441 9th Avenue, 12th Floor
New York, NY 10001

DATA PROCESSING ADDENDUM

In the course of providing the Sprinklr Services to Customer, Sprinklr may Process Personal Data on behalf of Customer. This Data Processing Addendum ("DPA") reflects the Customer's instructions and the parties' agreement for the Processing of Personal Data, in accordance with Data Protection Legislation. This DPA, as amended from time to time, is incorporated by reference as part of the Master Services Agreement (or other agreement for the license and purchase of the Sprinklr Services, hereinafter collectively "Agreement") between Customer and Sprinklr. Capitalized terms not defined in this DPA are defined in the main body of the Agreement.

For the avoidance of doubt, to the extent that Customer is a "Covered Entity" or a "Business Associate," as such terms are defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and Customer instructs Sprinklr to process "Protected Health Information" on Customer's behalf, the terms of the Business Associate Agreement between Sprinklr and Customer shall govern with respect to the processing of Protected Health Information.

This DPA will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this DPA or when Sprinklr ceases to Process Personal Data on behalf of Customer.

This DPA consists of:

A. DATA PROCESSING TERMS

1. DEFINITIONS

To the extent not defined in the applicable Agreement, the following definitions shall apply. In the event of any inconsistencies or conflict between the Agreement and the definitions set out below, the definitions in the Agreement shall prevail.

"Account Information" means any Content other than Customer Content and Inbound Content and Customer Care Data.

"Affiliate" means any entity which is directly or indirectly controlling, controlled by, or under common control with a party to this Agreement.

"Connected Services" means the various channels and integrations supported by the Platform that Customer desires to connect to through the Platform, including the social media services.

"Content" means Inbound Content, Customer Content and Account Information entered into the Sprinklr Account or Platform or any other data managed by the Customer via the Platform.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Care Data" means any material that is submitted to the Platform by a person other than a Customer User through the Connected Services that the Customer has integrated into the Sprinklr Platform for purposes of customer care and support (including, where applicable under the Order Form, voice data).

"Customer User" means an individual user who is authorized by Customer to use the Platform and to whom Customer supplied a user identification and password. Customer Users may include, for example, Customer's employees and contractors.

"Data Protection Legislation" means all applicable privacy, data protection, and data security laws and regulations of any jurisdiction applicable to Sprinklr's Processing of Personal Data under the Agreement, including, as applicable and without limitation, (a) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); (b) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing; and (c) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"), the Colorado Privacy Act ("**CPA**"), the Connecticut Data Privacy Act ("CTDPA"), the

Utah Consumer Privacy Act ("UCPA"), and the Virginia Consumer Data Protection Act (**"VCDPA"**), (collectively referred to as "**US Privacy Laws**") and any binding regulations promulgated thereunder.

"Data Subject" means the individual to whom the Personal Data pertains.

"EU-US Data Privacy Framework" means the approved mechanism as developed by the US Department of Commerce and the European Commission and the UK Government, to facilitate lawful transfers of data from the UK and EU to the US. Reference to the Data Privacy Framework is inclusive of the UK Extension to the Data Privacy Framework.

"Inbound Content" means any information received from any Connected Service, including any information published on any Connected Service, not created by a Customer User. Such information includes but is not limited to, in whatever form and/or nature, text, data, graphics, photos, audio, video, electronic messages, trademarks and other identifiers. Where applicable to the Sprinklr Services being purchased, Inbound Content may include Customer Care Data.

"Personal Data" means "personal data," "personal information," or an equivalent term, as defined by applicable Data Protection Legislation to the extent such data or information is accessed, collected, stored, transmitted, processed, hosted, used, handled, or disposed of by Sprinklr in connection with the Agreement; provided that, for purposes of this DPA, the foregoing shall not include "Protected Health Information," as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), which shall be addressed separately in the Business Associate Agreement executed by the parties.

"Personal Data Breach" means a failure of Sprinklr's security controls leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Sprinklr's possession, custody, or control, to the extent the breach materially compromises the confidentiality, security or integrity of the Personal Data.

"Platform" means Sprinklr's proprietary customer experience software service, accessed by Customer via the internet, as specified in an applicable Order Form. Platform includes Updates made during the Term.

"Processing" means any operation or set of operations which is performed by or on behalf of Sprinklr in connection with the Agreement upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller pursuant to the Controller's instructions and solely to provide the Sprinklr Services.

"Professional Services" means services other than the Platform that may be offered from time to time and that Customer elects to receive as described in an executed Statement of Work.

"SCCs" means, as applicable: (i) the Standard Contractual Clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which are attached as Part D ("**2021 EU SCCs**"); and (ii) the Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, which went into effect on 21 March 2022 and is attached as Part E ("**UK IDT Addendum"**).

"Sprinklr Services" means the Platform and Professional Services.

"Subprocessor" means any Processor engaged by Sprinklr or a Sprinklr Affiliate.

2. DATA PROCESSING

2.1 The parties acknowledge and agree that with regard to the Processing of Personal Data, Sprinklr is the **Processor** and Customer and/or the Customer Affiliate determines the purposes and means of the Processing of Personal Data and is the **Controller**.

2.2 The parties shall each comply with their respective obligations under Data Protection Legislation. Customer shall, in its use of the Sprinklr Services, Process Personal Data in accordance with Data Protection Legislation, the Agreement, and Sprinklr's Acceptable Use Policy.

2.3 Customer's instructions for the Processing of Personal Data shall comply with Data Protection Legislation. Sprinklr shall inform Customer immediately if, in Sprinklr's opinion, an instruction from Customer violates Data Protection Legislation.

2.4 Customer warrants that it has an appropriate lawful basis under Data Protection Legislation to share Personal Data with Sprinklr in connection with the Sprinklr Services.

2.5 Unless required under Applicable Law, Sprinklr shall only Process Personal Data (i) in accordance with Customer's documented instructions as set out in this DPA or the Agreement, Order Form, or Statement of Work for the purposes of providing the Sprinklr Services; (ii) to comply with other documented reasonable instructions provided by Customer. Sprinklr agrees it shall not sell any Personal Data.

2.6 Sprinklr shall take reasonable steps to (and instruct Sub-processors to) (i) train employees on applicable Data

Protection Legislation and security requirements; (ii) instruct and train employees who have access to Personal Data on maintaining the confidentiality of the Personal Data, and (iii) limit access to Personal Data on a need-to-know basis.

2.7 To the extent Sprinklr processes any de-identified data under the Agreement, Sprinklr shall (i) take reasonable measures to ensure such data cannot be associated with a natural person; and (ii) where required by Data Protection Legislation, publicly commit to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data unless permitted by Data Protection Legislation.

3. DATA SUBJECTS' RIGHTS REQUESTS

3.1 Sprinklr shall, to the extent legally permitted, promptly notify Customer if Sprinklr receives a request from a Data Subject to exercise the Data Subject's rights under Data Protection Legislation ("**DSR Request**").

3.2 Taking into account the nature of the Processing, Sprinklr shall assist Customer with appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a DSR Request under Data Protection Legislation.

3.3 To the extent Customer, in its use of the Sprinklr Services, does not have the ability to address a DSR Request using the measures provided by Sprinklr in 3.2, Sprinklr shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such a DSR Request, to the extent Sprinklr is legally permitted to do so and the response to such DSR Request is required under Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any costs arising from Sprinklr's provision of such assistance which exceeds Sprinklr's standard or legally required support for the management of DSR Requests.

4. DATA PROTECTION IMPACT ASSESSMENTS

Sprinklr shall provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with a competent data protection supervisory authority, as required under Data Protection Legislation, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of, the Processing and information available to, Sprinklr, in its provision of the Sprinklr Services to the Customer.

5. PERSONAL DATA BREACH NOTIFICATION

5.1 Sprinklr shall notify Customer without undue delay, and, in any event within forty-eight (48) hours after becoming aware of a Personal Data Breach. Where possible, Sprinklr shall provide Customer with sufficient information to allow Customer to meet any obligations to notify regulators and/or affected individuals of the Personal Data Breach. Such notification shall include, to the extent known to Sprinklr:

(a) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate volume of Personal Data records concerned;

(b) the likely consequences and impact of the Personal Data Breach;

(c) the measures taken or proposed to be taken by Sprinklr to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(d) the name and contact details of the DPO or a point of contact from whom more information can be obtained.

5.2 Sprinklr shall make reasonable efforts to identify the cause of a Personal Data Breach and take the steps as Sprinklr deems possible, necessary, and reasonable to remediate the cause of such a Personal Data Breach to the extent the remediation is within Sprinklr's reasonable control.

5.3 The obligations with regards to remediation in 5.2 above shall not apply to incidents that are caused by Customer.

6. SECURITY AND OTHER SUPPLEMENTARY MEASURES

Sprinklr shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, damage, or unauthorized disclosure or access, as described in Part C, below (*Enterprise Security Addendum*).

7. THIRD PARTY DISCLOSURES

7.1 Sprinklr agrees not to allow, unless required by applicable law, regulations, order of a court, or any regulatory, judicial, governmental, or similar body, or as authorized by Customer, access to Customer Content (excluding any publicly available data) by any administrative body, authority or agency.

7.2 Customer acknowledges that Sprinklr may be required by law to allow such access to Customer Content. Where Sprinklr receives such a demand, Sprinklr shall, where legally permitted, seek to redirect the demand to Customer, and Customer agrees that Sprinklr may provide information as reasonably necessary to facilitate such a redirect. If Sprinklr is not able to redirect the demand to the Customer, then Sprinklr shall (to the extent permitted by law) use commercially reasonable efforts to inform the Customer of the circumstances of the required disclosure and the Customer Content that must be disclosed. For the avoidance of any doubt, this shall in no way prejudice Sprinklr's obligations arising out Clause 15.2 of the 2021 EU SCCs.

8. DELETION OR RETURN OF PERSONAL DATA

8.1 Sprinklr shall delete the Personal Data upon termination/expiry of the Agreement, in accordance with the selected retention package as specified in the Order Form and configured by the Customer, or upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent legally required and only to the extent and for such period as legally required, and always provided that Sprinklr shall ensure the confidentiality of the Personal Data and that such Personal Data is only Processed as necessary for the legally required purpose(s).

