Exhibit C
Data Processing Agreement

This Data Processing Agreement (hereinafter "**DPA**") is an addendum to, and is hereby incorporated into, the Master SAAS Agreement, online Terms and Conditions, or other written subscription agreement, between the applicable Talon.One entity and Customer set forth therein (the "**Agreement**").

"Talon.One" and "Customer" refer to the respective entities as defined in the Order Form.

Preamble

(1) This DPA details the Parties' obligations on the protection of Personal Data, associated with the Processing of Personal Data on behalf of Customer, and described in detail in the applicable Order Form (hereinafter, the "Agreement"). This DPA shall apply to all activities associated with the Agreement to the extent Talon.One Processes Customer's Personal Data on behalf of Customer.

(2) For purposes of this DPA, Customer is the Controller and Talon.One is a Processor, except where Talon.One Processes Personal Data to carry out its Business Operations, in which case it acts as a Controller. Each Party is responsible for its own compliance with Applicable Data Protection Legislation.

(3) Any Processing of Personal Data subject to the UK GDPR will be governed by the UK DPA Addendum attached to this DPA. Any Processing of Personal Data subject to Applicable U.S. Data Protection Legislation will be governed by the U.S. DPA Addendum attached to this DPA. In the event of a conflict between this DPA and any Country-Specific DPA Addendum, the applicable Country-Specific DPA Addendum will prevail. In the event of any conflict between this DPA and any Country-Specific DPA Addendum, the applicable Country-Specific DPA Addendum shall prevail.

§ 1 Definitions

- **Applicable Data Protection Legislation** means the EU GDPR, the UK GDPR, the Applicable U.S. Data Protection Legislation and the Applicable Singaporean Data Protection Legislation.
- **Applicable U.S. Data Protection Legislation** means all U.S. state laws governing the protection and Processing of Personal Data, including but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act
- **Applicable Singaporean Data Protection Legislation** means the Singaporean Personal Data Protection Act 2012, as amended.
- **Business Operations** means such Personal Data Processing that Talon.One is authorized to carry out for its own internal purposes. This includes the generation and use of Usage Data in accordance with the Agreement.
- **Controller** shall have the meaning given to that term in the GDPR.
- **Commercial Purpose** shall have the meaning given to that term in the Applicable U.S. Data Protection Legislation.
- **Country-Specific DPA Addendum** means, as applicable, the UK DPA Addendum, or the U.S. DPA Addendum.
- **Data Subject** shall have the meaning given to that term in the GDPR.
- **Data Exporter** shall have the meaning given to that term in the GDPR.
- **Data Importer** shall have the meaning given to that term in the GDPR.
- **EU GDPR** means the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law.
- **GDPR** refers commonly to (i) the EU GDPR, and (ii) the UK GDPR.

- **International Data Transfer Addendum** or **IDTA** means the international data transfer addendum approved by the United Kingdom's parliament.
- **Personal Data** shall have the meaning given to that term in the GDPR.
- **Personal Data Breach** means a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
- **Processing, processes, processed, process** shall have the meaning given to that term in the GDPR.
- **Processor** shall have the meaning given to that term in the GDPR.
- **Standard Contractual Clauses** means the international data transfer addendum for data controller to data processor transfers approved by the European Commission in decision 2021/914 of June 4, 2021.
- **Sub-Processor** or further Processor shall have the meaning given to these terms in the GDPR.
- **UK Addendum** means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.
- **UK DPA 2018** means UK Data Protection Act 2018.
- **UK GDPR** has the meaning given to it in Section 3(10) (as supplemented by Section 205(4)) of the UK DPA 2018.
- **Usage Data** has the meaning given to it in the Agreement; if no so meaning exists, then it means anonymized and aggregated information or data, collected and owned by Talon.One, that a) tracks Customer's use of the Subscription Service, and b) tracks the performance of the Subscription Service.

§ 2 Scope of Application and Responsibilities

(1) Except for Business Operations, Talon.One shall Process Data on behalf of and as instructed by Customer. Within the scope of this DPA, Customer shall be solely responsible for compliance with the Applicable Data Protection Legislation with respect to the lawfulness of disclosing Personal Data to Talon.One and the lawfulness of having Personal Data Processed on behalf of Customer.

