teridion

Teridion – Customer Data Processing Addendum

This Data Processing Addendum ("DPA") forms an integral part of the Agreement ("Main Agreement") between Teridion Technologies Ltd. ("Teridion") and between the counterparty listed in the Main Agreement ("Customer"; each a "Party" and together "Parties") and applies to the extent that Teridion processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Main Agreement.

All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement.

1. Definitions

1.1. **"Approved Jurisdiction"** means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

or by the UK Information Commissioner's Office ("ICO"), where applicable.

1.2. **"Data Protection Law"** means any and all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the UK Privacy and Electronic Communications Regulations 2003 (PCER), the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), the Data Protection Act 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR").

1.3. **"Data Subject"** means an individual to whom Personal Data relates.

1.4. **"EEA"** means those countries that are member of the European Economic Area.

1.5. **"Permitted Purposes"** mean any purposes in connection with Teridion performing its obligations under the Main Agreement.

1.6. **"Security Incident"** shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the avoidance of doubt, any Personal Data Breach (as defined under the GDPR) will comprise a Security Incident.

1.7. **"Security Measures"** mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Teridion's business, the level of sensitivity of the data collected, handled and stored, and the nature of Teridion's business activities.

1.8. **"Standard Contractual Clauses"** mean Module Two or Module Three, as applicable, of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4th 2021.

1.9. **"Sub-Processor(S)"** mean any Affiliate, agent or assignee of Teridion that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by Teridion.

1.10. **"UK Addendum"** means the International Data Transfer Addendum to the Standard Contractual Clauses, as issued by the ICO under S119A(1) of Data Protection Act 2018.

1.11. The terms **"Controller"**, **"Personal Data"**, **"Processor"**, **"Process"**, and **"Processing"** shall have the meanings ascribed to them in the Data Protection Law, as applicable.

2. Application Of This DPA

2.1. This DPA will only apply to the extent all of the following conditions are met:

a. Teridion processes Personal Data that is made available by the Customer in connection with the Main Agreement; and

b. The Data Protection Law apply to the processing of Personal Data.

2.2. This DPA will only apply to the services for which the Parties agreed to in the Main Agreement ("Services"), which incorporates the DPA by reference.

3. Parties' Roles

3.1. in respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller or Processor and Teridion is a Processor or Sub-Processor, and accordingly:

a. Teridion agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;

b. The Parties acknowledge that the Customer discloses Personal Data to Teridion only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2. If Customer is a Processor, Customer warrants to Teridion that Customer's instructions and actions with respect to the Personal Data, including its appointment of Teridion as another Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant Controller.

3.3. This DPA shall not apply to Personal Data that is processed by Teridion in its capacity as an independent controller, as this term is defined in the GDPR, which includes, without limitation, processing for the administration of the contractual relationship with the Customer, billing, recordkeeping, protection against fraudulent activity, compliance with legal obligations and defense of legal claims.

4. Compliance With Laws

4.1. Each Party shall comply with its respective obligations under the Data Protection Law.

4.2. Teridion shall provide reasonable cooperation and assistance to Customer in relation to Teridion's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.

4.3. Teridion agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.

4.4. Throughout the duration of the DPA, Customer represents and warrants that:

a. Personal Data has been and will continue to be collected, processed and transferred by Customer in accordance with the relevant provisions of Data Protection Law;

b. Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Teridion and shall provide Teridion only instructions that are lawful under Data Protection Law;

c. The processing of Personal Data by Teridion for the Permitted Purposes, as well as any instructions to Teridion in connection with the processing of the Personal Data ("Processing Instructions"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and

d. Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained the relevant consents or lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions and the Permitted Purposes).

5. Processing Purpose And Instructions

5.1. The subject matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, shall be as set out in the Agreement, or in the attached Annex 1, which is incorporated herein by reference.

5.2. Teridion shall process Personal Data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Agreement and the Data Protection Law, unless Teridion is otherwise required to do so by law to which it is subject (and in such a case, Teridion shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

5.3. To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between Teridion and Customer, which may include any additional fees that may be payable by Customer to Teridion for carrying out such Processing Instructions. Teridion shall immediately inform Customer if, in Teridion's opinion, an instruction is in violation of Data Protection Law.

5.4. Additional instructions of the Customer outside the scope of the Agreement require prior and separate agreement between Customer and Teridion, including agreement on additional fees (if any) payable to Teridion for executing such instructions.

6. Reasonable Security And Safeguards

6.1. Teridion represents, warrants, and agrees to use Security Measures, in a manner which enables Teridion to comply with Data Protection Law, including by implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data

(i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed or processed by Teridion in connection with this Agreement, and

(ii) to protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2.

6.2. The Security Measures are subject to technical progress and development and Teridion may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the services procured by Customer.

6.3. Teridion shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who has access to and processes Personal Data. Teridion shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Security Incidents

7.1. Upon becoming aware of a Security Incident, Teridion will notify Customer without undue delay and will provide information relating to the Security Incident as reasonably available and requested by Customer. Teridion will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Security Incident.

8. Security Assessments And Audits

8.1. Teridion audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Teridion's internal audit team or by third party auditors engaged by Teridion, and will result in the generation of an audit report ("**Report**"), which will be Teridion's confidential information.

8.2. Teridion shall, upon reasonable and written notice of at least thirty (30) days and subject to obligations of confidentiality, no more than once a year (unless otherwise required by Data Protection Law) and in normal business hours, allow its data processing procedures and documentation to be inspected by Customer (or its designee), at Customer's expense, in order to ascertain compliance with this DPA; Teridion shall cooperate in good faith with such audit requests by providing access to relevant knowledgeable personnel and documentation.

8.3. At Customer's written request, and subject to obligations of confidentiality, Teridion may satisfy the requirements set out in this section by providing Customer with a copy of the Report so that Customer can reasonably verify Teridion's compliance with its obligations under this DPA.

9. Cooperation And Assistance

9.1. If Teridion receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under applicable Data Protection Law, Teridion will promptly redirect the request to Customer. Teridion will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Teridion is required to respond to such a request, Teridion will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so. The Customer is responsible for verifying that the requestor is the data subject whose information is being sought. Teridion bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2. If Teridion receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Teridion shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Teridion shall be entitled to provide such information.

9.3. Notwithstanding the foregoing, Teridion will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by Teridion in connection with its provision of such assistance.

9.4. Upon reasonable notice, Teridion shall:

a. taking into account the nature of the processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;

b. provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails material costs or expenses to Teridion, the Parties shall first come to agreement on Customer reimbursing Teridion for such costs and expenses.

10. Use Of Sub-Processors

10.1. Customer provides a general authorization to Teridion to appoint (and permit each Sub-Processor appointed in accordance with this Clause to appoint) Processors and/or Sub Processors in accordance with this Clause.

10.2. Teridion may continue to use those Processors and/or Sub Processors already engaged by Teridion as at the date of this Agreement, as set forth in Annex 3, subject to Teridion, in each case as soon as practicable, meeting the obligations set out in this Clause.

10.3. Teridion can at any time appoint a new Processor and/or Sub-Processor provided that Customer is given ten (10) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law. If, in Teridion's reasonable opinion, such objections are legitimate, Teridion shall either refrain from using such Processor and/or Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Processor and/or Sub-Processor. Where Teridion notifies Customer of its intention to continue to use the Processor and/or Sub Processor in these circumstances, Customer may, by providing written notice to Teridion, terminate the Agreement immediately.

10.4. With respect to each Processor and/or sub-processor, Teridion shall ensure that the arrangement between Teridion and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this Agreement and meet the requirements of article 28(3) of the GDPR.

10.5. Teridion will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Teridion to breach any of its obligations under this DPA.

10.6. Teridion will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Teridion's behalf. Teridion does not sell or disclose Personal Data to third parties for commercial purposes, except as required under applicable laws.

11. Transfer Of EEA Resident Personal Data Outside The EEA

11.1. Teridion may transfer Personal Data of residents of the EEA or the UK outside the EEA or the UK ("**Transfer**"), only subject to the following:

a. the Transfer is necessary for the purpose of Teridion carrying out its obligations under the Agreement, or is required under applicable laws; and

b. the Transfer is done:

(i) to an Approved Jurisdiction, or

(ii) subject to appropriate safeguards (for example, through the use of the Standard Contractual Clauses, or other applicable frameworks), or

(iii) in accordance with any of the exceptions listed in the Data Protection Law (in which event Customer will inform Teridion which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies).

