REPRISE DATA PROCESSING AGREEMENT

HOW THIS DPA APPLIES

This Reprise Data Processing Agreement ("DPA") forms part of your Agreement with Reprise and contains certain terms relating to data protection, privacy, and security in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199) ("CCPA"), where applicable. In the event (and to the extent only) that there is a conflict between the GDPR and the CCPA, the parties shall comply with the more onerous requirement or higher standard which shall, in the event of a dispute in that regard, be determined solely by Reprise.

This DPA is between the Customer and Reprise, Inc.

This is the latest version of the DPA (dated 27 July 2022).

DATA PROCESSING TERMS

1. **Interpretation.**

   In this DPA the following expressions shall, unless the context otherwise requires, have the following meanings:

1.1 "**Agreement**" means any agreement between Reprise Inc. and a customer for the Services. Such an agreement may have various titles, such as "Order Form", "Sales Order", "Subscription Agreement", or "Master Subscription Agreement".

1.2 "**Article 28**" means article 28 of GDPR.

1.3 "**Customer**" or "**you**" means the customer that is identified on, and/or is a party to, the Agreement.

1.4 "**Customer Data**" means all data (including but not limited to Customer Personal Data and End User data) that is provided to Reprise by, or on behalf of, Customer through Customer's use of the Services, and any data that third parties submit to Customer through the Services.

1.5 "**Customer Personal Data**" means all personal data (including that of End Users) that is submitted to the Services by or to Customer, processed by Reprise for the purposes of delivering the Services to the Customer including but not limited to the personal data set out in Appendix 2 to this DPA.

1.6 "**Data Protection Legislation**" means:

(a) the GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of personal data under the Agreement;

(b) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to CCPA;

(c) all laws and regulations that apply to processing of personal data under the Agreement from time to time in place in the United Kingdom and Canada, and

(d) the terms "controller", "data subject", "data protection impact assessment", "personal data", "process", "processing", "processor", "supervisory authority" have the same meanings as in the GDPR and with respect to CCPA (as defined above), Reprise and Customer hereby agree that Reprise is a "**Service Provider**" and Customer is the "**Business**", as defined under the CCPA and with respect to Personal Information (as defined under the CCPA).

1.7 "**End Users**" means Customer's employees, agents, independent contractors and other individuals authorized by Customer to access and use the Services.

1.8 "**Reprise**" or "**us**" means Reprise Inc.

1.9 "**Reprise Inc.**" means Reprise Inc., a Delaware corporation located at 407 Marlborough Street, Unit 6B, Boston, MA 02115, United States.

1.10 "**Reprise Privacy Notice**" means the Reprise Privacy Notice at https://www.getreprise.com/privacy/.

1.11 "**Services**" means the services ordered by Customer from Reprise under the Agreement.

1.12 "**Standard Contractual Clauses**" means the "Standard Contractual Clauses" annexed to the European Commission Decision of: i) 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR or ii) (until such times as Reprise has entered into the Standard Contractual Clauses outlined at i)), the 5 February 2010 for the Transfer of Customer Personal Data to Processors established in Third Countries under Directive 95/46/EC).

2. **Status of Reprise.**

In the provision of the Services to the Customer, Reprise is a processor of Customer Personal data for the purposes of GDPR.

3. **Term.**

This DPA shall remain in force until such time as the Agreement is terminated (in accordance with its terms) or expires.

4. **Customer's Obligations.**

Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Customer Data to Reprise so that Reprise may lawfully process and transfer the personal data in accordance with this DPA. Customer shall ensure that any relevant data subjects have been informed of such use, processing, and transfer as required by the Data Protection Legislation and that lawful consents have been obtained (where appropriate). Customer shall ensure that any personal data processed or transferred to Reprise will be done lawfully and properly.