(2) Except where this DPA stipulates obligations beyond the term of the Agreement, the term of this DPA shall be the term of the Agreement.

(3) Customer's individual instructions on Processing shall, initially, be as detailed in the Agreement and/or this DPA. Customer may modify, amend, or replace such instructions by issuing written instructions to Talon.One's designated point of contact. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the Agreement. Customer shall, without undue delay, confirm in writing any instruction issued orally.

(4) The subject matter of the Processing shall include, but not be limited to, the following:

Type of Personal Data	Type and purpose (subject matter) of Processing	Categories of Data Subjects affected
Customer's master data (especially name, address, email address, phone number)	Automated processing of promotional and/or loyalty activities (e.g. creation of coupon codes) for Customer	Customers of Customer
Order data (especially currently selected products, recently ordered products, product categories and types, revenue, delivery status)	Automated processing of promotional and/or loyalty activities (e.g. creation of coupon codes) for Customer	Customers of Customer
Session data (especially device, operating system)	Automated processing of promotional and/or loyalty activities (e.g. creation of coupon codes) for Customer	Customers of Customer
Location data (especially GPS location)	Automated processing of promotional and/or loyalty activities (e.g. creation of coupon codes) for Customer	Customers of Customer
User master data of Customer's employees with access to Talon.One's platform (especially name, email address)	Access control of Talon.One's platform; customer support and related services	Employees of Customer

§ 3 Processor's Obligations

(1) Talon.One will ensure that all employees and other persons involved in Processing Personal Data are prohibited from Processing Personal Data outside the scope of Customer's instructions.

(2) Talon.One shall notify Customer without undue delay and no later than 72 hours after receiving actual knowledge of a Personal Data Breach within its scope of responsibility. Talon.One shall implement the measures necessary for securing Personal Data and for mitigating potential negative consequences for the Data Subject; Talon.One shall coordinate such efforts with Customer without undue delay.

(3) Talon.One shall inform Customer without undue delay if, in its opinion, Customer's instruction infringes Applicable Data Protection Legislation. Customer acknowledges and agrees that Talon.One is not responsible for performing legal research or providing legal advice.

(4) Taking into account the nature of the processing and the information available to Talon.One, Talon.One shall provide reasonable assistance to Customer with any data protection impact assessments, risk assessments, and prior consultations with supervisory authorities that Customer reasonably considers to be required under Applicable Data Protection Legislation, in each case solely in relation to the processing of Personal Data by Talon.One under this Agreement. To the extent legally permitted, Customer shall be responsible for any costs arising from Talon.One's provision of such assistance.

§ 4 Controller's Obligations

(1) If Customer becomes aware that its processing instructions infringe upon Applicable Data Protection Legislation or that there is a material irregularity in Processor's provision of the Services, Customer shall promptly inform Processor thereof.

(2) Unless otherwise specified in the applicable Order Form, Customer may not provide Talon.One with any sensitive or special Personal Data that imposes specific data security or data protection obligations on Talon.One in addition to or different from those specified in the DPA, the Order Form and/or the Agreement.

§ 5 Enquiries by Data Subjects

Where a Data Subject asserts claims for rectification, erasure or access against Talon.One, and where Talon.One is able to correlate the Data Subject to Customer, based on the information provided by the Data Subject, Talon.One shall refer such Data Subject to Customer without undue delay. Talon.One shall support Customer, where possible, and based upon Customer's instruction insofar as agreed upon. Talon.One shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly, or in a timely manner. To the extent Customer, in its use of the Talon.One Services, does not have the ability to address such Data Subject request, Talon.One shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject request, to the extent Talon.One is legally permitted to do so and the response to such Data Subject request is required under Applicable Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any costs arising from Talon.One's provision of such assistance.