11.2. If the transfer of Personal Data is subject to the GDPR and Teridion processes Personal Data outside the EEA or an Approved Jurisdiction, then the Parties shall be deemed to enter into the Standard Contractual Clauses, which are incorporated into this DPA by reference, subject to any amendments contained in Exhibit A, in which event the Customer shall be deemed as the Data Exporter and Teridion shall be deemed as the Data Importer (as these terms are defined therein).

11.3. If the transfer of Personal Data is subject to the UK GDPR and Teridion processes Personal Data outside the UK or an Approved Jurisdiction, then the Parties shall be deemed to enter into the Standard Contractual Clauses, which are incorporated into this DPA by reference, subject to the UK Addendum and any amendments contained in Exhibit A, in which event the Customer shall be deemed as the Data Exporter and Teridion shall be deemed as the Data Importer (as these terms are defined therein).

11.4. If the Standard Contractual Clauses or the UK Addendum (where applicable) are superseded by a new or modified legal mechanism for transfers of Personal Data, the new or modified legal mechanism for transfers of Personal Data shall be deemed to be incorporated into this DPA, and the Parties will promptly begin complying with such legal mechanism for transfers of Personal Data.

12. Data Retention And Destruction

12.1. Teridion will only retain Personal Data for the duration of the Agreement or as required to perform its obligations under the Agreement, or has otherwise required to do so under applicable laws or regulations. Following expiration or termination of the Agreement, Teridion will delete or return to Customer all Personal Data in its possession as provided in the Agreement, except to the extent Teridion is required under applicable laws to retain the Personal Data. The terms of this DPA will continue to apply to such Personal Data. This section shall not apply to the activities that are the subject matter of section 3.1 herein. Teridion shall be entitled to retain Personal Data solely for compliance with its legal obligations and the establishment or exercise of legal claims. Notwithstanding the foregoing, Teridion shall be entitled to maintain Personal Data following the termination of this Agreement for other internal purposes, including but not limited to statistical and/or financial purposes, provided always that Teridion maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.

13. General

13.1. Any claims brought under this DPA will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

13.2. In the event of a conflict between the Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

Exhibit A – Standard Contractual Clauses Stipulations

1. This Exhibit A sets out the Parties' agreed interpretation of their respective obligations under Module Two or Module Three of the Standard Contractual Clauses (as applicable), and the UK Addendum (where applicable).

2. Where the transfer of Personal Data is subject to the GDPR and the transfer relies on the Standard Contractual Clauses, the following amendments shall apply to the Standard Contractual Clauses:

2.1. If Customer is a controller – the Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module Two); if Customer is a processor – the Parties shall be deemed to enter into the Processor to Processor Standard Contractual Clauses (Module Three).

2.2. The Parties agree that for the purpose of transfer of Personal Data between the Customer (Data Exporter) and Teridion (Data Importer), the following shall apply:

a. Clause 7 shall not be applicable.

b. In Clause 9, option 2 shall apply. Teridion shall inform Customer of any intended addition or replacement of Sub Processors at ten (10) days in advance.

c. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

d. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the laws of the Republic of Ireland.

e. In Clause 18(b) the Parties choose the courts of Dublin Ireland, as their choice of forum.

f. Annexes 1–3 below are incorporated into the Standard Contractual Clauses by reference.

3. Where the transfer of Personal Data is subject to the UK GDPR and the transfer relies on the UK Addendum, the following shall apply:

3.1. In Table 1 the "Exporter" is Customer; the "Importer" is Teridion; and the Parties details and signatures are included in this DPA and the Main Agreement;

3.2. In Table 2, the first option is selected and the "Approved EU SCCs" are those Standard Contractual Clauses incorporated into this DPA;

3.3. In Table 3, "Annex 1A, 1B, 2 and 3 to the Approved EU SCCs" are Annexes 1, 2 and 3 to the DPA; and

3.4. In Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum in accordance with section 19 of the UK Addendum.

Annex 1 - Description Of The Processing Activities

A. Identification of Parties

"Data Exporter": Customer;

"Data Importer": Teridion.

