DATA PROCESSING AGREEMENT FOR CLOUD SERVICES

1. DEFINITIONS

1.1. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to RELISH be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

1.2. "**Data Protection Law**" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.3. "**Data Subject**" means an identified or identifiable natural person as defined by Data Protection Law.

1.4. "**EEA**" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

1.5. "**GDPR**" means the General Data Protection Regulation 2016/679.

1.6. "**Relish Website**" means information available on the RELISH support portal (see: www.relishiq.com)

1.7. "**New SCC Relevant Transfer**" means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the New Standard Contractual Clauses.

1.8. "**New Standard Contractual Clauses**" means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.

1.9. "**Personal Data**" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:

a) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service; or

b) supplied to or accessed by RELISH or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

1.10. "**Personal Data Breach**" means a confirmed:

a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or

b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.11. "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

1.12. "**Schedule**" means the numbered Appendix with respect to the Standard Contractual Clauses (2010) and the numbered Annex with respect to the New Standard Contractual Clauses.

1.13. "**Standard Contractual Clauses (2010)**" means the Standard Contractual Clauses (processors) published by the European Commission, reference 2010/87/EU.

1.14. "**Subprocessor**" or "**sub-processor**" means RELISH Affiliates and third parties engaged by RELISH, or RELISH's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

1.15. "**Technical and Organizational Measures**" means the technical and organizational measures for the relevant

Cloud Service included in the Schedule II of this document.

1.16. "**Third Country**" means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Purpose and Application

2.1.1. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between RELISH and Customer.

2.1.2. This DPA applies to Personal Data processed by RELISH and its Subprocessors in connection with its provision of the Cloud Service.

2.1.3. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by RELISH. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects (Schedule 1) and the applicable Technical and Organizational Measures (Schedule 2).

2.3. Governance

2.3.1. RELISH acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA.

2.3.2. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use RELISH as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where RELISH informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Applicability of the Technical and Organizational Measures

RELISH has implemented and will apply the Technical and Organizational Measures. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

3.2. Changes

3.2.1. RELISH applies the Technical and Organizational Measures to RELISH's entire customer base hosted out of the same data center or receiving the same Cloud Service. RELISH may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3.2.2. RELISH will publish updated versions of the Technical and Organizational Measures on Relish Website and where available Customer may subscribe to receive e-mail notification of such updated versions.

4. RELISH OBLIGATIONS

4.1. Instructions from Customer

RELISH will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. RELISH will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or RELISH otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, RELISH will immediately notify Customer (email permitted).

4.2. Processing on Legal Requirement

RELISH may also process Personal Data where required to do so by applicable law. In such a case, RELISH shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, RELISH and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. RELISH and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Cooperation

4.4.1. At Customer's request, RELISH will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding RELISH's processing of Personal Data or any Personal Data Breach.

4.4.2. If RELISH receives a request from a Data Subject in relation to the Personal Data processing hereunder, RELISH will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

4.4.3. In the event of a dispute with a Data Subject as it relates to RELISH's processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably co-operate with the aim of resolving the dispute amicably with the Data Subject.

4.4.4. RELISH shall provide functionality for production systems that supports Customer's ability to correct, delete or anonymize Personal Data from a Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, RELISH will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. Personal Data Breach Notification

RELISH will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. RELISH may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by RELISH.

4.6. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, RELISH will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, Audit Reports and Certifications). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case RELISH and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, Customer may use RELISH's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs RELISH to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer or its independent third-party auditor reasonably acceptable to RELISH (which shall not include any third party auditors who are either a competitor of RELISH or not suitably qualified or independent) may audit RELISH's control environment and security practices relevant to Personal Data processed by RELISH only if:

a) RELISH has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third-party auditor or RELISH;

b) a Personal Data Breach has occurred;

c) an audit is formally requested by Customer's data protection authority; or

d) provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits, unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by RELISH on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to RELISH.

6.4. Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by RELISH of this DPA, then RELISH shall bear its own expenses of an audit. If an audit determines that RELISH has breached its obligations under the DPA, RELISH will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

RELISH is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

a) RELISH on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. RELISH shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

b) RELISH will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

c) RELISH's list of Subprocessors in place on the effective date of the Agreement is published by RELISH on the Relish Website or RELISH will make it available to Customer upon request, including the name, address and role of each Subprocessor RELISH uses to provide the Cloud Service.

7.2. New Subprocessors

RELISH's use of Subprocessors is at its discretion, provided that:

a) RELISH will inform Customer in advance (by email or by posting on the Relish Website) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to RELISH. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of RELISH's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this 30-day period, Customer is deemed to have accepted the new Subprocessor.

7.3.2. Within the 30-day period from the date of RELISH's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for termination and do not affect RELISH's right to use the new Subprocessor(s) after the 30-day period.

7.3.3. Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4. Emergency Replacement

RELISH may replace a Subprocessor without advance notice where the reason for the change is outside of RELISH's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, RELISH will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 applies accordingly.