8.2 Sprinklr shall return Personal Data to Customer upon request in accordance with the procedure and timeframe specified in the Agreement.

9. AUDITS AND INSPECTIONS

9.1 Subject to the terms of this section 9, Sprinklr shall make available to Customer the information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits by Customer or a mutually agreed to third-party auditor ("Auditor") in relation to the Processing of Personal Data. Sprinklr shall not unreasonably withhold approval of Customer-preferred Auditor.

9.2 Upon Customer's written request, Sprinklr shall, not more than once per year, accurately complete a reasonable information security questionnaire provided by Customer regarding Sprinklr's data protection and information security practices and policies. Sprinklr may refuse to provide answers to questions or information requests which, if broadly made available, could lead to (i) disclosure of sensitive Sprinklr intellectual property or trade secrets; (ii) disclosure of non-public information of other Sprinklr customers or Data Subjects or (iii) a material weakening of Sprinklr's security controls.

9.3 Customer or Auditor may, in accordance with applicable law, at Customer's expense and not more than once per year, perform an on-site audit of Sprinklr's data protection and information security practices and policies with written notice provided reasonably, but at least thirty (30) business days, in advance. The audit shall take place over not more than one day, unless Sprinklr permits otherwise, during Sprinklr's normal business hours on a mutually agreed schedule that will minimize the audit's impact on Sprinklr's operations. Customer or Auditor shall comply with Sprinklr's security requirements related to the performance of the audit. Due to confidentiality and security requirements, such audit shall exclude on-site inspections of other Sprinklr customer environments or multi-tenant environments (such as IaaS data centers or other shared services used by Sprinklr). On-site audits may be substituted by the provision of documentation regarding the respective data protection and security measures taken and specific certifications issued by reputable third-party auditors, provided by Sprinklr upon Customer's request.

9.4 Examinations performed via online video-sharing conferencing tools are considered on-site examinations. Customer shall promptly notify Sprinklr of any non-compliance discovered during such an audit/inspection.

9.5 Notwithstanding Sprinklr's obligations under Sections 9.2 or 9.3, if the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2 report or similar audit report or certificate performed by a qualified third-party auditor within twelve (12) months of Customer's audit request or by an applicable current ISO certificate, and Sprinklr has certified in writing that there are no known material changes in the controls audited, Customer may instead agree to accept such report in lieu of requesting an audit under Section 9.3.

9.6 Any type of assessment, review, questionnaire or audit required by the customer will be carried out in accordance with the applicable limitations in Sections 9.2 and 9.3.

9.7 All information provided to Customer or Auditor pursuant to this Section 9 is considered Sprinklr Confidential Information.

10. LIABILITY

10.1 Each party's liability arising out of or related to this DPA and all DPAs between Customer's Affiliates and Sprinklr, whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section agreed to under the Agreement, and any reference in such section to the liability of a party means the aggregate

liability of that party and all of its affiliates under the Agreement and all DPAs together, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any of Customer's Affiliate that is a contractual party to any such DPA.

10.2 To the maximum extent required by applicable law, as far as the parties' external relationship is concerned, the mandatory statutory provisions in Art. 82 et seq. GDPR, apply in the event of compensation or liability claims. Without prejudice to the foregoing, the parties' liability towards each other in the internal relationship is subject to the limitation of liability section in the Agreement.

10.3 Where a Data Subject asserts any claims against a party to this DPA in accordance with applicable Data Protection Legislation, the other party shall support in defending against such claims, where possible.

11. SUBPROCESSORS

11.1 Sprinklr has Customer's general authorization to use the Subprocessors linked at www.sprinklr.com/legal in the Processing of Personal Data, provided that Sprinklr shall (i) carry out adequate diligence prior to engaging the Subprocessor to select Subprocessors that are capable of maintaining the privacy, confidentiality, security, integrity, and availability of Personal Data consistent with the requirements of this DPA; and (ii) ensure that the arrangement between Sprinklr and Subprocessor is governed by a binding contract that includes terms which offer a substantially similar level of protection for Personal Data as those set forth in this DPA and which meet the requirements of Data Protection Legislation.

11.2 If Subprocessors are replaced or added during the term of the Agreement, Sprinklr shall give customer notice of such changes 30 days prior, allowing Customer 15 days from receipt of that notice to raise a material objection to the change provided Customer has subscribed to receive email notifications of such changes at www.sprinklr.com/subprocessors. Sprinklr and Customer shall work together in good faith to cure any material reasonable objection.

11.3 Sprinklr will remain liable to the Customer for the acts and omissions of Sprinklr's Subprocessors to the extent they relate to the provision of the Sprinklr Services to the Customer, consistent with the limitations of liability set forth in the Agreement.

12. CCPA

12.1 This section shall only apply where the CCPA is applicable to the Parties. For purposes of this Section 12, the terms "**Commercial Purpose**," "**Sell**," "**Service Provider," and "Share"** shall have the respective meanings given thereto in the CCPA, and "**Personal Information**" shall mean Personal Data that constitutes Personal Information governed by the CCPA.