5. **Reprise's Obligations.**

5.1 Where Reprise is processing Customer Personal Data for Customer as a processor, Reprise will:

(a) only do so on documented Customer instructions and in accordance with the Data Protection Legislation, including with regard to transfers of personal data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to Reprise to process Customer Personal Data (including to locations outside of the EEA) along with other reasonable instructions provided by the Customer to Reprise (e.g. via email) where such instructions are consistent with the Agreement;

(b) ensure that all Reprise personnel involved in the processing of Customer Personal Data are subject to confidentiality obligations in respect of the personal data;

(c) make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (if applicable to the Customer) where such information is held by Reprise and is not otherwise available to Customer through its account and user areas or on Reprise websites, provided that Customer provides Reprise with at least 14 days' written notice of such an information request;

(d) co-operate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a data subject afforded to data subjects by Data Protection Legislation in respect of personal data processed by Reprise in providing the Services;

(e) provide assistance, where necessary, with requests received directly from a Data Subject in respect of a Data Subject's Personal Data submitted through the Services;

(f) upon deletion by you, not retain Customer Personal Data from within your account other than in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to our retention policies;

(g) cooperate with any supervisory authority or any replacement or successor body from time to time (or, to the extent required by the Customer, any other data protection or privacy regulator under Data Protection Legislation) in the performance of such supervisory authority's tasks where required;

(h) assist Customer as reasonably required where Customer:

(i) conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow customer to conduct their own assessment); or

(ii) is required to notify a Security Incident (as defined below) to a supervisory authority or a relevant data subject

(i) will not (a) sell any Personal Information (as defined under the CCPA) for a commercial purpose, or (b) collect, retain, use, disclose, or otherwise process Personal Information other than (1) to fulfill its obligations to Customer under the Agreement, (2) on the Customer's behalf, (3) for the Customer's operational purposes, (4) for Reprise's internal use as permitted by Data Protection Legislation, (5) to detect data security incidents or protect against fraudulent or illegal activity, or (6) as otherwise permitted under Data Protection Legislation;

(j) Where required by Data Protection Legislation, Reprise will inform Customer if it comes to its attention that any instructions received by Customer infringe the provisions of Data Protection Legislation. Notwithstanding the foregoing, Reprise shall have no obligation to monitor or review the lawfulness of any instruction received from the Customer; and

(k) Reprise certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.

6. **Subprocessors.**

6.1 Subprocessing. Customer provides a general authorization to Reprise to engage onward subprocessors, subject to compliance with the requirements in this Section 6.

6.2 Subprocessor List. Reprise will, subject to the confidentiality provisions of the Agreement or otherwise imposed by Reprise:

(a) make available to Customer a list of the Reprise subcontractors who are involved in processing or subprocessing Customer Personal Data in connection with the provision of the Services

(b) ("Subprocessors"), together with a description of the nature of services provided by each Subprocessor ("Subprocessor List"). A copy of this Subprocessor List may be requested at https://www.reprise.com/subprocessors/;

(c) ensure that all Subprocessors on the Subprocessor List are bound by contractual terms that are in all material respects no less onerous than those contained in this DPA; and

(d) be liable for the acts and omissions of its Subprocessors to the same extent Reprise would be liable if performing the services of each of those Subprocessors directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.3 New / Replacement Subprocessors. Reprise will provide Customer with written notice of the addition of any new Subprocessor or replacement of an existing Subprocessor at any time during the term of the Agreement ("New Subprocessor Notice"). The Customer will sign up to a mailing list made available by Reprise through which such notices will be delivered by e-mail or alternatively will check on updates to the list here: https://www.reprise.com/subprocessors/. If Customer has a reasonable basis to object to Reprise's use of a new or replacement Subprocessor, Customer will notify Reprise promptly in writing and in any event within 30 days after receipt of a New Subprocessor Notice. In the event of such reasonable objection, either Customer or Reprise may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Subprocessor (which may, at Reprise's discretion and election, involve termination of the entire Agreement) with immediate effect by providing written notice to the other party. Such termination will be without a right of refund for any fees prepaid by Customer for the period following termination.

7. **Security.**

7.1 Security Measures. Reprise has, taking into account the state of the art, cost of implementation and the nature, scope, context and purposes of the Services and the level of risk, implemented appropriate technical and organizational measures (in accordance with Appendix 1) to ensure a level of security appropriate to the risk of unauthorized or unlawful processing, accidental loss of and/or damage to Customer Data. At reasonable

intervals, Reprise tests and evaluates the effectiveness of these technical and organizational measures for ensuring the security of the processing.

