PERSONAL DATA PROCESSING AGREEMENT FOR RELISH CLOUD SERVICES

1. BACKGROUND

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between RELISH and Customer. This DPA applies to Personal Data processed by RELISH and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by RELISH, and Customer shall not store Personal Data in such environments.

1.2 Structure. Appendices 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 and the applicable technical and organizational measures.

1.3 GDPR. RELISH and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 Governance. RELISH acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA, and as a Service Provider under the California Consumer Privacy Act and its successors (CCPA, CPRA). Customer acts as a single point of contact and is solely responsible for obtaining 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 and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

2. SECURITY OF PROCESSING

2.1 Appropriate Technical and Organizational Measures. RELISH has implemented and will apply appropriate measures, including the technical and organizational measures set forth in Appendix 2. 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.

2.2 Changes. RELISH applies the technical and organizational measures set forth in Appendix 2 to RELISH's entire customer base receiving the same Cloud Service. RELISH may change the measures set out in Appendix 2 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. RELISH OBLIGATIONS

3.1 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).

3.2 **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.

3.3 **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.

3.4 **Cooperation.** 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. RELISH shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. RELISH shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, RELISH will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.5 **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.

3.6 **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 or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1 **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.

4.2 **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 six months) unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

5.1 **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 and/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) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits.

5.2 Other Controller Audit. Any other Controller may audit RELISH's control environment and security practices relevant to Personal Data processed by RELISH in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 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.

5.3 Scope of Audit. Customer shall provide at least sixty 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 three 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.

5.4 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.

6. SUBPROCESSORS

6.1 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 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.

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

(a) RELISH will inform Customer in advance (by email and by posting on the support portal available through RELISH Support) 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 6.3.

6.3 Objections to New Subprocessors.

(a) 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 thirty days from the date of RELISH's notice to Customer

informing Customer of the new Subprocessor. If Customer does not terminate within this thirty-day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty-day period from the date of RELISH's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss 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 thirty day period.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 **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 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 **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.

7.2 **Standard Contractual Clauses.** Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally 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, then:

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

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by RELISH and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by RELISH) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when RELISH has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/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 with RELISH and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 **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. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 **Governing Law of the Standard Contractual Clauses.** The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. 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.

9. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

9.1 **"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.

9.2 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, or notified to Customer or otherwise agreed in an Order Form.

9.3 **"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 (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by RELISH on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not and the laws of other countries as applicable.).

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

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

9.6 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

9.7 **"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 (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) 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).

9.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) 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.

9.9 **"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.

9.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).

9.11 **"Subprocessor"** means RELISH Affiliates and third parties engaged by RELISH in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter
The Data Exporter 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.

Data Importer
RELISH and its Subprocessors provide the Cloud Service that includes the following support:

RELISH affiliates support the Cloud Service remotely from RELISH facilities and other locations where RELISH employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

RELISH Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. RELISH answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

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.

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, time zone, 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.

Special Data Categories (if appropriate)
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes
The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):

- **TOMs Set 1:** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.

- **TOMs Set 2**: applies to the TOMs Set 2 Services only. RELISH may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.

TOMs SET 1

Last Updated: November 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define RELISH's current technical and organizational measures. 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.

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

Measures:

- RELISH protects its assets and facilities using the appropriate means based on the RELISH Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- 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.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 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.
- RELISH employees and external personnel must wear their ID cards at all RELISH locations.

Additional measures for Data Centers:

- 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.
- 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.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- 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
- All personnel access RELISH's systems with a unique identifier (user ID).
- 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.
- 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.
- The company network is protected from the public network by firewalls.
- 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.
- 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.

1.3 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.

Measures:

- 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.
- 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.
- 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.
- RELISH does not allow the installation of software that has not been approved by RELISH.
- An RELISH security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 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 (for example, encryption and lead-lined containers).

Measures:

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

- 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).

1.5 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. 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.

1.6 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.

Measures:

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

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- RELISH employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- RELISH uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- 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.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- RELISH uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- 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.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

- RELISH has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, RELISH uses the following to implement the control and measure sections described above:
- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

TOMs SET 2

(*applies to TOMs Set 2 Services defined above*)

Last Updated: November, 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define RELISH's current technical and organizational measures. 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.

1.1 Physical Access Control.

- RELISH protects its assets and facilities using the appropriate means based on the RELISH Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- 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.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 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.
- RELISH employees and external personnel must wear their ID cards at all RELISH locations.

Additional measures for Data Centers:

- 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.
- 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.

1.2 System Access Control.

- 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.
- All personnel access RELISH's systems with a unique identifier (user ID).
- RELISH has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked.
- 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.
- The company network is protected from the public network by firewalls.

- 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.
- Security patch management processes to deploy relevant security updates on a regular and periodic basis.
- Full remote access to RELISH's corporate network and critical infrastructure is protected by authentication.

1.3 Data Access Control.

- 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.
- 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.
- 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/or penetration tests on its IT systems.
- Processes and policies to detect the installation of unapproved software on production systems.
- An RELISH security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

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

1.5 Data Input Control.

- RELISH only allows authorized personnel to access Personal Data as required in the course of their duty.
- RELISH has in most cases 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.

1.6 Job Control.

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

1.7 Availability Control.

- RELISH employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- RELISH uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- 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.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

- RELISH uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- 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.

1.9 Data Integrity Control.

- RELISH has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
- In particular, RELISH uses the following to implement the control and measure sections described above.
- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing and/or regular external audits to prove security measures.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPR	**Section of DPA**	**Click on link to see Section**
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data protection Impact Assessment.
28(3) (g)	4	Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses