STANDARD CONTRACTUAL CLAUSES (NEW TRANSFER SCCs – MODULE 3)

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 (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 (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.

(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) Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

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

(v) Clause 13;

---

[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.

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

(vii) Clause 16(e);

(viii) Clause 18 – Module 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

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

(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

(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 THREE - 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 exporter2.

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

[2] 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.

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 Union3 (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 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 [Specify time period] 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).

---

[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 purposes of these Clauses.

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.4 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 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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body (11) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it or follow a particular sequence in seeking redress.]

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

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

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

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

(b) 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.

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

---

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

(d) 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 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 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 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 0, they have taken due account in particular of the following elements:

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

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

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

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

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

(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 0, 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 0.

(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.

---

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

CLAUSE 15

OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES

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. [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 of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

CLAUSE 17

GOVERNING LAW

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 (specify Member State).]

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

CLAUSE 18

CHOICE OF FORUM AND JURISDICTION

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 Ireland.

(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.

Any dispute arising from these Clauses shall be resolved by the courts of (specify country) sufficient clarity, separate appendices should be used.

ANNEX I

(A) LIST OF PARTIES

Data exporter(s):

1 Name: [Relevant local MicroStrategy/Strategy legal entity contracting with customer/data controller]

Address: [local MicroStrategy/Strategy legal entity address]

Contact person's name, position and contact details: Global Data Privacy Officer; privacy@strategy.com

The local Strategy legal entity contracting with customer/data controller is the data exporter of personal data processed under the relevant master agreement and Data Processing Addendum in force with the customer/data controller.

Data importer(s):

1 Name: Strategy Inc and MicroStrategy Services Corp. d/b/a Strategy

Address: 1850 Towers Crescent Plaza, Tysons Corner, Virginia 22182

Contact person's name, position and contact details: Global Data Privacy Officer; privacy@strategy.com

Strategy is the data importer and processor and provider of the services and/or products provided under the relevant master agreement and Data Processing Addendum in force with the customer/data controller.

(B) DESCRIPTION OF TRANSFER

Categories of personal data transferred

Data controller (customer) may submit personal data to the cloud hosted MCE service or in connection with the provision of technical support or consulting services, the extent of which is determined and controlled by the data controller in its sole discretion, and which may include, but is not limited to personal data concerning the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of the data exporter's prospects, customers, business partners and vendors
- Employees or agents of the data exporter, including those who have been authorized to use the cloud hosted service
- Data exporter's users authorized by data exporter to use the cloud hosted service

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

On a one-off basis in connection with each technical support case raised by customer or on continuous basis throughout the term of the master agreement, due to the nature of the hosted cloud MCE service.

Nature of the processing

Storage, back-up and recovery and processing in connection with a technical support case, provision of consulting services, and/or the provision of the hosted cloud MCE Service, in connection with the performance of the cloud hosted services pursuant to the master agreement and DPA.

Purpose(s) of the data transfer and further processing

The objective of processing of personal data by the data importer is the performance of the cloud hosted service or in connection with the provision of technical support or consulting services pursuant to a governing agreement and includes:

- Storage and processing through the hosted cloud MCE service
- Processing in connection with a technical support case
- Processing in connection with providing consulting services

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

For the subscription term for hosted cloud MCE service and/or technical support services as agreed upon in the master agreement with the customer.

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

Strategy uses certain third-party sub-processors to fulfil its contractual obligations to its customers or to provide certain services on its behalf. Information regarding the sub-processors that are currently engaged to carry out specific processing activities can be found here:

- https://community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors
- https://community.microstrategy.com/s/article/GDPR-Technical-Support-Sub-Processors
- https://community.microstrategy.com/s/article/GDPR-Consulting-Sub-Processors-List

For its offered products and services, Strategy uses cloud service providers including Amazon Web Services (AWS), Microsoft Azure, or other such providers it may use in the future, for aspects of Strategy's data center hosting, infrastructure, and managed services. Strategy customer environments are hosted in data centers run by these cloud service providers, with which Strategy has entered into GDPR-specific Data Processing Addendums that mirror the terms of Strategy's own customer-facing Data Processing Addendum.

In addition, in providing Technical Support and/or Consulting Services, Strategy may utilize customer management or technical collaboration software platforms such as Salesforce, ServiceNow or Rally in order to temporarily store personal data in order to resolve a support case initiated by, or to provide the requested consulting services to, its customers.

(C) COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II

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

The technical and organisational security measures implemented by Strategy are as described in and will be implemented in accordance with the terms of a master agreement currently in effect between Strategy and the customer, or if one does not exist, by the Strategy Cloud Environment (MCE) Service Guide, Technical Support Policy and Procedures, and/or the Terms and Conditions listed at www.strategysoftware.com/legal/contract-hub on the effective date.

In addition, below are generally Strategy's current technical and organizational security measures to protect the confidentiality, integrity and availability of personal data with Strategy's products and services. Strategy may change these measures at any time without notice so long as it maintains a comparable or better level of security.

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.

This Annex provides Strategy's current technical and organizational security measures to protect the confidentiality, integrity and availability of personal data with Strategy's products and services. Strategy may change these measures at any time without notice so long as it maintains a comparable or better level of security.

- Measures of pseudonymisation and encryption of personal data
    - Strategy requires that personal data is encrypted at rest and in transit. This can be achieved through application-level encryption, filesystem encryption or hardware-based encryption at a storage media level.
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - Strategy has established processes that incorporate security into the evaluation of a vendor, system, or service to ensure the confidentiality, integrity and availability of its data.
    - Strategy has established rules of behaviour that are documented in its Acceptable Use Policy. The Strategy Acceptable Use Policy provides common rules on the appropriate use of all Strategy information technology resources for all users, including employees, interns, and contractors.
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
    - Strategy has taken steps to ensure its business continue to operate, even during a disaster disrupting normal mode of operation. Critical systems and services have been identified and regular exercises are being held to ensure that personnel are prepared in the event that disaster recovery procedures must be invoked.
    - Backups are completed nightly, ensuring that critical systems can be restored with minimal data loss.
    - Strategy has established incident response procedures, allowing for handling of incidents in a timely and controlled manner and in accordance with applicable law and obligations.
    - Strategy has defined contingency plan(s) for its critical systems. Those plan(s) are tested at least annually and updated as needed.
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Independent third-party audits/certifications:
    - SOC-2: Strategy has an independent accountant firm conduct an annual SOC-2 compliance audit of its Hosted Service, which is available to customers upon request.
    - ISO27001:2013: Strategy has an independent accountant firm conduct an annual ISO27001 recertification of its Hosted Service. The certification letter is available to customers upon request.
- Strategy has contracted with an independent third party to conduct an annual risk assessment of its Hosted Service.
- Vulnerability Scans
    - Strategy has established weekly internal scans of its systems, identifying security vulnerabilities that need to be addressed.
    - Quarterly external scans are part of the PCI-DSS compliance efforts, to identify if there are any remotely exploitable vulnerabilities, in the Hosted Service, accessible from the Internet.
- Independent third-party pen-test: Semi-annual pen-tests are performed as part of the PCI-DSS compliance efforts of the Hosted Service.
- Internal Security Assessments
    - Strategy conducts Health Insurance Portability and Accountability Act (HIPAA) self-assessments at least annually.
    - Strategy performs an annual self-assessment for PCI-DSS compliance of its Hosted Service.
- Risk Assessment: Strategy conducts independent third-party risk assessments at least annually for its Hosted Service.

- Measures for user identification and authorisation
    - Strategy has established Identification and Authentication Policy and Procedures for its critical systems.
    - Strategy has implemented physical access controls at all of our offices, requiring employees and onsite contractors to authenticate before entering the premises or special sections in the office. Third party hosting providers are required to provide evidence that physical access control requirements are met.
    - Strategy has implemented system access control for all systems that are not for public access. Access control includes the usage of a username and a complex password and, with critical systems, multifactor authentication leveraging one-time credentials.
    - Strategy has implemented network access control at all the ingress and egress network points. All network traffic is denied by default. Only traffic that meets an access control rule is allowed into the corporate network.
- Measures for the protection of data during transmission
    - Strategy requires that data is encrypted during transit by leveraging common industry protocols as Transport Layer Security (TLS) or Virtual Private Networks (VPN).
    - Encrypted communication is used for all sensitive communication between systems.
- Measures for the protection of data during storage
    - Strategy requires that data is encrypted during storage by leveraging common industry protocols such as AES-256bit level of encryption.

- Encrypted storage of sensitive information is available for customers of the Hosted Service, ensuring the confidentiality of their data.

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

  - Strategy requires that its data center hosting providers meet at a minimum SOC-2 and ISO27001 requirements. Hosting providers that host systems storing or processing regulated customer data (e.g., Protected Health Information (PHI) or card holder data) are required to have additional attestations in place, ensuring compliance and alignment with laws, regulations and business needs.

  - Strategy uses Public Cloud service providers, e.g. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as Sub-Processors providing the Hosted Service. The Public Cloud service providers meet SOC-2, ISO27001, HIPAA and PCI-DSS requirements. Each year Strategy requests the Public Cloud service providers to provide updated documentation that demonstrate their compliance with those security standards/frameworks.

- Measures for ensuring events logging

  - Critical log events have been identified for all critical systems. These critical log events include information that is meaningful in identifying security incidents.