12.2 It is the Parties intent that with respect to any Personal Information, Sprinklr is the Service Provider. Sprinklr (i) acknowledges that Personal Information is disclosed by Customer only for limited and specified purposes described in the Agreement; (ii) shall comply with applicable obligations under the CCPA, and shall provide the same level of privacy protection to Personal Information as is required by the CCPA; (iii) agrees that Customer has the right to take reasonable and appropriate steps under Section 9 of the DPA to help ensure that Sprinklr's use of Personal Information is consistent with Customer's obligations under the CCPA; (iv) shall notify Customer in writing of any determination made by Sprinklr that it can no longer meet its obligations under the CCPA; and (v) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate use of Personal Information.

12.3 Sprinklr, shall not (i) Sell or Share any Personal Information; (ii) retain, use, or disclose any Personal Information for any purpose other than for the specific Business Purpose of providing the Sprinklr Services under and in accordance with this Agreement, including retaining, using, or disclosing Personal Information for a Commercial Purpose other than the Business Purpose of providing the Sprinklr Services or as otherwise permitted by the Agreement or applicable law; (iii) retain, use, or disclose the Personal Information outside of the direct business relationship between Customer and Sprinklr; or (iv) combine Personal Information received pursuant to the Agreement with Personal Information (a) received from or behalf of another person or (b) or collected from Sprinklr's own interaction with any Consumer to whom such Personal Information pertains, except as otherwise permitted under the Agreement or Applicable Law.

12.4 Customer agrees that Sprinklr notifying Customer of Subprocessor engagements in accordance with Section 11 of this DPA shall satisfy Sprinklr's obligation under the CCPA to give notice of such engagements.

12.5 The Parties acknowledge that Sprinklr's retention, use, and disclosure of Personal Information authorized by Customer's instructions documented in the DPA are integral to the provision of the Sprinklr Services and the business relationship between the Parties.

13. INTERNATIONAL PERSONAL DATA TRANSFERS

13.1 Customer acknowledges and accepts that Sprinklr's provision of Sprinklr Services under the Agreement may involve the transfer of Personal Data to, or the Processing of Personal Data in, locations outside of the EEA, or UK, including to the United States or any other country in which Sprinklr, Sprinklr Affiliates, or Sprinklr Sub-processors perform their services. Customer agrees that such transfers are permitted, provided that they comply with Data Protection Legislation and are consistent with the safeguards included in this Section 13.

13.2 Sprinklr is an active participant in the EU-US Data Privacy Framework and agrees to maintain its participation in the EU-US Data Privacy Framework. Customer may choose to rely on the EU-US Data Privacy Framework as an adequate method of transferring Personal Data to Sprinklr. To the extent the EU-US Data Privacy Framework is invalidated, the parties will instead rely on the attached 2021 EU SCCs and UK IDTA, as set out in the following clauses.

13.3 The attached 2021 EU SCCs shall apply to any transfers of Personal Data under this DPA from the European Economic Area or where EU Data Protection Legislation or Swiss Data Protection Legislation applies to the Customer or Customer Affiliate making the transfer and where such transfer is made to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Legislation of the foregoing territories, to the extent such transfers are subject to such Data Protection Legislation. Where Customer is acting as Controller, Module 2 (Transfer controller to processor) of the 2021 EU SCCs in Part B shall apply. Where Customer Affiliate(s) is/are acting as Controller(s) and Customer is acting as Processor on Customer Affiliate's behalf, Module 3 (Transfer processor to processor) of the 2021 EU SCCs in Part B shall apply.

13.4 The attached UK IDT Addendum shall apply to any restricted transfer (as defined in the relevant Data Protection Legislation) of Personal Data under this DPA from the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Legislation of the United Kingdom, to the extent such transfers are subject to such Data Protection Legislation.

13.5 In the event of any conflict or inconsistency between this DPA and either the 2021 EU SCCs or the UK IDT Addendum, the 2021 EU SCCs and/or UK IDT Addendum shall prevail.

13.6 Where Personal Data is transferred to a country which does not ensure a level of protection essentially equivalent to that guaranteed within the United Kingdom or European Union, the Parties agree to work in good faith adopt and implement supplementary measures as required for compliance with regulations of the European Data Protection Board (hereinafter "Supplementary Measures").

14. CHANGE IN LAWS

Sprinklr may, on notice, amend this DPA to the extent reasonably necessary to address the requirements of Data Protection Legislation, including by replacing the relevant SCCs with (i) any new form of the relevant SCCs or any replacement thereof prepared and populated accordingly, or (ii) another transfer mechanism, other than the SCCs.

B. PARTIES AND DATA PROCESSING DETAILS

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	Customer name as per the MSA
Address	Customer addres. as per the MSA
Contact Person's name, position, and contact details	Customer contact as per the MSA
Activities Relevant to the data transferred under these Clauses:	The data exporter is a licensee and user of the Sprinklr platform.
Role (controller/processor):	As per section 2.1 of this DPA.

Data importer(s): Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union.

Name	**Sprinklr, Inc.**
Address	441 Ninth Avenue 12th Floor New York, NY 10001
Contact Person's name, position, and contact details	Bird & Bird DPO Services SRL, Avenue Louise 235 b 1, 1050 Brussels Belgium privacy@sprinklr.com
Activities Relevant to the data transferred under these Clauses:	The data importer provides the Sprinklr Platform (SaaS), a customer experience and social media management platform.
Role (controller/processor):	**Processor**

DETAILS OF PROCESSING AND DESCRIPTION OF TRANSFER

Categories of Data Subjects:	1. Customer's employees, agents and subcontractors who are operating the Sprinklr Platform, as well as individuals collaborating and communicating with Customer's customers, followers, fans, and other Internet users who use social networks and websites. 2. Any data subjects whose information is uploaded or stored by Customer into the Sprinklr Platform, including commercial contacts, prospects, or marketing contacts. 3. Customer's customers, followers, fans, and other Internet users who use social media networks and websites, blogs, forums, review sites, mainstream news sources, or any other website, including websites owned by Customer where Sprinklr provides social and content management functionality on Customer's behalf, or which Customer has integrated into the Sprinklr Platform.
Categories of Personal Data	1. Account Information, which includes Personal Data such as identification data (name, login), contact information (business email address), work related information (job title or role, social information (social contact handling data), and usage information (performance data, device data, and location data). 2. Inbound Content, which includes any Personal Data published or sent by third parties, (e.g., social media users) via the Connected Services, including Customer's social media profiles which are integrated into the Sprinklr Platform, as well as publicly accessible data from the social media networks or other websites used for social and content management and research capabilities. Inbound Content may include user IDs, social network profile names and information, social network communications (both public and private messages to Customer), information shared across social media networks and other websites, such as comments, reviews, reactions, and engagement. 3. Customer Care Data, which includes any Personal Data submitted by Customer's customers, followers, fans, and other individuals to Customer for purposes of customer care and support (including, where applicable under the relevant Order Form, voice data). 4. Customer Content, which includes any other category of Personal Data Customer provides as part of the Customer Content.
Special Categories of Data, Sensitive	Sprinklr does not require special categories of data to provide its services, but such data may be processed if:

Data, and Safeguards	1. Customer enables certain optional Platform features which require the processing of special categories of data. 2. Customer Content contains special categories of data, depending on what kind of data Customer uploads/stores into the Sprinklr Platform. 3. Inbound Content or Customer Care Data contains special categories of data, depending on what information individuals choose to provide through social networks, public internet sources, or as part of customer care and support inquiries. Sprinklr applies a consistent protection framework for all Personal Data, including special categories of data, and such controls include (i) address physical and logical access limitation based on a need-to-know principle; (ii) usage exclusively for providing the Sprinklr Services, as instructed by the Customer; (iii) adequate training for all operational staff with access to highly sensitive data; (iv) comprehensive logging; (v) encryption of data where technically feasible; and (vi) data destruction using industry standard destruction procedures.
Frequency of Transfer	Continuous.
Nature of Processing	Sprinklr processes, stores, collects, records, discloses by transmission, and erases Personal Data as a data Processor to provide the Sprinklr Platform and Sprinklr Services as contracted in the Agreement, in accordance with and only on Customer's instructions.
Purpose of Processing	Personal Data is Processed for the following purposes: (1) Account Information is processed to operate the Sprinklr Platform and provide the Sprinklr Services (authentication, login, and audit trail) (2) Inbound Content, Customer Care Data, and Customer Content is processed for purposes of providing the Sprinklr Services, including social media management, social media listening and analytics, customer care and support, marketing analytics, and marketing management.
Duration of Processing/Retention Period	Sprinklr shall delete Personal Data upon termination/expiry of the Agreement as specified in the Agreement, or upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent required by Data Protection Legislation and only to the extent and for such period as required by Data Protection Legislation, provided that Sprinklr shall ensure the confidentiality of all such Personal Data and that such Personal Data is only Processed as necessary for the purpose(s) specified in the Data Protection Legislation requiring its storage.

C. ENTERPRISE SECURITY ADDENDUM (ESA)

This Enterprise Security Addendum ("ESA") applies to all data processed on behalf of our customers in the Sprinklr Platform and in the provision of the Sprinklr Services, including any Sprinklr owned or leased servers used to host Customer's data.

The following technical and organizational measures are implemented by Sprinklr, in accordance with industry standards, to ensure an appropriate level of security related to use of the Sprinklr Platform. For access to documentation evidencing each of the measures listed below, including relevant certifications, please visit Sprinklr's Trust Center.

Information Security Program

Sprinklr has a dedicated security team led by Sprinklr's Chief Information Security Officer (CISO), chartered to define, supervise implementation of, and monitor all relevant security policies, standards, and controls (the "Security Team"). The Security Team is supported by Sprinklr's Board of Directors and the Executive Leadership Team and is independent from Sprinklr's Research & Development team, Information Technology team, and other operational teams. By independently validating the implementation of application security controls and reporting the outcome to Sprinklr leadership, the Security Team ensures proper accountability and a risk-informed decision process for maintaining and evolving the security program. In addition, Sprinklr's internal Governance, Risk, and Compliance function, alongside third-party auditors, provides oversight on Sprinklr's overall security posture and internal controls for risk management.

Security Manual

The Security Manual, available upon request, is maintained by the Security Team and provides an overview of all applicable security policies, controls, and procedures, as well as processes for the management of actual or reasonably suspected security incidents, including through (a) training personnel with access to the Sprinklr Platform and Customer data to recognize and report potential or actual security incidents; and (b) conducting post-incident reviews of events and actions taken.

Audit and Assurance

The Sprinklr Platform undergoes annual, independent audit and assurance assessments according to risk-based plans and policies. Sprinklr maintains the following: Reports – SOC 2 Type II, and SOC 3 and Certification – ISO 27001:2013, or an industry equivalent.

Sprinklr shall make available to Customer information necessary to demonstrate compliance with this ESA and shall reasonably allow for and contribute to audits by Customer as further defined in Sprinklr's Data Processing Addendum or as otherwise agreed to by Sprinklr and Customer in the Agreement.

Regular Risk Assessment of Information Security Program

Sprinklr conducts information security risk assessments annually, or whenever there is a material change in Sprinklr's business or technology practices that materially impacts the privacy, confidentiality, security, integrity, or availability of Customer data. These risk assessments include the validation of administrative, procedural, and technical controls and are conducted by independent third parties (e.g., third-party assessors and penetration testers) or the independent internal Security Team. Remediation of any material findings is tracked and validated.

Controls

- **Physical Access and Environmental Controls**

For all production systems, Sprinklr leverages our public cloud provider capabilities for the implementation and maintenance of physical controls to protect servers, networks, and facilities from unauthorized access. Controls include secure building with multiple secure access zones; secure perimeters; 24/7 video surveillance; on-site guard service; suitable environmental protections including climate-controlled data rooms and uninterruptible power sources; and other services as required by applicable regulations or requirements. Sprinklr periodically validates the suitability of these controls through third-party security audit reports and/or vendor audits. For more information on which cloud providers are used by Sprinklr, please refer to our subprocessor list, available at www.sprinklr.com/subprocessors.

- **Logical Access Controls**

Logical access to Sprinklr servers is limited to only those Sprinklr IT personnel who have the need and approval to directly access the servers. The Sprinklr Platform is set behind perimeter security controls jointly managed by the cloud provider and Sprinklr. No direct communication sessions originating from the Internet pass directly through the internal network. Sprinklr continuously monitors the key parameters for all Sprinklr Services for any unusual access activity.

- **Network Transport Controls**

Sprinklr has implemented industry standard security controls designed to protect all Customer data in transit from attacks against confidentiality or integrity. These controls include the implementation of applicable network protocols, encryption schemes, hashing of data, cryptographic signature, etc. Cryptographic keys and other secrets are managed using industry standard practices.

- **Data Storage Controls**

All media containing Customer data is protected from unauthorized physical access. Customer data at rest is encrypted using current and industry standard encryption mechanisms. Cryptographic keys are managed by Sprinklr in accordance with industry standard practices. Sprinklr's third party cloud hosting providers utilize NIST SP800-88 data destruction techniques. Customer data is deemed irrecoverable once deleted.

- **Authentication Controls**

Sprinklr implements industry standard identity governance processes and authentication mechanisms to ensure that only authorized users can interact with systems. This includes multi-factor authentication, single-sign-on architecture where technically feasible, and timely user provisioning and deprovisioning processes. All user actions, including successful and unsuccessful login attempts, user's first name and last name, IP address, date, and time stamp are logged. It is mandatory for all customers to integrate their SSO solution with their Sprinklr instance or utilize Sprinklr's 2FA capabilities for all user accounts to securely authenticate into the Sprinklr platform.

- **Data Access Controls (Authorization)**

Access to specific data, systems, or services is limited to users with a need to know, following a strict implementation of least privilege access authorization. Role Based Access Control ("RBAC") is used where feasible, and periodic access recertifications are in place.

- **Remote Access Controls**

Remote access to Sprinklr's backend systems is restricted to selective and authorized personnel based on their role. The access follows the principle of least privilege and a multi-tiered security protocol which includes employees with backend access to connect to the bastion host through Sprinklr's VPN which is whitelisted. Once authenticated, SSH is utilized to access the server. Username and password are required as the next step and two factor authentication as the final step**.** Device validation is performed during sign on.

- **Communication Controls**

Sprinklr verifies and establishes the parties to which personal data have been or may be transmitted, or otherwise made available. Subprocessors used by Sprinklr are initially - and afterwards periodically - assessed for data security and privacy practices consistent with Sprinklr's own data security and privacy practices. Sprinklr does not sell, furnish, or otherwise share Customer data without the consent of the Customer or the data subject, as applicable.

- **Input Controls**

Sprinklr limits, monitors, and logs where applicable how data is entered into our systems. Standard software development security controls are in place to sanitize potentially harmful external input. This includes industry standard controls designed to prevent the introduction or spread of malicious software ("Malware").

- **Processing Controls**

All processing by Sprinklr is conducted on behalf of and at the instruction of the Customer. Processes and technical controls in place to enforce this are reviewed on a periodic basis.

- **Availability Controls**

All data critical for the operation of Sprinklr's Platform, as well as Customer data, is protected by multiple controls to ensure continuous protection of such data such as runtime mechanisms including redundant storage of operational data and multiple backups (with the exception of Sprinklr Services that, by design, do not persist Customer data), and other industry standard controls as applicable.

Personnel Security and Training

Sprinklr requires that all employees complete a successful background check prior to beginning their employment at Sprinklr. Subject to local appliable laws, such background checks assess:

- Criminal history
- Prior Employment verification
- Education Verification
- Social Security Verification
- National Sex Offender Registry
- Global Sanctions & Enforcement
- Physical Address Verification

Employees also undergo mandatory security awareness training upon hire and at least annually thereafter.

Application Security and Vulnerability Management

Sprinklr has a rigorous security testing and vulnerability management program in place. Application level and infrastructure level penetration testing is performed using an external party on an annual basis and identified vulnerabilities are remediated in accordance with Sprinklr's vulnerability management standard using the following timeline:

Rating	Remediation Timeline
Critical	7 Days
High	30 Days
Moderate	90 Days
Low	180 Days

Sprinklr follows a Secure Development Lifecycle ("SDL") process based on industry standard guidelines and practices. Sprinklr follows a risk-based approach to identify security issues in SDL for major code releases utilizing a combination of periodic static testing, dynamic testing, and other techniques as appropriate. Identified issues are managed by the Security Team. Developers undergo secure code training which incorporates OWASP Top 10 guidelines. Source code management and deployment follow segregation of duties and least privilege principles. Sprinklr maintains separate environments for development, testing, QA, and production. Production data is not stored or used in testing environments.

Tools or techniques used to assess security or attack computer systems or networks (i.e. vulnerability scanners, port scanners, penetration tools, etc.) without Sprinklr's authorization are strictly prohibited.

Incident Response

Sprinklr maintains an Incident Response Plan ("IR Plan") that is managed by a dedicated team and reviewed and tested annually. IR training is conducted at least once a year. Identified incidents are assigned a severity level, triaged, and managed through resolution, as well as post-mortem, where needed based on the severity of the incident. The IR Plan defines response times according to incident severity level, roles and responsibilities, and incident declaration procedures. Depending on the severity level, the IR Sprinklr's Crisis Management Team, which includes Sprinklr Legal and Communications teams, as well as other relevant stakeholders across the company to support risk assessments, devise and execute on remediation plans, provide ongoing monitoring of issues, and communicate, where needed, with customers in accordance with the notification provisions of the Agreement and DPA. Notifications for personal data breaches are governed by Sprinklr's DPA.

Data and Systems Recovery

Production systems and services are implemented to achieve a Recovery Time Objective (RTO) of 24 hours with a Recovery Point Objective (RPO) of 24 hours. The associated processes are periodically reviewed and tested where applicable.

Integrity

Sprinklr has implemented protective controls designed to ensure that stored data cannot be corrupted by means of a malfunctioning of the system. Such controls include system redundancy, cryptographic hashing, checksumming, and other industry standard measures as applicable. Once data is entered into our systems, Sprinklr has appropriate development and operational controls to ensure the data quality of our systems.

Secure Configuration

Sprinklr leverages industry standard security baseline definitions and vendor best practices to ensure suitable secure configuration of Sprinklr production environments. Unused services are turned off and blocked. Configurations are reviewed and updated periodically by operational staff and the Security Team. These include suitable configurations for event logging and monitoring, which are alerted to the Network Operation Center ("NOC"), the Security Team, and other operational staff.

Endpoint Protection

Sprinklr is cloud based and Customer data is stored on an isolated cloud instance Storage of Customer data on employee devices is prohibited. Sprinklr employees laptops are pre-configured and centrally managed by Sprinklr's IT Team. The pre-configuration includes endpoint detection and response and antivirus agent, full disk encryption, read only USB, inactivity logout, minimum 16-character password, firewall, and revoked administrative rights. Connection to Sprinklr's backend systems is restricted to corporate issued laptops.

Penetration Testing

Any audit terms negotiated between the parties in the Agreement or data protection terms do not apply to penetration testing by the Customer. Requests for penetration testing must be in writing to the customer success manager and customerpentesting@sprinklr.com at least thirty (30) days in advance. Following receipt of such a request, Sprinklr will provide terms of engagement for the Customer to complete. Penetration testing is not permitted without Sprinklr's prior written approval, which may be denied at Sprinklr's sole discretion, following Customer's submission of the terms of engagement. Such approval must come from an authorized member of Sprinklr's Security Team, and any other approval shall not be valid. Within fifteen (15) days of Sprinklr's approval, Sprinklr will use all commercially reasonable efforts to set up an application test environment for Customer to carry out penetration testing. Customer should in no circumstance proceed with penetration testing unless penetration testing has been approved and the application test environment has been established. Even when a Customer request for penetration testing is approved, the following types of testing are strictly prohibited: network/infrastructure testing, social engineering (people testing), and ancillary systems. The results of Customer penetration testing must be shared with Sprinklr within 24 hours by emailing the same to customerpentesting@sprinklr.com. Such results are strictly confidential and shall not be shared with anyone other than Sprinklr, the Customer, and the penetration tester.

D. 2021 EU STANDARD CONTRACTUAL CLAUSES

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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.

Data exporting organisation

Name:	As set out in Part B (***Data Processing Details***).
Address:	As set out in Part B (***Data Processing Details***).
Tel./fax/e-mail:	As set out in Part B (***Data Processing Details***).
Customer enters into these Standard Contractual Clauses on behalf of itself and in the name and on behalf of its Affiliates	
hereinafter the "data exporter"	

Data importing organisation	
Name:	As set out in Part B (***Data Processing Details***).
Address:	As set out in Part B (***Data Processing Details***).
Tel./fax/e-mail:	As set out in Part B (***Data Processing Details***).
hereinafter the "data importer"	

each a "party"; together "the parties",

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 personal 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.

[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 of 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 [...].

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: 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

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.

MODULE TWO: Transfer controller to processor

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 benefiting 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 defense 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.

[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.

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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase the data.

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located

outside the European Union[4] (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 benefiting 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 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defense 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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

MODULE TWO: Transfer controller to processor

(a) 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 thirty (30) days 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.[5] The Parties agree that, by complying with this Clause, the data importer fulfills 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.

---

[4] 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 purposes of these Clauses.

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

(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 fulfill 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.

MODULE THREE: Transfer processor to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.[6] The Parties agree that, by complying with this Clause, the data importer fulfills 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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 fulfill 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

MODULE TWO: Transfer controller to processor

(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.

MODULE THREE: Transfer processor to processor

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

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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.

[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 behavior 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];

(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.

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 fulfill 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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

[7] 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.

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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) [For Modules Two and Three: 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 Germany.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 Hamburg, Germany.

(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.

ANNEX I - List of Parties and Description of Transfers

A. LIST OF PARTIES

As set out in Part B **(*Data Processing Details*).**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set out in Part B (*Data Processing Details*).

Categories of personal data transferred

*As set out in Part B (**Data Processing Details**).*

Sensitive Data Transferred (if applicable)

As set out in Part B (*Data Processing Details*).

The Frequency of the Transfer *As set out in Part B (**Data Processing Details**).*

Nature of the Processing

As set out in Part B (*Data Processing Details*).

Purpose(s) of the Data Transfer and Further Processing

As set out in Part B (*Data Processing Details*).

The Period for which the Personal Data will be Retained, or, if that is not Possible, the Criteria Used to Determine that Period

As set out in Part B *(**Data Processing Details*).**

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

Sub-processors used by the data importer throughout the entire duration of the DPA to provide its contractual services as of the effective date of the DPA, including their role and scope of sub-processing and the geographical area of sub-processing are set out in Section 11 of the DPA and in Annex III, below.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be Customer's supervisory authority, as defined in Clause 13(a) of the SCCs. Customer shall maintain up-to-date records of the applicable member state and supervisory authority and make such records available to Sprinklr upon request.

ANNEX II - Technical and Organizational Measures

As set out in Part C (*Enterprise Security Addendum*), above.

ANNEX III - List of Sub-processors

Sprinklr's current List of Subprocessors can be accessed at www.sprinklr.com/legal, and Sprinklr has Customer's general authorization for use of these Subprocessors. Sprinklr will inform the Customer via electronic means of any changes to that list in the event Subprocessors are added or replaced during the term of the Agreement in accordance with Clause 9(a), Option 2 and the process set out in Section 11 of the DPA.

E. UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

The Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, which went into effect on 21 March 2022.

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start Date	as per Agreement	
The Parties	**Exporter (Who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties Details	As set out in Part B (*List of Parties and Data Processing Details*).	As set out in Part B (*List of Parties and Data Processing Details*).
Contact Person's name, position, and contact details	As set out in Part B (*List of Parties and Data Processing Details*).	As set out in Part B (*List of Parties and Data Processing Details*).

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum to EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	**Module in Operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9(a) (Prior Authorization or General Authorization)**	**Clause 9(a) (Time Period)**	**Is personal data received from the importer combined with Personal Data Collected by Exporter**
1						
2	X	Yes	No	General Authorization	30 days	
3	X	Yes	No	General Authorization	30 days	
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: see Annex I(A) of the 2021 EU SCCs, above
Annex 1B: Description of Transfer: see Annex I(B) of the 2021 EU SCCs, above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see Annex II of the 2021 EU SCCs, above
Annex III: List of Sub processors (Modules 2 and 3 only): see Annex III of the 2021 EU SCCs, above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum Changes	Which Parties may end this addendum as set out in Section 19: {X} Importer (X) Exporter () neither party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act on 2 February 2022, as it is revised under 18 of those Mandatory Clauses.