§ 6 Security and Confidentiality

(1) Talon.One shall implement technical and organizational measures as set out in **Appendix C** to ensure the adequate protection of Customer's Personal Data, in accordance with Article 32 of the GDPR. Customer is familiar with these technical and organizational measures, and it shall be Customer's responsibility that such measures ensure a level of security appropriate to the risk. Talon.One reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(2) All Talon.One personnel involved in the Processing Personal Data, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Talon.One's policies concerning protection of confidential information.

§ 7 Audit Right

(1) Unless otherwise required by Applicable Data Protection Legislation or Customer's supervisory authority, Customer or its supervisory authority may audit Talon.One's compliance with its obligations under this DPA up to once per calendar year.

(2) If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and Talon.One (except if such third party is a supervisory authority). Talon.One will not unreasonably withhold its consent to a third-party auditor requested by Customer. The third party must execute a written confidentiality agreement acceptable to Talon.One or otherwise be bound by a statutory or legal confidentiality obligation.

(3) Customer must provide Talon.One with a prior written notice at least 10 days in advance of the proposed audit date, unless a shorter notice is required under Applicable Data Protection Legislation in which case such shorter notification period shall apply.

(4) The audit must be conducted during regular business hours at the applicable facility, subject to Talon.One's health and safety or other relevant policies and may not unreasonably interfere with Talon.One's business activities. If mandatory under Applicable Data Protection Legislation, the audit may be conducted outside Talon.One's regular business hours.

(5) Upon completion of the audit, Customer will provide Talon.One with a copy of the audit report, which is subject to the confidentiality terms of the Agreement. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

(6) Each Party will bear its own costs in relation to the audit, unless Talon.One incurs additional charges or fees in the performance of the audit that are not covered by the fees payable for the Services under the applicable Order Form, such as additional license or third-party contractor fees. The Parties will negotiate in good faith with respect to any such charges or fees. Talon.One shall bear the reasonable audit costs in case the audit reveals Talon.One's material violation of the terms of this DPA.

§ 8 Sub-Processors

(1) Customer gives Talon.One a general authorization to engage Sub-Processors in connection with the provision of the Services. Talon.One will enter into an agreement with each Sub-Processor that provides for, in substance, the same data protection obligations as those binding Talon.One under this DPA, to the extent applicable to the Services provided by each Sub-Processor.

(2) Talon.One currently uses the Sub-Processors set out in Appendix D below, which may be updated from time to time in accordance with this Clause 8(2). Prior to engaging any new Sub-Processors that Process Customer's Personal Data, Talon.One will notify Customer via email and allow Customer thirty (30) days to object. If Customer has legitimate objections to the appointment of any new Sub-Processors based on data security concerns, the Parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days. To the extent the Parties do not reach a mutually acceptable resolution within a reasonable timeframe, Customer's sole and exclusive remedy shall be the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to Customer or Talon.One and (iii) without relieving Customer from its payment obligations under the Agreement up to the date of termination. If the termination in accordance with this Section only pertains to a portion of Services under an Order Form, Customer will enter into an amendment or replacement Order Form to reflect such partial termination.

(3) Talon.One is responsible for the performance of such Sub-Processor's obligations in compliance with the terms of this DPA and Applicable Data Protection Legislation.

§ 9 Cross-Border Personal Data Transfers

(1) Without prejudice to any applicable restrictions for Services specified in the Agreement, Talon.One may Process Personal Data globally as necessary to perform the Services.

(2) To the extent such global access involves a transfer of Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Legislation, such transfers shall be subject to security and data privacy requirements consistent with the relevant requirements of this DPA and such Applicable Data Protection Legislation.

(3) Where Personal Data protected by the EU GDPR is being transferred via the Services from the European Union to outside the European Economic Area and/or Switzerland, either directly or via onward transfer, to Sub-Processors in countries that are not (yet) recognized by the European Commission as providing an adequate level of protection for Personal Data, Talon.One shall, as the exporting party, ensure its and its Sub-Processors' compliance with applicable laws, in particular the EU GDPR, prior to transmitting any Personal Data by appropriate measures, including by entering into the applicable Standard Contractual Clauses with such Sub-Processor.

