transit to and from the Services, and taking any appropriate technical, organizational, and security measures to securely encrypt or backup any Personal Data uploaded to the Services. The Customer is also responsible for the use of the Services by any person the Customer authorized to access or use the Services, and any person who gains access to its Personal Data or the Services as a result of its failure to use reasonable security precautions, even if the Customer did not authorize such use. The Customer agrees to, immediately upon awareness, notify the Provider of any unauthorized use of the Services or of any other breach of security involving the Services.

6. Cooperation

6.1. Data Subject Rights. To the extent that the Customer is unable to access the relevant Personal Data within the Services independently, the Provider shall, taking into account the nature of the Processing, provide assistance (including by appropriate technical and organizational measures) to provide reasonable cooperation to the Customer in order to (i) respond to any requests from a data subject seeking to exercise any of its rights under Data Protection Legislation (including its right of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the Processing of the Personal Data (collectively "**Correspondence**").

In the event that any such Correspondence is made directly to the Provider, it shall promptly notify the Customer and shall not respond directly unless legally compelled to do so. If the Provider is required to respond to such Correspondence, the Provider shall promptly notify the Customer and provide it with a copy of the request, unless legally prohibited from doing so.

6.2. Data Protection Impact Assessment. To the extent required by Data Protection Legislation, the Provider shall provide reasonable cooperation regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Legislation.

6.3. Request for Disclosure. The Provider is obliged to promptly notify the Customer about any legally binding request for disclosure of the personal data by a judicial or regulatory authority unless otherwise prohibited, such as the obligation under criminal law to preserve the confidentiality of a judicial enquiry and to assist the Customer accordingly (at Customer's expense).

7. Security Incidents

7.1. Data Breach. Upon becoming aware of a Data Breach, the Provider shall notify the Customer without undue delay and shall provide such timely information and cooperation as the Customer may reasonably require in order to fulfil its data breach reporting obligations under Data Protection Legislation, including the type of data affected and the identity of the affected person(s) as soon as such information becomes known or available to the Provider.

7.2. No acknowledgement. The Customer agrees that any notification that the Provider provides to the Customer in relation to a Data Breach shall not be construed or understood as an acknowledgement of any fault or liability.

7.3. Further Conduct. The Provider shall further take all such measures and actions as are reasonable to remedy or mitigate the effects of the Data Breach and shall keep Customer informed of all developments in connection with the Data Breach.

7.4. Cooperation. If a Data Breach is caused or materially contributed to by the Customer, the Provider will cooperate in the investigation of the Data Breach subject to Customer's obligation to compensate the Provider for its expenses and costs.

8. Sub-processing

8.1. Authorized Sub-processors. The Customer provides a general authorization for the Provider to engage Sub-processors to Process Personal Data on Customer's behalf. The Sub-processors currently engaged by the Provider are listed in Annex B or at faceup.com/en/data-processing-addendum.

8.2. New Sub-processors. The Provider shall provide at least ten (10) days prior written notice to the Customer of the engagement of any new Sub-processor (including details of the Processing and location), whereas the Provider provides such notifications of new sub-processors via offering a subscription on the Provider's website https://www.faceup.com/en.

8.3. Objections. If the Customer has a reasonable objection to any new sub-processor, it shall notify the Provider of such objections in writing to support@faceup.com within ten (10) days from receiving the notification and the Parties will seek to resolve the matter in good faith. If Customer does not provide a timely objection to any new sub-processor in accordance with this Section 8.3, Customer will be deemed to have consented to the sub-processor and waived its right to object.

8.4. Liability for sub-processors. The Provider remains liable for any breach of this DPA caused by an act, error, or omission of such Sub-processor.

9. Data Transfers

9.1. International Data Transfers. The Provider shall take all such measures necessary to ensure that the Processing and transfer of Personal Data in or to a territory other than the territory in which the Personal Data was first collected complies with Data Protection Legislation.

9.2. Application of Standard Contractual Clauses. The Parties agree that when and to the extent the transfer of Personal Data from the Customer to the Provider is a Restricted Transfer and EU Data Protection Laws or UK Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the EU SCCs, which shall be incorporated by reference into and form an integral part of this DPA.

9.3. EU Data. For the purposes of Personal Data that is subject to the EU Data Protection Laws ("**EU Data**"):

a) Where the Customer is a Controller of Personal Data, Module Two (Controller to Processor Clauses) will apply and where the Customer is a Processor acting on behalf of third-party Controllers, Module 3 (Processor to Processor Clauses) will apply;

b) in Clause 7 (Docking Clause), the optional docking clause will apply;

c) in Clause 9 (Use of Sub-processors), Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Section 8.2 of this DPA and the period for notification of objections in Section 8.3 of this DPA;

d) in Clause 11 (Redress), the optional language to permit data subjects to lodge complaints with an independent dispute resolution body will not apply;

e) in Clause 17 (Governing Law), Option 1 will apply, and the EU SCCs will be governed by Irish law;

f) in Clause 18(b) (Choice of forum and jurisdiction), disputes shall be resolved before the courts of Dublin, Ireland;

9.4. UK Data. For the purposes of Personal Data that is subject to the UK Data Protection Laws ("**UK Data**"), the EU SCCs will also apply in accordance with paragraphs 9.3.a) to 9.3.d) above, with the following modifications:

a) references to "Regulation (EU) 2016/679" shall be interpreted as references to UK GDPR;

b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK GDPR;

c) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to the "UK" and "UK law";

d) the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK from the possibility of suing for their rights in their place of habitual residence (i.e., the UK);

e) Clause 13(a) of the EU SCCs and Part C3of Annex A of the DPA are not used and the "Supervisory authority" is the UK Information Commissioner's Office;

f) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales";

g) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales; and

h) with respect to transfers to which UK GDPR apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts",

i) unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer Personal Data in compliance with the UK GDPR, the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in Annexes A, B and C (as applicable).

10. Limitations of Liability

Customer's remedies, including its Affiliates, and the Provider's liability arising out of or in relation to this DPA (including Standard Contractual Clauses), are subject to those limitations of liability and disclaimers set forth in the Agreement. For the avoidance of doubt, nothing in this DPA is intended to limit the rights a Data Subject may have against either Party arising out of such Party's breach of the Standard Contractual Clauses, where applicable.

11. Final Provisions

11.1. Third-Party Beneficiaries. Data Subjects are the sole third-party beneficiaries to the Standard Contractual Clauses, and there are no other third-party beneficiaries to this DPA, unless specified to the contrary in the Agreement.

11.2. Governing Law and Jurisdiction. This DPA shall be governed by and construed with governing law and jurisdiction provisions in the Agreement, unless and to the extent required otherwise by the Data Protection Legislation or the Standard Contractual Clauses.

11.3. Scope of this DPA. For the avoidance of doubt, the processing of information other than Personal Data for the Permitted Purposes does not fall under the scope of this DPA.

11.4. Term. This DPA shall continue to be in effect for the term of the Agreement plus the period from expiry of the Agreement until the Provider ceases to process Personal Data on behalf of the Customer.

Annex A

Description of the Processing Activities / Transfer

Annex A(1) List of Parties:

Data Exporter	Data Importer
Name: Customer, as identified in the Order Form	**Name**: Provider, as identified in the Agreement
Address: As identified in the Order Form	**Address**: As identified in the Agreement
Contact details: As identified in the Order Form	**Contact details:** As identified in the Agreement
Activities relevant to the transfer: See Annex A(2) below	**Activities relevant to the transfer:** See Annex A(2) below
Role: Controller	**Role:** Processor

Annex A(2) Description of Transfer

	Description
Categories of data subjects:	• **Permitted users** – any of Customer's employees or other personnel, suppliers and other third parties authorised under the Agreement to use the Services. • employees, contractors, business partners, customers or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by The Provider.
Categories of personal data:	• **Permitted users** – contact data • Customer determines the categories of Personal Data which could be processed in The Provider's Platform.
Sensitive data:	The Provider does not require any special categories of data to provide the Services and does not intentionally collect or process such data in connection with the provision of the Services.
Frequency of the transfer:	Continuous