7.2 Security Incident and Breach Notification. If Reprise becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Personal Data ("**Security Incident**"), Reprise will take reasonable steps to notify Customer without undue delay. A Security Incident does 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, or other network attacks on firewalls or networked systems. Any notification of a Security Incident to the Customer does not constitute any acceptance of liability by Reprise.

7.3 Reprise will also reasonably cooperate with Customer with respect to any investigations relating to a Security Incident with preparing any required notices, and provide any information reasonably requested by Customer in relation to any Security Incident.

8. **Audits.**

8.1 Audits. Where Reprise is processing Customer Personal Data for Customer as a processor (only), the Customer will provide Reprise with at least one month's prior written notice of any audit, which may be conducted by Customer or an independent auditor appointed by Customer (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of Reprise) ("**Auditor**"). The scope of an audit will be as follows:

(a) Customer will only be entitled to conduct an audit once per subscription year unless otherwise legally compelled or required by a regulator with established authority over the Customer to perform or facilitate the performance of more than 1 audit in that same year (in which circumstances Customer and Reprise will, in advance of any such audits, agree upon a reasonable reimbursement rate for Reprise's audit expenses).

(b) Reprise agrees, subject to any appropriate and reasonable confidentiality restrictions, to provide evidence of any certifications and compliance standards it maintains and will, on request, make available to Customer an executive summary of Reprise's most recent annual penetration tests, which summary shall include remedial actions taken by Reprise resulting from such penetration tests.

(c) The scope of an audit will be limited to Reprise systems, processes, and documentation relevant to the processing and protection of Customer Personal Data, and Auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by Reprise.

(d) Customer will promptly notify and provide Reprise on a confidential basis with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

8.2 The parties agree that, except as otherwise required by order or other binding decree of a supervisory authority or regulator with authority over the Customer, this Section 8 sets out the entire scope of the Customer's audit rights as against Reprise.

9. **International Data Transfers.**

9.1 To the extent applicable, for transfers of Customer Personal Data from the European Economic Area to locations outside the European Economic Area (either directly or via onward transfer) that do not have adequate standards of data protection as determined by the European Commission, Reprise relies upon:

(a) the Standard Contractual Clauses as attached to this DPA at Appendix 3; or

(b) such other appropriate safeguards, or derogations (to the limited extent appropriate), specified or permitted under the Data Protection Legislation.

9.2 With respect to Reprise's reliance on the Standard Contractual Clauses for international transfers of Customer Personal Data under the Agreement, Reprise shall act in its capacity as 'data importer' or 'data exporter' (as appropriate) as set out in the relevant modules of the Standard Contractual Clauses (as applicable). Upon written request and in accordance with the provisions of the Standard Contractual Clauses, Reprise will provide copies of the Standard Contractual Clauses entered into with data importers in its capacity as processor to the Customer.

10. **General Provisions.**

10.1 Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.

10.2 Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the Agreement, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

10.3 Independent Processing. Customer remains exclusively liable for its own compliance with Data Protection Legislation with respect to any independent collection and processing of personal data unrelated to the Services. Customer will provide its own clear and conspicuous privacy notices that accurately describe how it does this and Reprise will not be liable for any treatment of personal data by Customer in those circumstances. Customer hereby indemnifies Reprise in full for any and all claims or liability arising as a result of such collection and use of personal data by it in those circumstances.

10.4 Entire Agreement. The Agreement (which incorporates this DPA) and any Order Form represent the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations not recorded in the Agreement inducing it to enter into the Agreement.

10.5 Severance. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, nor authorise any party to make or enter into any commitments for or on behalf of any other party except as expressly provided herein.

10.6 Electronic Copy. This DPA is delivered as an electronic document.

10.7 Governing Law. This DPA shall be governed by the laws of Ireland and the parties submit to the exclusive jurisdiction of the Irish courts (in relation to all contractual and non-contractual disputes) except in the case of any alleged breach or breach of current or future privacy laws, regulations, standards, regulatory guidance, and self-regulatory guidelines at state or federal level in the United States of America, in which case the laws of the State of Massachusetts shall govern unless otherwise dictated by that law.

APPENDIX 1

Description of the technical and organisational security measures implemented by Reprise

Reprise will maintain appropriate administrative, physical, and technical safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of personal data provided to it for provision of the Services to the Customer.

The Security Safeguards include the following:

1) **Domain: Organization of Information Security**.
   a) **Security Roles and Responsibilities.** Reprise personnel with access to data are subject to confidentiality obligations.
   b) **Risk Management Program.** Reprise performs a risk assessment where appropriate before processing the data.
2) **Domain: Asset Management.**
   a) **Asset Handling.**
      i) Reprise has procedures for disposing of printed materials that contain Customer Data.
      ii) Reprise maintains an inventory of all hardware on which Customer Data is stored.
3) **Domain: Human Resources Security.**
   a) **Security Training.**
      i) Reprise informs its personnel about relevant security procedures and their respective roles. Reprise also informs its personnel of possible consequences of breaching the security rules and procedures.
4) **Domain: Physical and Environmental Security.**
   a) **Physical Access to Facilities.** Reprise limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.
   b) **Protection from Disruptions.** Reprise uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
   c) **Component Disposal.** Reprise uses industry standard processes to delete Customer Data when it is no longer needed.
5) **Domain: Communications and Operations Management.**
   a) **Operational Policy.** Reprise maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.
   b) **Data Recovery Procedures.**
      i) On a regular and ongoing basis, Reprise creates backup copies of Customer Data from which Customer Data may be recovered in the event of loss of the primary copy.
      ii) Reprise stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is

located.

iii) Reprise has specific procedures in place governing access to copies of Customer Data.

c) **Malicious Software.** Reprise has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

d) **Data Beyond Boundaries**.

i) Reprise encrypts Customer Data that is transmitted over public networks.

e) Event Logging.

i) Reprise logs the use of its data-processing systems.

ii) Reprise logs access and use of information systems containing Customer Data, registering the access ID, timestamp, and certain relevant activity.

6) **Domain: Information Security Incident Management.**

a) **Incident Response Process.**

i) Reprise maintains an incident response plan.

ii) Reprise maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and remediation steps, if applicable.

7) **Domain: Business Continuity Management.**

a) Reprise's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

8) **Access Control to Processing Areas**. Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Customer Personal Data are processed or used, to include:

a) establishing secure areas;

b) protection and restriction of access paths;

c) securing the mobile/cellular telephones;

d) data processing equipment and personal computers;

e) all access to the data centers where Customer Personal Data are hosted is logged, monitored, and tracked;

f) the data centers where Customer Personal Data are hosted is secured by a security alarm system, and other appropriate security measures; and

g) the facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, keycard and/or biometric access (as appropriate to level of risk) screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

9) **Access Control to Data Processing Systems.** Processes to prevent data processing systems from being used by unauthorized persons, to include:

a) identification of the terminal and/or the terminal user to the data processor systems;
b) automatic time-out after 30 minutes or less of user terminal if left idle, identification and password required to reopen;
c) issuing and safeguarding of identification codes;
d) password complexity requirements (minimum length, expiry of passwords, etc.); and
e) protection against external access by means of an industrial standard firewall.

10) **Access Control to Use Specific Areas of Data Processing Systems.** Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Personal Data cannot be read, copied, modified or removed without authorization, to include by:
a) implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Personal Data;
b) effective and measured disciplinary action against individuals who access Customer Personal Data without authorization;
c) release of data to only authorized persons;
d) implementing principles of least privileged access to information which contains Customer Personal Data strictly on the basis of "need to know" requirements;
e) production network and data access management governed by VPN, two factor authentication, and role- based access controls;
f) application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and
g) policies controlling the retention of backup copies which are in accordance with applicable laws and which are appropriate to the nature of the data in question and corresponding risk.