Where Talon.One is based outside the European Economic Area and/or Switzerland and Personal Data is being protected by the EU GDPR, the Parties enter, with the conclusion of this DPA, also into the Standard Contractual Clauses, Module 2 (2021/914/EU) attached as **Appendix E**, including Appendices I to III. Customer enters into the Standard Contractual Clauses as the Data Exporter and Talon.One as the Data Importer.

In Clause 7 of the Standard Contractual Clauses, the optional docking clause does not apply.

In Clause 9 of the Standard Contractual Clauses, option 2 applies, and the time period for prior notices of Sub-Processor changes is stated in Clause 7(2) of this DPA.

In Clause 11 of the Standard Contractual Clauses, the optional language does not apply.

In Clause 17 of the Standard Contractual Clauses, option 1 applies, and the Standard Contractual Clauses are governed by the laws set out in the Agreement.

In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts set out in the Agreement.

With respect to the Appendices I to III the Standard Contractual Clauses the following shall apply:

(a) With respect to the information required according to Appendix I A of the Standard Contractual Clauses including the information about the Parties, the information laid down in the Order Form shall apply;
(b) With respect to the information required according to Appendix I B of the Standard Contractual Clauses, the information laid down in in this DPA, particularly Clause 2(2) and Clause 2(4), shall apply;
(c) Competent supervisory authority within the meaning of Appendix I C of the Standard Contractual Clauses shall be the competent supervisory authority in the country in which Controller has its headquarter;
(d) **Appendix C** shall apply as Appendix II of the Standard Contractual Clauses;
(e) Approved sub-processors according to Appendix III of the Standard Contractual Clauses are laid down in **Appendix D**.

In the event of a conflict between the Standard Contractual Clauses according to **Appendix E** and this DPA, the Standard Contractual Clauses shall prevail.

(4) If for any reason the aforementioned data transfer mechanisms are deemed inadequate by the appropriate regulatory body, such as the European Commission, the Parties will show good faith to enter into the appropriate data transfer mechanism(s) pursuant to Article 46 of the EU GDPR.

§ 10 Records

(1) Talon.One will keep detailed, accurate and up-to-date written records regarding its Processing of the Personal Data ("**Records**"). The Records shall include, at a minimum, all information required by Article 30 of the GDPR. Talon.One shall make such Records available to Customer in accordance with Section 7 (Audit Right) above.

§ 11 Return and Deletion of Personal Data

(1) Upon termination of the Agreement, Talon.One will, without undue delay, return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Data on Talon.One systems or Services environments, except as otherwise stated in the Agreement or except as Applicable Data Protection Legislation or other applicable law requires storage of such Personal Data. Export and retrieval may be subject to technical limitations, in which case Talon.One and Customer will find a reasonable method to allow Customer access to Personal Data.

(2) For Personal Data held on Customer's systems or environments, or for Services for which no data retrieval functionality is provided by Talon.One as part of the Services, Customer is advised to take appropriate action to back up or otherwise store separately any Personal Data while the production Services environment is still active prior to termination.

§ 12 Miscellaneous

(1) Talon.One may modify this DPA from time to time, including to comply with new data protection laws or regulations. If a modification will have a material adverse impact on Customer, Talon.One will use reasonable efforts to notify Customer through the Service and/or in accordance with the notification section of the Agreement before the change will take effect. Any changes to this DPA posted on the Talon.One website will be effective upon the earlier of a) the Customer consenting to such changes in writing or b) upon Customer's next Term renewal, except changes required by Applicable Data Protection Legislation or necessary for the use of new features that Customer has chosen to enable will become effective immediately to the extent necessary to comply with such law or as required to use such new features. If Customer objects to the updated DPA, as Customer's exclusive remedy and without penalty, Customer may choose: i) not to renew in accordance with the renewal terms set out in the applicable Order Form or ii) to terminate this DPA and cease providing Talon.One with Personal Data by giving written notice to Talon.One within thirty (30) days of being informed by Talon.One of the change.

(2) In case of any conflict, the data protection regulations of this DPA shall take precedence over the regulations of the Agreement. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

(3) To clarify, where this DPA requires written notices from the Parties, the provision of a notice in documented form (such as email) shall suffice.

Appendix A
UK DPA Addendum

§ 1 Cross-Border Personal Data Transfers

(1) Where Personal Data that is transferred via the Services from the United Kingdom to outside the United Kingdom, either directly or via onward transfer, to recipients in countries that are not (yet) recognized by United Kingdom regulatory authorities as meeting the data protection test in relation to the transfer of personal data (as described in the UK GDPR), Talon.One shall, in addition to Standard Contractual Clauses, sign an UK Addendum or, instead of the Standard Contractual Clauses combined with the UK Addendum, an IDTA with such Sub-Processor.

(2) Where Talon.One is based outside the United Kingdom and/or European Economic Area and/or Switzerland and Personal Data is being protected by the UK GDPR, the Parties enter, with the conclusion of this DPA, also into the Standard Contractual Clauses, Module 2 (2021/914/EU) attached as Appendix E, including Appendices I to III, as detailed in Clause 9(3) of the DPA. In addition, the Parties agree to sign an UK Addendum along with the Standard Contractual Clauses.

For Table 1 of the UK Addendum, the Parties' key contact information is located in the applicable Order Form.

For Table 2 of the UK Addendum, the relevant information about the version of the Standard Contractual Clauses, modules, and selected clauses which this UK Addendum is appended to is located above in Clause 9(3) of the DPA.

For Table 3 of the UK Addendum:

(a) The information required for Annex 1A is located in the applicable Order Form.
(b) The information required for Annex 1B is located in Clause 2(2) and Clause 2(4) of the DPA.
(c) The information required for Annex II is located in **Appendix C**.
(d) The information required for Annex III is located in **Appendix D**.

In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

(3) If for any reason the aforementioned data transfer mechanisms are deemed inadequate by the appropriate regulatory body, such as the European Commission, the Parties will show good faith to enter into the appropriate data transfer mechanism(s) pursuant to Article 46 of the UK GDPR.

Appendix B
U.S. DPA Addendum

§ 1 Scope of Processing

(1) Talon.One shall not retain, use, disclose or otherwise Process such Personal Data for a Commercial Purpose other than for the limited and specified purposes set out in this DPA and/or the Agreement, and/or any applicable Order Form, or as otherwise permitted under the DPA.

(2) Talon.One shall not Sell or Share such Personal Data within the meaning of the Applicable U.S. Data Protection Legislation.

(3) Talon.One shall not retain, use, disclose or otherwise Process such Personal Data outside the direct business relationship with Customer and not combine such Personal Data with Personal Data that it receives from other sources, except as permitted under the Applicable U.S. Data Protection Legislation.

§ 2 Compliance and Same Level of Protection

(1) Talon.One shall comply with all applicable obligations under the Applicable U.S. Data Protection Legislation and shall provide the same level of privacy protection for the Personal Data as is required of Customer under the Applicable U.S. Data Protection Legislation.

(2) Talon.One shall notify Customer in written form without undue delay if it makes a determination that it can no longer meet its obligations under the Applicable U.S. Data Protection Legislation or this U.S. DPA Addendum. Such notification shall include a detailed description of the circumstances leading to such determination.

§ 3 Assistance with Controller's Obligations

(1) Talon.One shall reasonably cooperate and – as far as such obligations relate to the Processing of Personal Data by Talon.One under this DPA – assist Customer with meeting Customer's compliance with Applicable U.S. Data Protection Legislation and responding to related inquiries, including responding to verifiable Data Subject, taking into account the nature of the Talon.One's Processing and the information available to Talon.One. Talon.One may charge Customer reasonable fees for any such assistance.

(2) Talon.One shall without undue delay notify Customer if it receives any complaint, notice, or communication that directly or indirectly relates either Party's compliance with the Applicable U.S. Data Protection Legislation.

§ 4 Further Processor Obligations

(1) Talon.One must promptly comply with any Customer request or instruction from Customer requiring Talon.One to provide, amend, transfer, or delete Personal Data, or to stop, mitigate, or remedy any unauthorized Processing.

(2) If the Business Purposes require the collection of Personal Data from Data Subjects on the Customer's behalf, Talon.One shall provide a notice in compliance with Applicable U.S. Data Protection Legislation addressing use and collection methods used by Talon.One.

§ 5 Sub-Processing

Talon.One may use Sub-Processors to provide the Services. Any Sub-Processor used must qualify as a 'service provider' under the Applicable U.S. Data Protection Legislation, shall not Sell Personal Data as defined and interpreted under the Applicable U.S. Data Protection Legislation, and Talon.One cannot make any disclosures to the Sub-Processor that the Applicable U.S. Data Protection Legislation would treat as a Selling of Personal Data.

Appendix C
Technical and Organizational Security Measures

Purpose of this document
This document outlines Talon.One GmbH's technical and organizational measures to secure customer data against unauthorized access, disclosure, alteration, or destruction. These measures are maintained and regularly audited in accordance with industry standards and top level attestations and certifications.

As our services operate in a cloud environment without proprietary server infrastructure, measurements are tailored to each service.

Talon.One continuously monitors the effectiveness of its information safeguards.

1. People and awareness

- All candidates are subject to thorough screening as part of the hiring process. Background checks are performed where permitted by law and are appropriate to the role
- All new employees are required to sign an employment agreement that includes clauses on confidentiality, ethical conduct, and information protection awareness
- All employees receive mandatory annual security and privacy awareness training, and their participation is documented.
- A clear disciplinary process is in place and communicated to all personnel to address and act on any violations of information security policies in place
- Security Policies are maintained and updated regularly and are shared with all employees
- Access to systems is provided on a ‘need to have basis’ taken into account segregation of duties

2. Physical security and access control

Services’ infrastructure is hosted on cloud platforms with utmost security standards, which maintains high-security data centers. Physical access is restricted to authorized personnel and is monitored 24/7 with video surveillance and intrusion detection systems. A review of Talon.One’s SOC2 and relevant reports is conducted annually.

At Talon.One’s Berlin office:
- Physical entry is restricted to authorized employees via a designated access control system
- All visitors must be registered upon arrival
- All visitors must be escorted by an employee at all times
- Physical access is reviewed periodically
- Clean desk, clear screen and follow me printing, process implemented

3. Remote users and access control

Remote users work with laptops and desktops provided by and maintained by Talon.One

Additional security measures are incorporated in addition as follows:
- Encryption of the hard disk on company assigned laptops
- Centrally managed and anti-virus protection
- Management and monitoring of end points to control an authorized software installation
- Login ID and password controls are implemented to access information
- A strong password policy is enforced across all systems, including minimum length and complexity requirements, enforce periodic changes and account suspension after a maximum number of failed login attempts
- Multi-factor authentication is used in general for remote access to systems
- Access to critical systems require connection via added VPN special policies and approval flow

4. Access control to personal data

Access to personal data is governed by the principle of least privilege ('need to know' and 'need to access'), ensuring that only authorized individuals can view or process it. Data access is granted solely for the fulfillment of employees' responsibilities.

Access logs are maintained, and accountability for access control is assigned.

In addition, the following measures are in place:
- Employees must comply with the applicable security policies and data management policy
- Access to data and resources is controlled via role-based access control
- User and administrator permissions are periodically reviewed, updated and approved
- User accounts are promptly disabled or deleted upon an employee's job termination
- Segregation of duties is maintained to prevent unauthorized changes and avoid operational risk
- Electronic access control: particularly through passwords, automatic lock mechanisms, multi-factor authentication
- Internal access control: namely, by using
- standard-authorisation profiles on a “need to know” basis, a standard process for assigning user rights, access logging, periodic review of the assigned rights, especially of administrator accounts
- Controlled destruction of data media

5. Data security and confidentiality

Talon.One employs robust measures to protect the confidentiality, integrity, and availability of data throughout its lifecycle, based on a risk assessment:

- Data is encrypted both in transit and at rest:
- In-transit: All inbound communication to our systems is exclusively facilitated through an authenticated TLS connection, utilizing the most robust algorithms available.
- At-rest: Customer data is encrypted at rest and hosted on secured storage services
- Electronic transmission or transport must run through encryption and Virtual Private Networks (VPN)
- Compliance with processing registers according GDPR requirements
- The ability to restore the availability and access to Data in a timely manner in the event of a physical or technical incident:
- Backups are conducted daily via snapshots
- Restore tests are conducted at least annually to validate disaster recovery capabilities