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

RELISH shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2. Applicability of the Standard Contractual Clauses (2010)

8.2.1. Where, for the period up to and including 26 September 2021, Personal Data of a Controller that is subject to GDPR is processed in a Third Country, or where Personal Data of a Swiss or United Kingdom based Controller or another Controller is processed in a Third Country and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses (2010), then:

a) RELISH and Customer enter into the Standard Contractual Clauses (2010);

b) Customer joins the Standard Contractual Clauses (2010) entered into by RELISH and the Subprocessor as an independent owner of rights and obligations; or

c) other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses (2010) with RELISH or the relevant Subprocessors in the same manner as Customer in accordance with Section 8.2.1 a) and b) above. In such case, Customer will enter into the Standard Contractual Clauses (2010) on behalf of the other Controllers.

8.2.2. The Standard Contractual Clauses (2010) shall be governed by the law of the country in which the relevant Controller is established.

8.2.3. Where applicable Data Protection Law adopts the New Standard Contractual Clauses as meeting any required adequacy means as an alternative or update to the Standard Contractual Clauses (2010) then the New Standard Contractual Clauses shall apply in accordance with Section 8.3.

8.3. Applicability of New Standard Contractual Clauses

8.3.1. The following shall apply with effect from 27 September 2021 and shall solely apply in respect of New SCC Relevant Transfers:

8.3.1.1. Where RELISH is not located in a Third Country and acts as a data exporter, RELISH has entered in to the New Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the New Standard Contractual Clauses shall apply to such New SCC Relevant Transfers.

8.3.1.2. Where RELISH is located in a Third Country:

RELISH and Customer hereby enter into the New Standard Contractual Clauses with Customer as the data exporter and RELISH as the data importer which shall apply as follows:

a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and

b) Module 3 (Processor to Processor) shall apply where Customer is a Processor. Where Customer acts as Processor under Module 3 (Processor to Processor) of the New Standard Contractual Clauses, RELISH acknowledges that Customer acts as Processor under the instructions of its Controller(s).

8.3.2. Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the New Standard Contractual Clauses with RELISH in the same manner as Customer in accordance with Section 8.3.1.2 above. In such case, Customer enters into the New Standard Contractual Clauses on behalf of the other Controllers or Processors.

8.3.3. With respect to a New SCC Relevant Transfer, on request from a Data Subject to the Customer, Customer may make a copy of Module 2 or 3 of the New Standard Contractual Clauses entered into between Customer and RELISH (including the relevant Schedules), available to Data Subjects.

8.3.4. The governing law of the New Standard Contractual Clauses shall be the law of Germany.

8.4. Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses (2010) or the New Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the Standard Contractual Clauses (2010) and the New Standard Contractual Clauses.

8.5. Third Party Beneficiary Right under the New Standard Contractual Clauses

8.5.1. Where Customer is located in a Third Country and acting as a data importer under Module 2 or Module 3 of

the New Standard Contractual Clauses and RELISH is acting as Customer's sub-processor under the applicable Module, the respective data exporter shall have the following third-party beneficiary right:

8.5.2. In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Cloud Service soley to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs RELISH to erase or return the Personal Data.

9. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

1. A. LIST OF PARTIES

1.1. Under the Standard Contractual Clauses (2010)

1.1.1. Data Exporter

The data exporter under the Standard Contractual Clauses (2010) is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also data exporters.

1.1.2. Data Importer

RELISH and its Subprocessors that provide and support the Cloud Service are data importers under the Standard Contractual Clauses (2010).

1.2. Under the New Standard Contractual Clauses

1.2.1. Module 2: Transfer Controller to Processor

Where RELISH is located in a Third Country, Customer is the Controller and RELISH is the Processor, then Customer is the data exporter and RELISH is the data importer.

1.2.2. Module 3: Transfer Processor to Processor

Where RELISH is located in a Third Country, Customer is a Processor and RELISH is a Processor, then Customer is the data exporter and RELISH is the data importer.

2. B. DESCRIPTION OF TRANSFER

2.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

2.2. Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

2.3. Special Data Categories (if agreed)

2.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("**Sensitive Data**"). RELISH has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.

2.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

a) training of personnel;

b) encryption of data in transit and at rest;

c) system access logging and general data access logging.

2.3.3. In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

2.4. Purposes of the data transfer and further processing; Nature of the processing

2.4.1. The transferred Personal Data is subject to the following basic processing activities:

a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support);
b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
c) provision of embedded Professional Services;
d) communication to Authorized Users;
e) storage of Personal Data in dedicated data centers (multi-tenant architecture);
f) release, development and upload of any fixes or upgrades to the Cloud Service;
g) back up and restoration of Personal Data stored in the Cloud Service;
h) computer processing of Personal Data, including data transmission, data retrieval, data access;
i) network access to allow Personal Data transfer;
j) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;
k) security monitoring, network-based intrusion detection support, penetration testing; and
l) execution of instructions of Customer in accordance with the Agreement.