B. Description of Transfer

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

- Customer's end-users
- Customer's employees
- Customer's customers

Categories of Personal Data

The Personal Data transferred concern the following categories of data:

- Contact information (name, age, gender, address, telephone number, email address etc.)
- Device identifiers and internet or electronic network activity (IP addresses)

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

- None.

The frequency of the transfer

- Continuous

Nature of the processing

- Collection
- Adaptation or alteration
- Analysis

Purpose of the transfer and further processing

As defined in the Agreement.

Retention period

Personal Data will be retained for the term of the Agreement.

The competent supervisory authority will be in accordance with the provisions of Clause 13 of the Standard Contractual Clauses.

Annex 2 – Technical And Organizational Measures To Ensure The Security Of The Data

This Annex forms part of the DPA and describes the technical and organizational security measures implemented by the data importer.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Teridion shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Additional and specific security measures are described below.

Introduction

This Annex 2 outlines the technical and organizational measures for safeguarding Personal Data undertaken by Teridion, in support of our global security framework. We take a systematic approach of data protection, privacy, and security. We believe a robust security and privacy program requires active involvement of stakeholders, ongoing education, internal and external assessments and installment and enforcement of best practices within the organization. We hold a SOC-II Type 2 certification.

Organizational And Personal Management

- We have appointed an information security officer who designs, develops, and deploys our technical architectures, security policies, standards, and awareness program along with our IT teams.
- We have appointed a Data Privacy Officer who oversees our privacy program.
- Our Annual Risk Assessment includes an Information Security Audit, owned, operated and maintained by the Security Officer. Its results are presented to the steering committee and afterwards to management during management security reviews.

Physical Security

- Teridion's servers are managed by Google Cloud Platform (GCP) and overseen by Teridion's team. GCP is widely regarded as employing highly protective and industry standard protective measures ensuring the security of physical servers managed by them, relied upon by thousands of technology providers around the world (more on GCP security measures can be found here -https://cloud.google.com/security).
- Teridion has implemented suitable measures in order to prevent unauthorized persons from gaining access to its resources equipment, regardless of whether those resources are directly related to where Personal Data are processed or used. These measures may include all or a combination of any of the following:
  1. Maintaining offices that are within facilities requiring registration for entry and accompaniment beyond the front entrance.
  2. Strict measures to ensure that all visitors are accompanied, and awareness among employees to challenge any exceptions.
  3. Restricted access to areas including any communications or other technological equipment on an employee role basis.
  4. A high security card key system is utilized to control facility access.

HR Security

- Teridion personnel are trained and briefed about contractual obligations undertaken by Teridion towards its clients with respect to data security, and their compliance therewith is monitored by company's management.
- All Teridion employees and contractors are required to sign confidentiality agreements ("NDA") that apply during their engagement with Teridion and post termination.
- New employees go through an on-boarding process that includes security guidelines, expectations, and code of conduct. All Teridion's employees undergo annual security awareness training.
- The Security Officer communicates with all employees on a regular basis, covering topics such as emerging threats, phishing awareness campaigns, and other industry-related security topics.
- A formal and communicated disciplinary process is in place against employees who have committed an information security breach.

Third Party Security

- Third Party used by Teridion are checked by 3rd party questionnaires and a certification review prior to engagement to validate that prospective third parties meet Teridion's security standards.
- The procedure takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

Logical Access Control

- Access to our servers is managed by personal password-protected user accounts.
- MFA is enforced while accessing to our production environment
- All users access the Teridion systems with a unique identifier and must authenticate via Teridion's SSO (Single Sign On) platform.
- We have established a password policy that prohibits the sharing of passwords. All passwords must fulfill defined minimum requirements and are stored in encrypted form.
- Automatic lock out of the user ID when several erroneous passwords are entered.
- Automatic time-out of the user terminal if left idle; identification and password required to reopen.
- Role-based access controls implemented in a manner consistent with the principle of least privilege.
- Granting of access according to a strict formal procedure and periodic review of the access.
- Employees' access to production systems that contain personal data is logged, audited and reviewed on a regular basis.