Nature and subject matter of processing:	The Personal Data may be subject to the following processing activities: • storage (hosting) and other processing necessary to provide, maintain and improve the Services provided to Customer under the Agreement, • technical support provided to the Customer on a case by case basis, • disclosures in accordance with the Agreement and the DPA, as compelled by law, and • collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Duration of the processing:	Processing Term.
Purpose(s) of the data transfer and further processing:	(i) Processing to provide, maintain, support, and improve the Services provided to the Customer in accordance with the Agreement; (ii) Processing initiated by the Permitted users in their use of the Services; and

	(iii) Processing to comply with other documented reasonable instructions provided by the Customer (e.g., via email) where such instructions are consistent with the Agreement of the Agreement (including this DPA).
Retention period (or, if not possible to determine, the criteria used to determine that period):	Processing Term

Annex A(3): Competent supervisory authority

With respect to EU Data the competent supervisory authority is The Office of the Information Commissioner of Czech Republic (the "**Supervisory Authority**").

Annex B
Approved Sub-processors

Country	Identification of sub-processor	Services	Additional information

California, USA or Ireland, European Union	**Amazon Web Services with the registered office at 410 Terry Ave. N., Seattle, WA 98109-5210, United States**	Cloud data storage infrastructure tools
USA	**Functional Software, Inc. (sentry.io) with the registered office at 45 Fremont Street, 8th Floor, San Francisco, CA 94105, United States**	Error reporting tools
USA	**Vonage Holdings Corp. with the registered office at 101 Crawfords Corner Rd, Suite 2416, Holmdel, NJ 07733, United States**	Hotline telephone line tool

Annex C

Technical and Organizational Measures

The technical and organisational measures implemented by the Provider (including any relevant certifications) to ensure an appropriate level of security taking into account the nature, scope, context, and purposes of the processing, and the risks for the rights and freedoms of natural persons, are described at privacy policy and:

Type of measure	Implemented measure
Measures of pseudonymisation and encryption of personal data	User has the option to choose between two encryption modes: ● Standard encryption ● End-to–end encryption Standard encryption is the mode that is normally a viable option for most of our users. In end-to-end encryption, keys are stored and do not leave the user's device and all of the data is encrypted and decrypted only there.
Measures for ensuring ongoing confidentiality of processing systems and the Services	Contracts with all our employees contain confidentiality clauses and employees are obliged to follow internal rules on personal data processing. All employees go through security training which contains mandatory security and data privacy training. All employees follow our stringent password policy.
Measures for ensuring ongoing integrity of processing systems and the Services	We follow security requirements from ISO 27001:2013 standard which we have been granted. We regularly run independent security penetration tests. We ensure functional Vulnerability and Patch management. We enable exit procedures by downloading data from the system. We ensure compliance with

	all measures to ensure the ongoing integrity of processing systems and the Services.
Measures for ensuring ongoing availability and resilience of processing systems and the Services	To monitor platform availability, we rely on UptimeRobot, which notifies us promptly in the event of any unavailability or potential issues. Our infrastructure is configured using Terraform, enabling us to easily redeploy the entire stack to an alternative availability zone in the event of some disaster (availability zone failure), ensuring continuous service. For data integrity, we maintain regular backups of our database, allowing for swift restoration in a matter of minutes if necessary. If any incident occurs, we maintain an incident report database, where an exact description of the reason behind the incident, scope of incident and the precautions applied are mentioned. We are open to signing SLAs. In case of any incidents, we maintain an incident report database for accurate documentation.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	To ensure data protection and disaster recovery capabilities, we have implemented automated backups for our database. These backups are scheduled to occur once per day. The backups are performed for both regions and stored in two availability zones (a and b zones) to ensure redundancy and fault tolerance. With a retention period of 25 days and point-in-time recovery in place, we can restore any exact database state in any chosen