6. Other security measures

In addition, a range of technical and procedural controls are implemented to ensure the overall security of Talon.One's platform and systems, including but not limited to:

- All connectivity up to the secured area is encrypted
- All client data is stored in encrypted storage
- Access to production only possible using multi-factor authentication and enforced SSO connections via provided security client
- Network security components and mechanisms, including logical segregation
- Access managed according to role-based access control paradigms
- Privacy management, including regular employee training
- Continuous vulnerability assessments and annual penetration tests by a 3rd party
- Incident response management
- Established Change management process for code changes utilizing a formal SDLC process and IaC practices
- Periodic audits to ensure up-to-date certifications (ISO27001; SOC2)

7. Organizational controls

The security program is underpinned by a strong organizational framework, utilizing:

- Policies and Procedures: Security and privacy policies are formally documented, reviewed, and approved on an annual basis by a dedicated information security team
- Risk Management: A formal risk assessment process is in place, in order to identify and manage risks to Talon.One's systems. Risk assessment meetings are held at least annually to evaluate threats and ensure compliance
- Vendor Management: To ensure adherence to data protection standards and evaluate supply-chain risks, a thorough vendor management process is maintained, including evaluations of vendors and suppliers and obtaining contractual commitments

Appendix D
Sub-Processor Addendum

Category	Name	Headquarters	Description
Talon.One Affiliates (except for the contracting Talon.One affiliate, which qualifies as Processor)	Talon.One GmbH	Germany	Services & Support
	Talon.One Inc.	United States	Services & Support
	Talon.One UK Ltd	United Kingdom	Services & Support
	Talon.One SG Pte Ltd	Singapore	Services & Support
Cloud Platforms & Data Management:	Aiven Oy	Finland	Managed service for database hosting, runs on Google Cloud Platform.
	Fivetran Inc.	United States	Data integration tool that extracts, loads, and transforms data from various sources into data warehouses like BigQuery.
	Google Ireland Limited (Google Cloud Platform (GCP), BigQuery, Looker, Google Workspace, Gemini)	Ireland; globally in accordance with Customer's selection	Cloud infrastructure and analytics for Talon.One products and workplace; provider of generative AI services
	Prismatic Software Inc.	United States	Development, hosting, and delivery of software integrations
Data Analytics & Visualization:	MixPanel, Inc.	United States	User analytics tool focused on tracking product usage, customer behavior, and engagement.
Monitoring, Incident Management & Error Tracking:	Pineapple Technology Ltd (Incident.io)	United Kingdom	Incident management tool for tracking and resolving operational incidents.
	Datadog, Inc.	United States	Monitoring tool for infrastructure, applications, and log management, providing real-time performance data and alerting.
Customer Relationship & Success Management:	Planhat AB	Sweden	Customer success platform used to manage and optimize customer relationships.
	Salesforce.com Germany GmbH	United States	Customer relationship management (CRM) platform for sales, marketing, and customer service.
	FGPL Business Solutions Inc (Virtua)	Philippines	Customer Support services
Communication & Collaboration Tools:	Salesforce.com Germany GmbH (Slack)	United States	Team communication platform for messaging, file sharing, and collaboration within teams.

Appendix E
Standard Contractual Clauses

(EU/2021/914)

Module 2

SECTION I

***Clause 1*- Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

***Clause 2* - Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3* - Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4* - Interpretation**

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5* - Hierarchy**

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

***Clause 6* - Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7 – Optional* Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

***Clause 8* - Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning

health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

***Clause 9* - Use of sub-processors**

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10 **- Data subject rights**

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 **- Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 **- Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 **- Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

***Clause 14* - Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

---

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Clause 15* - Obligations of the data importer in case of access by public authorities**

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

***Clause 16* - Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 **- Governing law**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Clause 18 **- Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*
Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

...

Categories of personal data transferred

...

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

...

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

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

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

...

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

...

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

...

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

…

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …