DATA PROCESSING STATEMENT FOR ERM LIBRYO SUBSCRIPTION SERVICES

This Data Processing Statement applies to, and forms part of, the Agreement for ERM Libryo Subscription Services Terms ("**Libryo Terms**") between ERM and the Customer. Capitalized terms not defined in this Data Processing Statement are defined elsewhere in the Agreement.

1. DEFINITIONS

1.1 "**Audit**" and "**Audit Parameters**" are defined in clause 9.3 below.

1.2 "**Audit Report**" is defined in clause 9.2.1 below.

1.3 "**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 Processing of Personal Data.

1.4 "**Customer Instructions**" means: (i) Processing to provide the Libryo Platform and perform ERM's obligations in the Agreement (including this Data Processing Statement) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

1.5 "**Customer Personal Data**" means Personal Data contained in any information, materials or Other Content hosted or contained within the Libryo Platform.

1.6 "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.7 "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.8 "**EEA**" means European Economic Area.

1.9 "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.10 "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.12 "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a

transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.13 "**Schedule**" means any of the Schedules attached to this Data Processing Statement.

1.14 "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by ERM.

1.15 "**Specified Notice Period**" is 48 hours.

1.16 "**Subprocessor**" means any third party authorized by ERM to Process any Customer Personal Data.

1.17 "**Subprocessor List**" means the list of ERM's Subprocessors as identified in Schedule 5.

2. SCOPE AND DURATION

2.1 This Data Processing Statement applies to ERM as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.

2.2 This Data Processing Statement applies to ERM's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This Data Processing Statement is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3 This Data Processing Statement commences on the Effective Date and terminates upon expiration or termination of the Agreement (or, if later, the date on which ERM has ceased all Processing of Customer Personal Data).

2.4 In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the Order Form, (2) any Standard Contractual Clauses or other measures to which the Parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (3) this Data Processing Statement and (4) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this Data Processing Statement (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. PROCESSING OF PERSONAL DATA

3.1 Customer Instructions

3.1.1 ERM will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with ERM's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

3.1.2 Details regarding the Processing of Customer Personal Data by ERM are set forth in Schedule 1 (Subject Matter and Details of Processing).

3.1.3 ERM will notify Customer if it receives an instruction that ERM reasonably determines infringes Data Protection Laws (but ERM has no obligation to actively monitor Customer's compliance with Data Protection Laws).

3.2 Confidentiality

3.2.1 ERM will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

3.2.2 ERM will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3 Compliance with Laws

3.3.1 ERM and Customer will each comply with Data Protection Laws in their respective Processing of

Customer Personal Data.

3.3.2 Customer will comply with Data Protection Laws in its issuing of Customer Instructions to ERM. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable ERM to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this Data Processing Statement), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.3.3 The Parties will work together in good faith to negotiate an amendment to this Data Processing Statement as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. SUBPROCESSORS

4.1 Customer generally authorizes ERM to engage Subprocessors to Process Customer Personal Data. Customer further agrees that ERM may engage its Affiliates as Subprocessors.

4.2 ERM will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this Data Processing Statement and (ii) remain liable for compliance with the obligations of this Data Processing Statement and for any acts or omissions of a Subprocessor that cause ERM to breach any of its obligations under this Data Processing Statement.

4.3 ERM will keep its Subprocessor List updated.

4.4 Notice of New Subprocessors

4.4.1 ERM may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, ERM will add such Subprocessor to the Subprocessor List and notify Customer through email or other means specified in the Agreement.

4.4.2 If, within 30 days after notice of a new Subprocessor, Customer notifies ERM in writing that Customer objects to ERM's appointment of such new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith.

4.4.3 If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience and ERM will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. SECURITY

5.1 ERM will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, and as further described in Schedule 2 (Technical and Organizational Measures). ERM will regularly monitor its compliance with its security measures and Schedule 2 (Technical and Organizational Measures).

5.2 Incident Notice and Response

5.2.1 ERM will implement and follow procedures to detect and respond to Security Incidents.

5.2.2 ERM will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within ERM's reasonable control.

5.2.3 Upon Customer's request and taking into account the nature of the applicable Processing, ERM will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

5.2.4 Customer acknowledges that ERM's notification of a Security Incident is not an acknowledgement

by ERM of its fault or liability.

5.2.5 Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3 Customer Responsibilities

5.3.1 Customer is responsible for reviewing the information made available by ERM relating to data security and making an independent determination as to whether the Libryo Platform meets Customer's requirements and legal obligations under Data Protection Laws.

5.3.2 Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. DATA PROTECTION IMPACT ASSESSMENT

6.1 Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to ERM, ERM will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Libryo Platform, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. DATA SUBJECT REQUESTS

7.1 Upon Customer's request and taking into account the nature of the applicable Processing, ERM will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Libryo Platform).

7.2 If ERM receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, ERM will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. DATA RETURN OR DELETION

8.1 During the Subscription Term, Customer may, through the features of the Libryo Platform or such other means specified in the Agreement, access, return to itself or delete Customer Personal Data.

8.2 Post Termination

8.2.1 Following termination or expiration of the Agreement, ERM will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from ERM's systems.

8.2.2 Deletion will be in accordance with industry-standard secure deletion practices. ERM will issue a certificate of deletion upon Customer's request.

8.2.3 Notwithstanding the foregoing, ERM may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, ERM will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this Data Processing Statement with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such

purpose(s) and duration specified in such applicable Data Protection Laws.

9. AUDITS

9.1 ERM will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with ERM's obligations under this Data Processing Statement and Data Protection Laws.

9.2 Third-Party Compliance Program

9.2.1 ERM will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).

9.2.2 Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

9.2.3 Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of clause 9.3 (Customer Audit) below.

9.3 Customer Audit

9.3.1 Subject to the terms of this clause 9.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with ERM that is consistent with the Audit Parameters (an "**Audit**").

9.3.2 Customer may exercise its Audit right: (i) to the extent ERM's provision of an Audit Report does not provide sufficient information for Customer to verify ERM's compliance with this Data Processing Statement or the Parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

9.3.3 Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with ERM, (ii) be limited in scope to matters reasonably required for Customer to assess ERM's compliance with this Data Processing Statement and the Parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during ERM's Business Hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by ERM, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. CROSS-BORDER TRANSFERS/REGION-SPECIFIC TERMS.

10.1 ERM (and members of its Group) may Process and transfer Customer Personal Data globally as necessary to perform its obligations under the Agreement.

10.2 If ERM engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.3 To the extent that ERM Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this Data Processing Statement.

This Data Processing Statement uses the standard Bonterms Data Protection Addendum (version 1.0), which has been designed with balanced positions in mind to meet the needs of both Parties. These terms are free to use under CC BY 4.0. ERM has modified these terms to align them with the structure and defined terms used in the Agreement.

SCHEDULE 1: SUBJECT MATTER AND DETAILS OF PROCESSING

Customer / 'Data Exporter' Details	
Name	As specified in the ERM Services Agreement.
Contact details for data protection	As specified in the ERM Services Agreement.
Main address	As specified in the ERM Services Agreement.
Customer activities	As specified in the ERM Services Agreement.
Role	Controller

ERM / 'Data Importer' Details	
Name	As specified in the ERM Services Agreement.
Contact details for data protection	As specified in the ERM Services Agreement.
Main address	As specified in the ERM Services Agreement.
Customer activities	As specified in the ERM Services Agreement.
Role	Processor

Details of Processing	
Categories of Data Subjects	Authorised Users of the Libryo Platform
Categories of Customer Personal Data	Name, professional email address, user name
Sensitive Categories of Data and additional associated restrictions /safeguards	None
Nature of the Processing	Authentication and identification of Authorised Users
Purpose of the Processing	To provide the Libryo Platform
Duration of Processing / retention period	For the Subscription Term and post termination in accordance with the terms of the Agreement.
Categories of Data Subjects	Authorised Users of the Libryo Platform

SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL MEASURES

General Information Security Management
ERM has a dedicated Cyber and Information Security team responsible for maintaining security and implementing security roadmap enhancements across its organization. A comprehensive set of global information security policies and standards are maintained and reviewed at least annually. ERM's Information Security Management System (ISMS), global information security policies, risk management practices, and security controls are aligned with ISO/IEC 27001.

Secure Development
Development teams within ERM align their development practices with an internal Secure Development Life Cycle (SDLC). An internal assurance program is maintained to ensure that ERM products comply with the SDLC and ERM's global information security policies and standards.

Access Control
Access to the underlying Libryo Platform infrastructure and development platforms is strictly controlled. Access is only provisioned to authorized employees following the principle of least privilege.

Technology Resilience
Annual business impact assessments (BIA) are performed against business-critical services and systems. Technology resilience plans containing business continuity and disaster recovery requirements are implemented for ERM's business-critical services.

Asset Management
The Libryo Platform infrastructure assets are centrally managed within Amazon Web Services (AWS).

Physical Security
The Libryo Platform is hosted within AWS data centers which employ strong physical security controls.

Personnel Security
ERM includes provisions for confidentiality and non-disclosure in all employment agreements and contracts where local jurisdiction law allows. All ERM employees and temporary workers undertake mandatory information security training within their first ten days of employment and annually thereafter. Phishing simulations are conducted to evaluate the awareness of employees and the effectiveness of security training.

Incident Management
ERM maintains an Information Security Incident Management Policy, a Security Incident Response Plan, and supporting runbooks and procedures to ensure a consistent approach to incident management. The incident response plan is tested annually to ensure its effectiveness in a real incident scenario.

Internet Protection
ERM protects all internet-based traffic originating from an ERM endpoint through security tooling which provides a protected web gateway. The tooling utilized also provides intrusion prevention capabilities.
All endpoint internet traffic is routed through the proxy software, which enforces various policies to block access to malicious content. TLS inspection is performed to identify threats in encrypted channels and all downloads are run in a sandbox environment to protect endpoints from malicious content.

Supply Chain Risk Management
ERM's third parties are continually monitored for security risk using dedicated supply chain risk management tooling.

SCHEDULE 3: CROSS-BORDER TRANSFER MECHANISMS

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the Data Processing Statement.

   a. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

   b. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

   c. "**Designated EU Governing Law**" means the laws of Ireland.

   d. "**Designated EU Member State**" means Ireland.

2. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

   a. The EU SCCs are hereby incorporated by reference as follows:

      i. Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and ERM is a Processor of Customer Personal Data;

      ii. Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and ERM is a Processor of Customer Personal Data;

      iii. Customer is the "data exporter" and ERM is the "data importer"; and

      iv. by entering into this Data Processing Statement, each Party is deemed to have signed the EU SCCs (including their Annexes) as of the Effective Date.

   b. For each Module, where applicable the following applies:

      i. the optional docking clause in Clause 7 does not apply;

      ii. in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this Data Processing Statement, and ERM shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with clause 4.4 of this Data Processing Statement;

      iii. in Clause 11, the optional language does not apply;

      iv. in Clause 13, all square brackets are removed with the text remaining;

      v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;

      vi. in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;

      vii. Schedule 1 (Subject Matter and Details of Processing) to this Data Processing Statement contains the information required in Annex 1 of the EU SCCs; and

      viii. Schedule 2 (Technical and Organizational Measures) to this Data Processing Statement contains the information required in Annex 2 of the EU SCCs.

   c. Where context permits and requires, any reference in this Data Processing Statement to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this paragraph 2.

3. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

a. The EU SCCs apply as set forth in paragraph 2 (EU Transfers) of this Schedule 3 with the following modifications:

i. in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

ii. in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

iii. in Clause 18(b), disputes will be resolved before the courts of Switzerland;

iv. the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

v. all references to the EU GDPR in this Data Processing Statement are also deemed to refer to the FADP.

4. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

a. The EU SCCs apply as set forth in paragraph 2 (EU Transfers) of this Schedule 3 with the following modifications:

i. each Party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

ii. the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

iii. in Table 1 of the UK Addendum, the Parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this Data Processing Statement;

iv. in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

v. in Table 3 of the UK Addendum:

1. the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this Data Processing Schedule;

2. the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this Data Processing Statement;

3. Annex II is located in Schedule 2 (Technical and Organizational Measures) to this Data Processing Statement; and

4. the list of Subprocessors is located in Schedule 5 (Subprocessor List) to this Data Processing Statement.

5. in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

6. in Part 2: Part 2 – Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

SCHEDULE 4: REGION-SPECIFIC TERMS

A. CALIFORNIA

1. **Definitions**. CCPA and other capitalized terms not defined in this Schedule are defined in the Data Processing Statement.

   a. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

   b. The definition of "Data Subject" includes "consumer" as defined under the CCPA.

   c. The definition of "Controller" includes "business" as defined under the CCPA.

   d. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. **Obligations**

   a. Customer is providing the Customer Personal Data to ERM under the Agreement for the limited and specific business purposes of providing the Libryo Platform as described in Schedule 1 (Subject Matter and Details of Processing) to this Data Processing Statement and otherwise performing under the Agreement.

   b. ERM will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

   c. ERM acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under clause 9 (Audits) of this Data Processing Statement to help to ensure that ERM's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from ERM notice and assistance under clause 7 (Data Subject Requests) of this Data Processing Statement regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

   d. ERM will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

   e. ERM will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in paragraph 2.a of this Section A (California) of Schedule 4 or (ii) outside of the direct business relationship between ERM with Customer, except, in either case, where and to the extent permitted by the CCPA.

   f. ERM will not sell or share Customer Personal Data received under the Agreement.

   g. ERM will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

SCHEDULE 5: SUBPROCESSOR LIST

Customer hereby authorizes ERM to use the following Subprocessors:

- Amazon Web Services
  - Service provided: hosting of the Libryo Platform
  - Personal data processed: names and corporate email addresses
  - Location of the processing: Ireland
  - Duration of the processing: Contract period plus one year
  - Transfer tool: SCC
  - Additional measures implemented if any: encryption

- Hubspot
  - Service provided: CRM and customer success
  - Personal data processed: names and corporate email addresses, corporate contact numbers
  - Location of the processing: United States
  - Duration of the processing: Contract period plus one year
  - Transfer tool: SCC
  - Additional measures implemented if any: data encryption

- Microsoft
  - Service provided: office 365 including outlook for email
  - Personal data processed: names and corporate email addresses
  - Location of the processing: Ireland
  - Duration of the processing: Contract period plus one year
  - Transfer tool: SCC
  - Additional measures implemented if any: encryption

- Sendgrid by Twillio
  - Personal data processed: names and corporate email addresses
  - Location of the processing: United States
  - Duration of the processing: Contract period plus one year
  - Transfer tool: SCC
  - Additional measures implemented if any: encryption