11) **Transmission Control.** Procedures to prevent Customer Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Customer Personal Data by means of data transmission facilities is envisaged, to include:
a) use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
b) implementation of VPN connections to safeguard the connection to the internal corporate network;
c) constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and
d) monitoring of the completeness and correctness of the transfer of data (end-to-end check).

12) **Storage Control.** When storing any Customer Personal Data: it will be backed up as part of a

designated backup and recovery processes in encrypted form, using a commercially supported encryption solution and all data defined as Customer Personal Data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption;

13) **Input Control.** Measures to ensure that it is possible to check and establish whether and by whom Customer Personal Data has been input into data processing systems or removed, to include:
    a) authentication of the authorized personnel;
    b) protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
    c) utilization of user codes (passwords);
    d) proof established within data importer's organization of the input authorization; and
    e) ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.
14) **Availability Control.** Measures to ensure that Customer Personal Data are protected from accidental destruction or loss, to include infrastructure redundancy and regular backups performed on database servers.
15) **Segregation of Processing.** Procedures to ensure that data collected for different purposes can be processed separately, to include:
    a) separating data through application security for the appropriate users;
    b) storing data, at the database level, in different tables, separated by the module or function they support;
    c) designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately; and
    d) barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.
16) **Vulnerability management program.** A program to ensure systems are regularly checked for vulnerabilities and any detected are immediately remedied, to include:
    a) all networks, including test and production environments, regularly scanned; and
    b) penetration tests are conducted regularly and vulnerabilities are remedied promptly.
17) **Data Destruction.** In the event of expiration or termination of the Agreement by either side or otherwise on request from the Customer following receipt of a request from a data subject or regulatory body:
    a) all Customer data shall be securely destroyed within 3 months; and
    b) all Customer data shall be purged from all Reprise and/or third-party storage devices including backups within 6 months of termination or receipt of a request from Customer unless Reprise is otherwise required by law to retain a category of data for longer periods. Reprise will ensure that all such data which is no longer required is destroyed to a level where it can be assured that it is no longer recoverable.

18) **Standards and Certifications.** Data storage solutions and/or locations have at least SOC 1 (SSAE 16) or SOC 2 reports – equivalent or similar certifications or security levels will be examined on a case-by-case basis.

APPENDIX 2

Purposes and Nature of Personal Data Processing, Categories of Personal Data, Data Subjects

The parties agree that the purpose and nature of the processing of Customer Personal Data, the types of personal data and categories of data subjects are as set out in this Appendix 2.

Purposes and Nature of Processing	Reprise may process Customer Personal Data as necessary to technically perform the Services, including where applicable: Hosting and storage; Backup and disaster recovery; Technically improve the service; Service change management; Issue resolution; Providing secure, encrypted Services; Applying new product or system versions, patches, updates and upgrades; Monitoring and testing system use and performance; Proactively detect and remove bugs; IT security purposes including incident management; Maintenance and performance of technical support systems and IT infrastructure; Migration, implementation, configuration and performance testing; Making product recommendations; Providing customer support; transferring data, and Assisting with data subject requests (as necessary).

Categories of Personal data	The Customer may submit Customer Personal Data to the Services, and may request for the Customer's respondents to submit personal data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation: Personal data of all types that may be submitted by the Customer's respondents to the Customer via users of the Services (such as via surveys or other feedback tools). For example: name, geographic location, age, contact details, IP address, profession, gender, financial status, personal preferences, personal shopping or consumer habits, and other preferences and other personal details that the Customer solicits or desires to collect from its respondents. Personal data of all types that may be included in forms hosted on the Services for the Customer (such as may be included in form questions). The Customer's respondents may submit special categories of personal data to the Customer via the Services, the extent of which is determined and controlled by the Customer.
Data Subjects	Data subjects include: Natural persons who submit personal data to Reprise via use of the Services (including via forms hosted by Reprise on behalf of the Customer); Natural persons whose personal data may be submitted to the Customer by Respondents via use of the Services; Natural persons who are employees, representatives, or other business contacts of the Customer; The Customer's users who are authorized by the Customer to access and use the Services.

Appendix 3

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least seven (7) business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Articles 33, 36 to 38 Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.