29 West 35th Street, 7th Floor
New York, NY 10001

Data Processing Addendum

In the course of providing its services to Customer, Sprinklr may Process Personal Data on behalf of Customer. This Data Processing Addendum ("DPA") reflects the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Legislation. This Data Processing Addendum ("DPA") is incorporated by reference as part of the Master Services Agreement (or other agreement for the purchase of Sprinklr's services, hereinafter collectively "MSA") between Customer and Sprinklr

This DPA reflects the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Legislation. This DPA shall not replace any additional rights relating to Processing of Personal Data previously negotiated by Customer in the MSA.

This DPA will terminate automatically upon termination of the MSA, or as earlier terminated pursuant to the terms of this DPA.

This DPA consists of two parts:

A. **Data Processing Terms**
B. **Modernised Standard Contractual Clauses (version 4th June 2021)**

A. DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

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

"Data Protection Legislation" means all laws and regulations, including laws and regulations applicable to the Processing of Personal Data under the MSA.

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

"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.

"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.

"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; where the entity Processes the Personal Data pursuant to the Controller's instructions and solely to provide the Services.

"Services" shall mean Sprinklr's customer experience and social media management platform, provided as SaaS, and any required, usual, appropriate or acceptable activities relating to the Services, including without limitation to (a) carry out the Services or the business of which the Services are a part, (b) carry out any benefits, rights and obligations relating to the Services, (c) maintain records relating to the Services, or (d) comply with any legal or self-regulatory obligations relating to the Services.

"Sub-processor" means any Processor engaged by Sprinklr or a Sprinklr Affiliate.

"Users" shall mean Customer', Customer's Affiliates' and Customer's contractors' employees, entitled to use the Services under the MSA.

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** which, determines the purposes and means of the Processing of Personal Data, **is the Controller**.

Where Customer is acting as Controller, Module 2 (Transfer controller to processor) of the Modernised Standard Contractual Clauses in Part B shall apply.

Where Customer Affiliate(s) is/are acting as Controller(s), Module 3 (Transfer processor to processor) of the Modernised Standard Contractual Clauses in Part B shall apply.

2.2 The parties shall each comply with their respective obligations under the Data Protection Legislation. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Legislation.

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 Sprinklr shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for purposes of (i) Processing for business purposes, in accordance with the MSA; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer, as further set out in Sprinklr's published privacy policies. Sprinklr agrees that it shall not sell any Personal Data.

2.5 Sprinklr shall take reasonable steps to instruct and train any of its and/or its Sub-processors' employees who have access to Personal Data to maintain the confidentiality and security of the Personal Data, and shall limit access to Personal Data on a need-to-know basis.

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 right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("DSR Request").

3.2 Taking into account the nature of the Processing, Sprinklr shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment 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 Services, does not have the ability to address a DSR Request, 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.

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, 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.

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. 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.

5.2 Sprinklr shall make reasonable efforts to identify the cause of a Personal Data Breach and take those steps as Sprinklr deems necessary and reasonable in order 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 herein shall not apply to incidents that are caused by Customer.

6. SECURITY AND OTHER SUPPLEMENTARY MEASURES

Sprinklr shall maintain technical and organizational measures designed to protect the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data. Where Personal Data is transferred to a country which does not ensure a level of protection essentially equivalent to that guaranteed within the European Union and where the EU standard of essential equivalence cannot be achieved through the measures set out in Appendix 2, the Parties shall adopt and implement supplementary measures as required for compliance with regulations of the European Data Protection Board (hereinafter "Supplementary Measures"). As part of such Supplementary Measures, Sprinklr agrees not to allow, unless required by law, regulations,

order of a court or any regulatory, judicial, governmental or similar body or authorized by Customer, access to Customer Personal Data (excluding any publicly available data) by any administrative body, authority or agency. Customer acknowledges that Sprinklr may be required by law to allow such access to Customer Personal Data. Before Sprinklr discloses any such Customer Personal Data, 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 Personal Data 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 Modernised Standard Contractual Clauses.

7. DELETION OR RETURN OF PERSONAL DATA

7.1 Sprinklr shall delete the Personal Data upon termination/expiry of the MSA as specified in the MSA or upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by the applicable laws and always provided that Sprinklr shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

7.2 Sprinklr shall return Personal Data to Customer in accordance with the procedure and timeframe specified in the MSA.

8. AUDITS AND INSPECTIONS

8.1 Sprinklr shall make available to Customer all 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. 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 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.

8.2 To the extent applicable Data Protection Legislation requires Sprinklr to submit to such an audit, Customer or Auditor may, at Customer's expense and not more than once per year, perform an on-site inspection of Sprinklr's data protection and information security practices and policies with written notice reasonably, but at least fifteen (15) business days, in advance. The inspection shall take place over not more than one day 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 inspection. Due to confidentiality and security requirements, such inspections shall exclude on-site inspections of multi-tenant environments (such as IaaS data centres or other shared services used by Sprinklr). On-site examinations of such environments can be substituted by detailed 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. Examinations performed via online video-sharing conferencing tools (such as Google Meet or Zoom) are considered to be on-site examinations.