	minute up to the retention period. Additionally, during major data migrations, we also take manual snapshots to create additional restore points.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	To ensure the robustness of our security measures, we conduct regular security testing. Once a year, we engage an external penetration testing firm, to evaluate the strength of our systems against potential threats. The results of these tests are discussed in security team meetings, where findings are discussed and prioritized for remediation. Findings are then integrated into developers team sprint cycles to resolve them. We also convene an annual security team meeting to review our security measures, propose enhancements, and suggest changes to our processes.
Measures for user identification and authorization	Users can utilize multiple options for strengthening their account security. This section goes through MFA, SSO providers we provide and also more into the user permissions, which can be leveraged.
Measures for the protection of Data during storage	Data are encrypted, both at rest and in transit, using a modern cryptographic cypher, with a minimum 128-bit key for symmetric encryption and a 1024-bit key length for asymmetric

	encryption. Additionally, backups are performed on a regular basis and stored in multiple locations. We follow the principle of least privilege for all our internal systems.Our platform supports MFA and enforces strong passwords of our users.
Measures for ensuring physical security of locations at which personal data are processed	Given the fact that all of our platform is run in the cloud, most of the software centered physical security is transferred to our cloud provider, currently AWS. When setting up their accounts, users are also free to choose in which region they want to have their data stored. Data between regions are not shared, apart from the bare minimum used for discovery of the preferred region of the user. Personal information (emails) in the global database is also hashed, so there is no way of actually retrieving them back. Physical security of the platform data is thus handled by AWS exhaustive security measures, some of which are: • ISO9001, ISO22301, ISO27001, ISO27017 • SOC1, SOC2, SOC3 and many more.
Measures for ensuring events logging	All system events must be recorded and logged for a minimum of 3 months. Additionally, there are various monitoring tools

	and services in place, such as AWS CloudWatch with the database and application logs, Sentry for error events and Datadog Cloud SIEM for security alerting, to ensure comprehensive monitoring and prompt notification of any anomalies or critical incidents. This allows for immediate action to be taken to maintain the reliability and security of the system.
Measures for ensuring system configuration, including default configuration	The system configuration is located in AWS cloud where all of the needed variables are stored in secure manner. The access to the configurations is then limited to a small amount of senior engineers, with a set up approval processes for managing change through the Terraform configurations.
Measures for internal IT and IT security governance and management	We have a dedicated team of information security and development/IT services who is responsible for the information security of our product. We carry out regular IT and data security audits and maintain separate systems for development, testing, and production. We have a Business Continuity Plan in place that has been tested and validated. Additionally, we have a policy and procedure in place for information security incidents, and all employees are trained to report any incidents. We also have measures in place for internal IT and IT security governance and management, including penetration testing, access controls,

	and authentication for API connections. We maintain records of all audits and have certifications for IT and data security.
Measures for certification/assurance of processes and products	We regularly review and enhance our security measures through an annual security team meeting. We also have a disaster recovery process in place that is tested and validated. We maintain a list of service providers and evaluate the risks presented by each of them in terms of data protection. We have an access management policy in place and perform periodic reviews of users' access rights.
Measures for ensuring data minimization	We strictly follow the principle of data minimization. This includes strict purpose limitation, access restrictions, keeping a record of access to the data, restrictions for onward transfers, and additional security measures. We always review these measures regularly to ensure their appropriateness with regards to evolving risks.

Measures for ensuring data quality	Data quality is ensured through stringent security policy and regular IT and data security audits and penetration tests, as well as risk management governance. Our company puts emphasis on the highest standard of data security. The organization maintains separate systems for development, testing, and production, and has a tested and validated Business Continuity Plan in place.
Measures for ensuring limited data retention	The data retention period can be customized to the specific needs of our clients. After such retention period has expired or upon specific request of the client, we discard all personal data and reports belonging to the organization.
Measures for ensuring accountability	There are several measures in place to ensure accountability within the organization. These include a dedicated team or individual who is appropriately trained to manage security incidents, access controls that restrict access on a 'least privilege' methodology and are role-based, regular information security awareness training for employees, an incident management process for reporting and investigating unauthorized information disclosure, and a backup management process that includes regular backups and storage in multiple locations. Additionally, there is a designated leader responsible for information security. These measures aim to

	promote accountability and protect the integrity of the information provided by employees.
Measures for allowing data portability and ensuring erasure	Data can be downloaded at any time in various industry standard formats. We follow strict protocols for data deletion.

Data Processing Addendum