  - A third-party 24x7 monitoring services conducts log reviews, analysis and reporting and notifies Strategy in case suspicious events are identified.

  - Strategy has installed file integrity monitoring on critical systems. Any unauthorized change of files monitored would be detected and investigated.

  - Logs for critical systems are maintained according to the retention time required by law, regulation, business need or standard best practice.

- Measures for ensuring system configuration, including default configuration

  - Strategy has established secure baseline configuration for its critical systems. Baselines are reviewed and updated as new security threats or needs are identified.

  - Hardening of systems is part of the deployment of new critical systems.

  - Strategy has established a configuration management plan that identifies tools, methods, and processes on how changes are being implemented with its critical systems.

- Measures for internal IT and IT security governance and management

  - Strategy has defined an IT governance program that addresses security. It establishes “security gates” with projects, ensuring that requirements and design address potential security threats.

- Measures for certification/assurance of processes and products

  - Strategy has established change control processes for its critical systems. Every change request must be reviewed for impact, back-out procedure and approved by the Change Control Board (CCB).

- Measures for ensuring data minimisation

  - Data minimisation is conducted on a regular basis with systems or when deemed necessary to ensure only the minimum amount of necessary data is retained.

- Measures for ensuring data quality

  - File integrity monitoring is used to ensure that critical systems are protected from unauthorized changes by users or malicious code.

  - Malicious code protection uses a next generation based third party vendor solution that identifies malicious behaviour and allows roll-back of any actions taken.

- Measures for ensuring limited data retention

    - Data is retained on systems only for as long as deemed necessary to ensure system operability or as determined by contractual agreement.

- Measures for ensuring accountability

    - Strategy adjusts access rights of personnel whenever they are transferred or assume different responsibilities.

    - Strategy revokes all access of employees upon termination.

- Measures for allowing data portability and ensuring erasure

    - Strategy has established Digital Media Handling Procedures addressing media access, media marking, media storage, media transport and media sanitization.

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

Strategy may use its own affiliated companies as sub-processors for the purposes of providing its products and services to its customers. Strategy's affiliated companies use many of the technical and organizational security measures described above to protect the confidentiality, integrity and availability of personal data. In addition, Strategy uses certain third-party sub-processors to fulfill its contractual obligations to its customers or to provide certain services on its behalf. Information regarding the specific technical and organizational measures taken by Strategy's sub-processors can be found at the following Strategy websites, which list its sub-processors that are currently engaged to carry out specific processing activities:

- https://community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors

- https://community.microstrategy.com/s/article/GDPR-Technical-Support-Sub-Processors

- https://community.microstrategy.com/s/article/GDPR-Consulting-Sub-Processors-List

ANNEX 3 TO THE STANDARD CONTRACTUAL CLAUSES

LIST OF SUB-PROCESSORS

MODULE THREE: Transfer processor to processor

The Parties agree to use "Option 2" in clause 9(a) of the SCCs (i.e., Company's general written authorization for the engagement of Vendor's Subprocessors from an agreed list).

The controller authorizes the use of the following sub-processors:

1. **Name: MicroStrategy Services Corporation d/b/a Strategy**
   Address: 1850 Towers Crescent Plaza, Tysons Corner, VA 22182
   Contact person's name, position and contact details: privacy@strategy.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): MicroStrategy Services Corp. d/b/a Strategy is a U.S.-based subsidiary that manages technical support and consulting services for the company and serves as the data importer for any personal data transferred during the course of the provision of these services.

2. **Name: MicroStrategy Poland Sp. z o.o**
   Address: Skyliner Building, 22nd floor, Prosta 67, 00-838 Warszawa, Poland
   Contact person's name, position and contact details: privacy@strategy.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): MicroStrategy Poland Sp. z o.o is a Poland-based subsidiary, that provides cloud support, technical support and consulting services for the company and may process personal data in onward transfers during the course of the provision of these services.

3. **Name: MicroStrategy Brasil Ltda. Sucursal Argentina**
   Address: Av. Leandro N. Alem 1134 - Floor 13, Ciudad Autónoma de Buenos Aires, C1001AAT
   Contact person's name, position and contact details: privacy@strategy.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): MicroStrategy Brasil Ltda. Sucursal Argentina is a branch office of MicroStrategy subsidiary, MicroStrategy Brasil, located in Argentina that provides technical support and consulting services for the company and may process personal data in onward transfers during the course of the provision of these services.

4. **Name: MicroStrategy China Technology Center Ltd.**
   Address: Floor 7, Building A, Huang Long Knowledge City, No. 77 Xue Yuan Lu, Xihu District, Hangzhou, China
   Contact person's name, position and contact details: privacy@strategy.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): MicroStrategy China Technology Center Ltd. is a China-based subsidiary that provides technical support services for the company and may process personal data transmitted by customer as part of a technical support case requiring an onward transfer to MicroStrategy China for resolution.