2.4.2. The purpose of the transfer is to provide and support the Cloud Service. RELISH and its Subprocessors may support the Cloud Service data centers remotely. RELISH and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

2.5. Additional description in respect of the New Standard Contractual Clauses:

2.5.1. Applicable Modules of the New Standard Contractual Clauses

a) Module 2: Transfer Controller to Processor
b) Module 3: Transfer Processor to Processor

2.5.2. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

In respect of the New Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

2.5.3. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous

basis). Transfers shall be made on a continuous basis.

2.5.4. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Personal Data shall be retained for the duration of the Agreement and subject to Section 5.2 of the DPA.

3. C. COMPETENT SUPERVISORY AUTHORITY

3.1. In respect of the New Standard Contractual Clauses:

3.1.1. Module 2: Transfer Controller to Processor

3.1.2. Module 3: Transfer Processor to Processor

3.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the New Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures (TOMs) for RELISH Cloud Services

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

To the extent that the provisioning of the Cloud Service comprises New SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

The following sections define RELISH's current technical and organizational measures and are incorporated into Schedule 2 of the DPA. RELISH may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. PHYSICAL ACCESS CONTROL

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process or use Personal Data are located.

1.1. Measures

1.1.1. RELISH and its sub processors protect its assets and facilities using the appropriate means based on the RELISH Security Policy and RELISH Physical Security Standard

1.1.2. In general, buildings are secured through access control systems (e.g., badge readers, PIN code or traditional keys).

1.1.3. Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.

1.1.4. Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see below). This also applies to visitor access. Guests and visitors to RELISH buildings must register their names at reception and must be accompanied by authorized RELISH personnel.

1.1.5. RELISH employees and external personnel must wear their ID cards at all RELISH locations.

1.2. Additional measures for data centers

1.2.1. All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

1.2.2. RELISH and all third-party data center providers log the names and times of authorized personnel entering RELISH's private areas within the data centers.

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the Cloud Service must be prevented from being used without authorization by taking the following measures:

2.1. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the RELISH Security Policy

2.2. All personnel access RELISH's systems with a unique identifier (user ID).

2.3. RELISH has procedures in place so that requested authorization changes are implemented only in accordance with

the RELISH Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.

2.4. RELISH has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

2.5. The company network is protected from the public network by firewalls.

2.6. RELISH uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

2.7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to RELISH's corporate network and critical infrastructure is protected by strong authentication.

3. DATA ACCESS CONTROL

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage. RELISH takes the following measures:

3.1. As part of the RELISH Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the RELISH Information Classification standard.

3.2. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. RELISH uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the RELISH Security Policy.

3.3. All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, RELISH conducts internal and external security checks and penetration tests on its IT systems.

3.4. RELISH does not allow the installation of software that has not been approved by RELISH.

4. DATA TRANSMISSION CONTROL

Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at RELISH to provide the agreed-upon service levels (specifically, encryption). RELISH takes the following measures:

4.1. Personal Data in transfer over RELISH internal networks is protected according to RELISH Security Policy.

4.2. When data is transferred between RELISH and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of RELISH-controlled systems (e.g. data being transmitted outside the firewall of the RELISH data center).

5. DATA INPUT CONTROL

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from RELISH data processing systems. RELISH takes the following measures: RELISH only allows authorized personnel to access Personal Data as required in the course of their duty.

RELISH has implemented a logging system for input, modification and deletion, or blocking of Personal Data by RELISH or its Subprocessors within the Cloud Service to the extent technically possible.

6. JOB CONTROL

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer. RELISH takes the following measures:

6.1. RELISH uses controls and processes to monitor compliance with contracts between RELISH and its customers, subprocessors or other service providers.

6.2. As part of the RELISH Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the RELISH Information Classification standard.

6.3. All RELISH employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of RELISH customers and partners.

7. AVAILABILITY CONTROL

Personal Data will be protected against accidental or unauthorized destruction or loss. RELISH employs regular backup processes to provide restoration of business-critical systems as and when necessary. RELISH takes the following measures:

7.1. RELISH uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the data centers.

7.2. RELISH has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.

7.3. Emergency processes and systems are regularly tested.

8. DATA SEPARATION CONTROL

Personal Data collected for different purposes can be processed separately. RELISH takes the following measures:

8.1. RELISH uses the technical capabilities of the deployed software (for example: multi- tenancy, or partition keys) to achieve data separation among Personal Data originating from multiple customers.

8.2. Customer (including its Controllers) has access only to its own data.

8.3. If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

9. DATA INTEGRITY CONTROL

Personal Data will remain intact, complete and current during processing activities. RELISH takes the following measures:

9.1. RELISH has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

9.2. In particular, RELISH uses the following to implement the control and measure sections described above:

9.3. Firewalls and Security Monitoring Center;

9.4. Antivirus software;

9.5. Backup and recovery;

9.6. External and internal penetration testing;

9.7. Regular external audits to prove security measures.