Monitoring And Control

- We utilize a wide range of tools to monitor our environment across data centers on both the server and application level and are continuously reviewed for anomalies by our 24x7 NOC team.
- We use third party tools to assess, audit, and evaluate the configurations of our cloud resources.

Security In Development And Support Process

- We use an industry-standard security model in our platform development process.
- We design, review and test our platform using applicable OWASP Top 10 standards.
- Our developers and project team members receive training at least once a year in application security while focusing on secure software development.
- Our production environment is segregated from our development and staging environments with restricted access controls.
- Periodic penetration testing are carried out by rotating third party companies at least annually.

Privacy By Design

- We incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

Workstation And Laptop Protection

- We use up-to-date Anti-Malware / Anti Virus software on all appropriate laptops.
- We use a security management solution that enables scalable and centralized management of multiple endpoints.

Change Management

- We follow a strict change management process.
- Changes are tracked, reviewed and approved to ensure operational changes are aligned with our business objectives and compliance requirements.

Account Segregation

- Our solution is a multi-tenant service, meaning, multiple customer network deployments data are stored in the same management system.
- We use logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while preventing customers from accessing one another's data.

Infrastructure & Amp; Network Security

- Remote access via SSL VPN using Two Factor Authentication.
- We review our network architecture schema and data flows, including firewall rules and access restrictions on a regular basis.
- Our WiFi internal corporate LAN is separated from guest Wi-Fi, encrypted by WPA2 – PSK and protected by a complex password.
- We establish a vulnerability and patch management process for our systems which includes technical vulnerability assessments, patch testing, patch deployment and verification.

Encryption

- **Data in Transit** - Any personal Data is encrypted during transmission using up to date versions of TLS (1.2 or higher).
- **Data in Rest** - Personal data is encrypted with AES256.

System Availability

- All Teridion data is stored on Google Cloud which is trusted by thousands of businesses to store and serve their data and services. As Teridion data is all stored on the cloud and nowhere on any proprietary physical servers, the risk of any local disaster affecting Teridion's ability to maintain business continuity or data completeness is low.
- We perform backups, which are tested regularly.
- Architecture which eliminates single points of failure, both with regards to Cloud based production and relevant Teridion critical supporting resources, up to and including full disaster recovery.
- We have sophisticated internal procedures including release control and approvals, following security best practices.
- We established a business continuity plan that enables the company to respond quickly and remain resilient in the event of most failure modes, including natural disasters and system failures.

Incident Response

- To ensure effective and orderly response to incidents pertaining to personal data, we defined an incident response plan with detailed procedures.
- The incident response plan includes a list of possible mitigation actions and clear assignment of roles.
- In the event of a security breach, Teridion will notify customers without undue delay after becoming aware of the security breach.

Documentation

- Emphasis is placed on documentation, to support the processes and procedures noted in this document and to enable audit should the need arise, in keeping with regulatory dictates and best practices.

Compliance

- Teridion conducts regular internal and external audits of its security, led by the Security officer.
- Teridion has appointed a Data Privacy Officer responsible for overseeing the implementation of the privacy program at Teridion.

Summary

- We are committed to confidentiality, data privacy and security of our customers and their end-users. We are investing and will continue to invest extensive resources towards maintaining the highest levels of data protection, privacy and security standards. We are compliant with applicable laws and regulations, and are committed to compliance with the GDPR's related guidelines.
- We cannot guarantee that your information may not be disclosed, accessed, altered or destroyed by breach of any of our industry standard safeguards. No method of transmission over the Internet or electronic storage is full-proof. We cannot guarantee absolute security.
- Our security measures are constantly evolving to keep up with the changing security landscape, so we may update these measures pages from time to time to reflect these technical and organizational changes. If any security measure changes in a manner detrimental to our customers' interests, we will notify our customers of such changes.

Annex 3 – List Of Sub-Processors

Below is the list of Teridion's Sub-Processors:

#	Name	Details
1	Google HQ	Address: 1600 Amphitheatre Parkway Mountain View, CA 94043, USA Contact details: tal@doit-intl.com (650) 253-0000 Description of Processing: Storage services