8.3 Notwithstanding Sprinklr's obligations under Section 8.2., 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 agrees to accept such report in lieu of requesting an audit – as set out in Section 8.2 -- of such controls or measures.

8.4 Customer shall promptly notify Sprinklr of any non-compliance discovered during such an audit/inspection. All information provided to Customer or Auditor during such an audit or inspection is considered Sprinklr confidential information.

9. LIABILITY

9.1 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 under the MSA, 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 MSA and all DPAs together.

9.2 For the avoidance of doubt, Sprinklr's total liability for all claims from the Customer and all of Customer's Affiliates arising out of or related to the MSA and each DPA shall apply in the aggregate for all claims under both the MSA and all DPAs established under this Agreement, including by Customer and all Customer's Affiliates, 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.

9.3 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.

10. INTERNATIONAL PERSONAL DATA TRANSFERS

10.1 Sprinklr Processes Personal Data in various jurisdictions, including the United States.

10.2 The attached Standard Contractual Clauses shall apply to any transfers of Personal Data under this DPA from the

European Economic Area and/or their member states, Switzerland and the United Kingdom 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.

10.3 In the event of any conflict or inconsistency between these Data Processing Terms and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

B. 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:	Customer name as per MSA
Address:	Customer address as per MSA
Tel./fax/e-mail:	As per MSA
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 organization	
Name:	Sprinklr, Inc. (including its Affiliates)
Address:	29 West 35th Street, New York, NY 10001, USA
Tel./fax/e-mail:	+1-917-933-7800; fax: n/a; e-mail: privacy@sprinklr.com
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.

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); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(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); Module Four: Clause 18.

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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 [(5)].

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.

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 [6] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter 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 as long as the period stated in Annex III 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. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

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 at least as long as the period stated in Annex III 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. [(9)] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's 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 fulfil its obligations under that contract.

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

Clause 10

Data subject rights

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

(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 behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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 authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(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 fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [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.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority [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 One, 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

---

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

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) 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.

(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 purpose of these Clauses.

(5) 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.

(6) 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.

(7) This includes whether the transfer and further processing 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 or offences.

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

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

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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

(12) 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.

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 MSA

Address: ...Customer address as per MSA

Contact person's name, position and contact details: ...Customer contact as per MSA

Activities relevant to the data transferred under these Clauses: Customer Experience Management including Social Media Management

The data exporter is a licensee and user of the Sprinklr Platform.

Signature and date: ...As per MSA

Role (controller/processor): As per section 2.1 of this DPA.

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

Name: **Sprinklr, Inc.**

Address: 29 W. 35th Street, New York, NY 10001, USA

Contact person's name, position and contact details: Sprinklr DPO: 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.

Signature and date: ...As per MSA

Role (controller/processor): **processor**

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

1. Data subjects include individuals collaborating and communicating with the data exporter's customers, followers, fans and other Internet users who use social networks and websites and data exporter's employees, data exporter's agents and data exporter's subcontractors' employees operating the Sprinklr Platform ("Account Information").
2. The personal data transferred may also concern the data exporter's customers, prospects, marketing addressees etc. uploaded/imported by data exporter into the Sprinklr Platform ("Customer Content").
3. The personal data transferred may also concern the data exporter's customers, followers, fans and other Internet users who use social media networks and websites, blogs & blog comments, mainstream news sources and forums, and websites owned by the data exporter where the data importer provides social and content management functionality on the data exporter's behalf ("Social Data").

Categories of personal data transferred

The personal data transferred concern the following categories of data:

1. Account Information transferred includes identification data (name, login), contact information (business email address) and work related information (usage/performance data, social contact handling data).
2. Customer Content transferred includes any category of personal data the data exporter uploads/stores into the Sprinklr Platform.
3. Social Data transferred includes content published or sent by social media users via data exporter's social media profiles (e.g. data exporter's Facebook page), connected to the Sprinklr Platform (both public and private messages to data exporter) and publicly accessible data from the social media networks and websites based on certain search queries (e.g. #customer), defined by the data exporter. Social Data includes user/add IDs, social network profile names and information, social network communications and all types of information shared across social media networks and websites, including, where applicable under the relevant Order Form, voice data (not to be used for identification or authentication purposes).

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

The personal data transferred may include the following special categories of data:

1. Customer Content transferred may contain special categories of data, depending on what kind of data the data exporter uploads/stores into the Sprinklr Platform.
2. Social Data transferred may concern special categories of personal data, depending on data exporter's usage of the Sprinklr Platform (e.g. definition of specific search queries for collection of publicly accessible personal data on the social media networks).

Sprinklr treats all Customer Data as highly sensitive and applies a consistent protection framework across such Customer Data. The overall level of protection employed is consistent with the requirements for protecting sensitive data.. Controls include (i) address physical and logical access limitation based on a need-to-know principle; (ii) usage exclusively for providing the 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.

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

Continuous.

Nature of the processing

Sprinklr is processing, storing, collecting, recording, disclosing by transmission and erasing personal data as a data processor in order to provide its services as contracted in the MSA in accordance and only on Customer's instructions.