5. **Name: MicroStrategy India Pvt Ltd.**
   Address: 3A116, WeWork Enam Sambhav, C-20, G Block Rd, Bandra Kurla Complex, Bandra East, Mumbai – 400051
   Contact person's name, position and contact details: privacy@strategy.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): MicroStrategy India Pvt Ltd. is a India-based subsidiary that provides technical support services for the company and may process personal data transmitted by customer as part of a technical support case requiring an onward transfer to MicroStrategy India for resolution.

6. **Name: Amazon Web Services (AWS) – For hosted cloud service only – at choice of data controller**
   Address: 410 Terry Avenue North, Seattle, WA 98109
   Contact person's name, position and contact details: aws-EU-privacy@amazon.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): For its hosted MCE service, Strategy uses cloud service provider AWS for aspects of Strategy's data center hosting, infrastructure, and managed services. Strategy customer environments are hosted in data centers run by these cloud service providers, with which Strategy has entered into GDPR-specific Data Processing Addendums that mirror the terms of Strategy's own customer-facing Data Processing Addendum.

7. **Name: Microsoft Corporation (Azure) - For hosted cloud service only – at choice of data controller**
   Address: One Microsoft Way, Redmond, WA 98052
   Contact person's name, position and contact details: Microsoft EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
   Telephone: +353 (1) 706-3117

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): For its hosted MCE service, Strategy uses cloud service provider Microsoft Azure for aspects of Strategy's data center hosting, infrastructure, and managed services. Strategy customer environments are hosted in data centers run by these cloud service providers, with which Strategy has entered into GDPR-specific Data Processing Addendums that mirror the terms of Strategy's own customer-facing Data Processing Addendum.

   For its Strategy AI service (Auto), Strategy leverages Microsoft's Azure OpenAI service to provide generative AI functionality within the customer's Strategy enterprise software platform environment. Strategy AI is a closed system and the Azure OpenAI service can only query data sources uploaded by the customer, which may or may not include personal data. Interactions with the Azure OpenAI service ensure that no data is retained or employed for model training.

8. **Name: Google LLC (Google Cloud) - For hosted cloud service only –at choice of data controller**
   Address: 1600 Amphitheatre Pkwy, Mountain View, CA 94043
   Contact person's name, position and contact details: dpo-google@google.com

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): For its hosted MCE service, Strategy uses cloud service provider Google Cloud for aspects of Strategy's data center hosting, infrastructure, and managed services. Strategy customer environments are hosted in data centers run by these cloud service providers, with which Strategy has entered into GDPR-specific Data Processing Addendums that mirror the terms of Strategy's own customer-facing Data Processing Addendum.

9. **Name: STACKIT GmbH & Co. KG - For hosted cloud service only –at choice of data controller**
   Address: Stiftsbergstraße 1, 74172 Neckarsulm
   Contact person's name, position and contact details: datenschutz@mail.schwarz

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): For its hosted MCE service, Strategy uses cloud service provider STACKIT for aspects of Strategy's data center hosting, infrastructure, and managed services. Strategy customer environments are hosted in data centers run by these cloud service providers, with which Strategy has entered into GDPR-specific Data Processing Addendums that mirror the terms of Strategy's own customer-facing Data Processing Addendum.

10. **Name: Salesforce.com, Inc.**
    Address: Salesforce Tower, 415 Mission Street, San Francisco, CA 94105
    Contact person's name, position and contact details: privacy@salesforce.com

Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): Salesforce.com is a cloud-based customer relationship management platform utilized by Strategy to manage our relationships and interactions with customers and potential customers. Strategy uses the Salesforce CRM tool to maintain information on our customers including basic business contact information, contractual documents, and key communications.

11. **Name: ServiceNow Inc.**
    Address: 2225 Lawson Lane, Santa Clara, CA 95054
    Contact person's name, position and contact details: privacy@servicenow.com

    Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): ServiceNow is a cloud-based customer support management tool used by Strategy to log, track and resolve technical support cases raised by its customers. ServiceNow is Strategy's automated workflow tool for overseeing and tracking all communications with its customers related to product and technical support issues.

12. **Name: Broadcom Inc. (Rally)**
    Address: 1320 Ridder Park Drive, San Jose, CA 95131
    Contact person's name, position and contact details: Chrystel Cayzac, CA Europe Sarl, data.privacy@broadcom.com

    Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized): Rally is a project management application used internally by Strategy to track the development of technological product features implemented in our products or under consideration for release. The tool is also used to document product defects and the resulting resolution of such defects, as well as document user stories regarding customers' experience with various product features.