Purpose(s) of the data transfer and further processing

The personal data transferred will be subject to the following basic processing activities (please specify):

1. Account Information that is transferred will be processed solely for the purpose of operating the Sprinklr Platform (authentication, login and audit trail)
2. Customer Content and Social Data that is transferred will be processed for purposes of social media management, including social media listening and analytics, customer care and support, marketing analytics and marketing management.

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

Sprinklr shall delete the Personal Data upon termination/expiry of the MSA as specified in the MSA or upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by the applicable laws and always provided that Sprinklr shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

Sprinklr shall return Personal Data to Customer in accordance with the procedure and timeframe specified in the MSA.

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 Annex C.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

...Depending on the Customer address stated in the MSA

ANNEX II

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

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

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

Security Program

Sprinklr has a dedicated Security Team chartered to define, supervise implementation, and monitor all relevant security and privacy policies, standards, and controls. The team is supported by Sprinklr's Board of Directors and the Executive Leadership Team. Periodic tests by independent third parties (such as third-party auditors, assessors, penetration testers, etc.) are organized and conducted under the guidance of the Security Team. Remediation of any material findings is tracked and validated. These tests include the validation of administrative, procedural, and technical controls. The Security Team maintains a Security Manual which provides implementation details for all applicable security and privacy controls.

Organizational Alignment and Accountability

The Security Team is independent from Sprinklr's Research & Development team, the IT team, and other operational teams. By independently validating the implementation of application security controls and reporting the outcome to Senior and Executive Leadership, the Security Team ensures proper accountability and a risk-informed decision process for maintaining and evolving the security program.

Equipment Access Control

For all production systems, Sprinkler relies on our public cloud provider capabilities to protect servers, networks, and facilities from unauthorized access. Typical 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 3rd party security audit reports and/or vendor audits.

Data Media Control

All media containing sensitive data is protected from unauthorized physical access. Where applicable, data at rest is encrypted using current encryption mechanisms. Cryptographic keys are managed by Sprinklr in accordance with industry standard practices. Generally, mobile media or devices do not contain Customer Data.

Storage Control

Sprinklr prevents the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored data through appropriate security controls. These include: (i) industry standard application security processes during development, testing, and deployment; (ii) secure operations implementing least privilege access and multi-factor authentication; (iii) vulnerability management; and (iv) ongoing security monitoring.

User Control (Authentication)

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

Data Access Control (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.

Communication Control

Sprinklr verifies and establishes the parties to which personal data have been or may be transmitted or made available. Subprocessors used by Spinklr 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 or other covered sensitive data without the consent of the Customer or the data subject, as applicable.

Input Control

Sprinklr limits, monitors, and logs where applicable how data is entered into our systems. This includes industry standard controls designed to prevent the introduction or spread of malicious software or other code ("malware"), including viruses, trojans, ransomware, root kits, etc.

Transport Control

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

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.

Reliability

Sprinklr has implemented controls to ensure continued operations. Production systems have high-availability capabilities implemented which allow to dynamically address partial systems failures while maintaining 99.5% service uptime.

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.

Processing Control

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

Availability Control

All data critical for the operation of Sprinklr's services including sensitive and Customer Data are protected by multiple controls to ensure continuous protection of such data. These controls include runtime mechanisms including redundant storage of operational data, multiple backups, and other industry standard controls as applicable.

Purpose Limitation

All data is collected and processed for specific purposes. Personal data or data derived from personal data collected for a specific purpose is not used for other purposes without permission from the Customer or the data subject, as applicable. Production data is not used for testing or development purposes unless explicit permission is given.

Data Minimization

Sprinklr minimizes personal and sensitive data processing and storage. Data is only processed or stored if needed to meet Customer or Sprinklr business requirements. Whenever technically, legally, and commercially possible, Sprinklr will use anonymization or pseudonymization techniques such as redacting personal information from transactional data.

Secure Configuration

Sprinklr leverages industry standard security baseline definitions (such as Center for Internet Security Benchmarks) 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. This include suitable configurations for event logging and monitoring, which are alerted to the Network Operation Center (NOC), the Security Team, and other operational staff.

Data Retention

Customer defines the data retention timelines by selecting the appropriate support package, as defined in the MSA and the Statement of Work. Sprinklr does not retain Customer Data beyond the contracted expiration time, unless obligated under different laws and regulations (such as financial accounting rules).

Data Subject Rights

Sprinklr continuously monitors our obligations under all applicable privacy laws and regulations. Data Subject rights (such as erasure, data portability, etc.) are implemented through technical and administrative processes. As processor, Sprinklr will ensure that Data Controllers can implement all relevant Data Subject processes.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

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

The controller has authorised the use of the following sub-processors: Not applicable as the parties have opted for Option 2, General written authorisation.

Sprinklr's current List of Sub-Processors is located at www.sprinklr.com/legal and Customer hereby consents to Sprinklr's usage of these Sub-Processors. Sprinklr will specifically inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors in accordance with Clause 9(a), Option 2 and the process set out in the List of Sub-Processors.