General Terms and Conditions for Indirect Qualtrics Services ("GTC")

The below Parties enter into this GTC as of the date signed by the last Party to sign.

Qualtrics, LLC ("**Qualtrics**")

Signature: DocuSigned by: Mark Creer F3B7DF0FFCA34AF...

Name: Mark Creer

Title: Director, Legal Sales

Date: December 5, 2023

Address: Qualtrics, LLC
333 W River Park Dr.
Provo, UT 84604
USA

PagoPA S.p.A. ("**Customer**"):

Signature: MAURIZIO FATARELLA 30.11.2023 15:01:24 GMT+01:00

Name: Maurizio Fatarella

Title: General Manager

Date:

Address: PagoPA S.p.A.
Piazza Colonna 370
00187 Rome,
Italy

qualtrics XM

Exhibit A
Data Processing Agreement

Personal Data Processing Agreement for Qualtrics Services

1. Definitions.

1.1 "**Controller**" means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of Personal Data the purposes of this DPA, if Customer acts as processor for another controller, Customer will, in relation to Qualtrics, be deemed as an additional and independent Controller with the controller rights and obligations under this DPA.

1.2 "**Data Privacy Framework**" means the set of rules set out by or otherwise stemming from the European Commission's adequacy decision for the EU-U.S. of July 10, 2023

1.3 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

1.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein, and Norway.

1.6 **"EU Standard Contractual Clauses"** means the unchanged standard contractual clauses published by the European Commission, reference 2021/914, or any subsequent final version thereof as adopted by Qualtrics. For the avoidance of doubt, Modules 2 and 3 will apply as set out in Section 8.3.

1.7 **"GDPR"** means the General Data Protection Regulation 2016/679.

1.8 **"Personal Data"** means any information relating to a Data Subject that is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data that is (a) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service; or (b) supplied to or accessed by Qualtrics or its Subprocessors to provide support under the Agreement. Personal Data is a subset of Customer Data (as defined under the Agreement).

1.9 "**Personal Data Breach**" means a confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized third-party access to Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

1.10 **"Processor"** means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller, either directly as a processor of a controller or indirectly as a subprocessor of a processor that processes personal data on behalf of the controller.

1.11 **"SCC Relevant Transfer"** means a transfer (or an onward transfer) of Personal Data to a Third Country if such transfer requires an adequacy means pursuant to GDPR or other Data Protection Law and such adequacy means may be met by the parties entering into the EU Standard Contractual Clauses.

qualtrics XM

1.12 **"Subprocessor"** or **"sub-processor"** means a Qualtrics Affiliate or a third party engaged by Qualtrics or a Qualtrics Affiliate, in each case that processes Personal Data in accordance with this DPA.

1.13 **"Technical and Organizational Measures"** means the technical and organizational measures for the relevant Cloud Service set out in Schedule 3.

1.14 **"Third Country"** means any country, organization, or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. Background.

2.1 **Purpose and Application**.

(a) This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Qualtrics and Customer.

(b) This DPA applies to Personal Data processed by Qualtrics and its Subprocessors in connection with its provision of the Cloud Service.

(c) This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by Qualtrics. Customer will not store Personal Data in such environments.

2.2 **Structure**. Schedules 1, 2, 3, 4 and 5 are incorporated into and form part of this DPA. Schedule 1a and 1b sets out the agreed EU Standard Contractual Clauses; Schedule 2 sets out the agreed subject matter, the nature and purpose of the processing, the type of Personal Data, and categories of data subjects; Schedule 3 sets out the applicable Technical and Organizational Measures and includes the Cloud Security and Privacy Framework; Schedule 4 sets out the Subprocessors applicable to Customer's use of Qualtrics; Schedule 5 sets out information on usage data processed by Qualtrics in relation to Cloud Service.

2.3 **Governance**.

(a) Qualtrics acts as a Processor, and Customer and those entities that it permits to use the Cloud Service act as Controllers or Processors, as the case may be, under the DPA.

(b) Customer acts as a single point of contact and will obtain any relevant authorizations, consents, and permissions for the processing of Personal Data in accordance with this DPA. If Customer provides authorizations, consent, instructions, or permissions, these are also provided on behalf of any other Controller using the Cloud Service. If Qualtrics informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service, and Customer will forward such information and notices to the relevant Controllers.

2.4 Order of precedence. For the avoidance of doubt, Qualtrics and Customer agree that, to the extent the terms of this DPA conflict with the Agreement, the DPA shall control for all purposes related to the collection, processing, storage, transmission, or use of Personal Data.

3. Security of Processing.

3.1 **Applicability of the Technical and Organizational Measures**. Qualtrics has implemented and will apply the Technical and Organizational Measures set forth in Schedule 3, as detailed in the Cloud Security and Privacy Framework attached therein. Customer has reviewed such measures and acknowledges that, as to the Cloud Service selected by Customer in the EULA Acceptance Form, on the effective date of the Agreement, the measures are appropriate taking into account the

state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of Personal Data.

3.2 Changes.

(a) Qualtrics applies the Technical and Organizational Measures to Qualtrics' entire customer base hosted in the same data center or receiving the same Cloud Service. Qualtrics may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

(b) Qualtrics may publish updated versions of the Technical and Organizational Measures at www.qualtrics.com/terms-of-service, provided, however, any update will not materially reduce the overall protections set forth therein.

4. Qualtrics Obligations.

4.1 Instructions from Customer. Qualtrics will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes the initial documented instructions, and each use of the Cloud Service then constitutes further instructions. For any Customer instructions not made in the Agreement (including this DPA) or through Customer's use of the Cloud Service, Qualtrics will use reasonable efforts to follow such instructions to the extent they are required by Data Protection Law, technically feasible, and do not require changes to the Cloud Service. If Qualtrics cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Qualtrics will immediately notify Customer (email permitted).

4.2 Processing on Legal Requirement. Third Party Access Requests. Qualtrics may also process Personal Data if required to do so by applicable law, in which case Qualtrics will notify Customer of that legal requirement before processing unless that law prohibits such notification. Without prejudice to Clause 15 of the EU Standard Contractual Clauses, and upon Customer's written request, Qualtrics shall provide an attestation regarding access requests received from public authorities. Such Attestation shall confirm whether or not Qualtrics received any access requests from public authorities to Customer Data.

4.3 Personnel. To process Personal Data, Qualtrics and its Subprocessors will only grant access to authorized personnel who have committed themselves to confidentiality. Qualtrics and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

Cooperation. Qualtrics shall take reasonable steps at the Customer's request to assist Customer in meeting Customer's obligations under Article 32 to 36 of the GDPR, taking into account the nature of the processing under this DPA;

(a) At Customer's request, Qualtrics will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Qualtrics' processing of Personal Data or any Personal Data Breach.

(b) If Qualtrics receives a request from a Data Subject in relation to Personal Data, Qualtrics will promptly notify Customer (if the Data Subject has provided information to identify the Customer and if such notification is permitted by applicable law) by email and will not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

(c) In the event of a dispute with a Data Subject as it relates to Qualtrics' processing of Personal Data under this DPA, the Parties will keep each other informed and, if appropriate, reasonably cooperate with the aim of resolving the dispute amicably with the Data Subject.

(d) Qualtrics will provide functionality for production systems that supports Customer's ability to correct, delete, or anonymize Personal Data within a Cloud Service, or to restrict its processing in line with Data Protection Law. If such functionality is not provided, Qualtrics will correct, delete, or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

(e) Except to the extent required by applicable law, neither Party will notify any third party or make any public announcement regarding an incident involving Personal Data or any Personal Data Breach in a manner that would identify the other Party without the other Party's written consent (not to be unreasonably withheld).

4.4 **Personal Data Breach Notification**. Qualtrics will notify Customer without undue delay, but in any event within fourty-eight (48) hours, after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Qualtrics may provide such information in phases as it becomes available. Such notification will not be interpreted or construed as an admission of fault or liability by Qualtrics.

4.5 **Data Protection Impact Assessment**. If Data Protection Law requires Customer or its Controllers to perform a data protection impact assessment or prior consultation with a regulator, then, at Customer's request, Qualtrics will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, and audit reports and certifications). The parties, acting reasonably and in good faith, will agree on any additional assistance.

4.6 **Transfer Impact Assessment**. Prior to the execution of this DPA, the Parties conducted their respective assessments provided by Clause 14 of the EU Standard Contractual Clauses ("**Transfer Impact Assessment**") and concluded that the laws and practices of the the third country of destination applicable to the processing of the Personal Data by Qualtrics, along with the safeguards put in place by Qualtrics, do not in practice prevent the Parties from fulfilling their obligations under the EU Standard Contractual Clauses with regard to transfers of personal data outside of the EU, and are compatible with the commitments required by Article 46 of the GDPR regarding the transfer tools. As long as processing of Personal Data by Qualtrics while providing the Cloud Service implies a transfer of such Personal Data, as authorized by Customer in accordance with this DPA, the Parties agree to maintain and update their respective Transfer Impact Assessments.

5. Data Export and Deletion.

5.1 **Export and Retrieval by Customer**. During the Subscription Term and subject to the Agreement, Customer may access Personal Data at any time and may export and retrieve Personal Data in a standard format (such export constituting a "return" of Personal Data). Export and retrieval may be subject to technical limitations, in which case Qualtrics and Customer will find a reasonable method to allow Customer access to Personal Data, which may include Qualtrics delivering an export to Customer upon Customer's request through a support ticket.

5.2 **Deletion**. At the end of the Subscription Term, Customer hereby instructs Qualtrics to delete all Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in

line with Data Protection Law (not to exceed six months) unless applicable law requires retention. Notwithstanding the foregoing Customer may access the Cloud Service for 30 days after the Subscription Term expires solely to export Customer Data as set out in section 4.4 of the GTC.

6. Certifications and Audits.

6.1 **Customer Audit**. Customer or its independent third-party auditor reasonably acceptable to Qualtrics (which will not include any third-party auditors who are either a competitor of Qualtrics or not suitably qualified or independent) may audit Qualtrics' control environment and security practices relevant to Personal Data only:

(a) if Qualtrics has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through either: (1) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (2) a valid SOC1-3 attestation report;

(b) if a Personal Data Breach has occurred;

(c) if an audit is formally requested by Customer's data protection authority; or

(d) if Data Protection Law grants Customer a direct audit right, in which case Customer will only audit once in any 12-month period unless Data Protection Law requires more frequent audits.

6.2 **Other Controller Audit**. Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer will use all reasonable means to combine audits of all Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law.

6.3 **Scope of Audit**. Customer will provide at least 30 (thirty) days' advance notice of any audit unless Data Protection Law or a competent data protection authority requires shorter notice. The Parties, acting reasonably and in good faith, will agree on the frequency and scope of any audits. Customer audits will be limited in time to a maximum of three business days. Beyond such restrictions, the Parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer will provide the results of any audit to Qualtrics unless prohibited to do so by Data Protection Law.

6.4 **Cost of Audits**. Customer will bear the costs of any audit unless such audit reveals a material breach by Qualtrics of this DPA, in which case Qualtrics will bear its own costs. If an audit determines that Qualtrics has breached its obligations under the DPA, Qualtrics will promptly remedy the breach at its own cost.

7. Subprocessors.

7.1 **Permitted Use**.

(a) Qualtrics is granted a general authorization to subcontract the processing of Personal Data to Subprocessors.

(b) Qualtrics, or Qualtrics affiliates on its behalf, will engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Qualtrics is responsible for the Subprocessor's performance under the Agreement to the same extent it is responsible for its own performance.

(c) Qualtrics will evaluate the security, privacy, and confidentiality practices of a Subprocessor prior to selection to establish that it can provide the level of protection of Personal Data required by this DPA.

(d) Qualtrics' list of Subprocessors in place on the effective date of the Agreement is published by Qualtrics at www.qualtrics.com/subprocessor-list. Qualtrics will make it available to Customer upon request any information on Personal Data processed, location of processing activities, data retention and security measures adopted by, including the name, address, and role of each Subprocessor, along with any other information as necessary to allow Customer to assess their adequacy with regard to the level of protection of Personal Data required by this DPA. Subprocessors applicable to Customer on the effective date of the Agreement are listed in Schedule 4, that Qualtrics will update according to Section 7.2 below.

7.2 Modifications of Subprocessors; Objections.

(a) Qualtrics will inform Customer via email 30 (thirty) days before any modification to its Subprocessors list for processing Personal Data.

(b) Customer shall promptly review such modification in good faith and lodge any objections to such modification in writing to Qualtrics. If Customer does not object to the modification within 30 (thirty) days, Customer shall treat such non-objection as approval of the modification. If Customer objects to the modification based on a legitimate reason under Data Protection Law, Customer must provide written support for the objection and provide such other information as Qualtrics may reasonably request. Such discussions do not affect Qualtrics' right to use the new Subprocessor after the 30 day period. Solely in the case Qualtrics cannot provide the Cloud Service with or without use, as the case may be, of the objectionable Subprocessor, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used). Such termination must be effective no later than 30 days after the date of Qualtrics' notice to Customer informing Customer of the modification to the Subprocessor list;

(c) Any termination under this Section will be deemed to be without fault by either Party and will be subject to the terms of the Agreement.

7.3 Emergency Replacement. Qualtrics may replace a Subprocessor without advance notice if the reason for the change is outside of Qualtrics' reasonable control and prompt replacement is required for security or other urgent reasons. Qualtrics will inform Customer of the replacement Subprocessor as soon as possible following its appointment, and Section 7.2 applies accordingly.

8. International Processing.

8.1 Conditions for International Processing. Qualtrics may process Personal Data, including by using Subprocessors, outside the country in which the Customer is located, solely as strictly necessary to provide the Cloud Service and related support to Customer, or as otherwise requested by Customer.

8.2 Applicability of EU Standard Contractual Clauses if Qualtrics is not located in a Third Country. With respect to SCC Relevant Transfers, if Qualtrics is not located in a Third Country and acts as a data exporter, Qualtrics has entered into the EU Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses will apply to such SCC Relevant Transfers.

qualtrics XM

8.3 Applicability of EU Standard Contractual Clauses if Qualtrics is located in a Third Country.

(a) With respect to SCC Relevant Transfers, if Qualtrics is located in a Third Country, or in a country that otherwise requires use of the EU Standard Contractual Clauses for transfers of Personal Data to that country, the Parties rely on the EU Standard Contractual Clauses, which are hereby entered into with Customer as the data exporter and Qualtrics as the data importer as follows:

(1) Module 2 (Controller to Processor), attached as Schedule 1a, will apply when Customer acts a Controller; and

(2) Module 3 (Processor to Processor), attached as Schedule 1b, will apply when Customer acts a Processor under the instructions of its Controller.

(b) Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the EU Standard Contractual Clauses with Qualtrics in the same manner as Customer in accordance with Section 8.3(a) above, in which case Customer enters into the EU Standard Contractual Clauses on behalf of such other Controllers or Processors.

(c) On request from a Data Subject, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and Qualtrics (including the relevant Schedules) available to such Data Subject.

(d) As of the Effective Date Qualtrics is currently investigating the requirements to register under the Data Privacy Framework. Qualtrics is using good faith efforts to register under the Data Privacy Framework.

8.4 Applicability of EU Standard Contractual Clauses if applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses. Subject to Sections 8.2 to 8.4, if Data Protection Law requires a variation to the EU Standard Contractual Clauses, then the EU Standard Contractual Clauses are interpreted as follows:

(a) **Switzerland**. In relation to the Swiss Data Protection Act ("**FADP**"):

(1) the references to a "Member State" in the EU Standard Contractual Clauses will be deemed to include Switzerland;

(2) references to the law of the European Union or of a Member State in the EU Standard Contractual Clauses will be deemed to be a reference to the FADP;

(3) the Swiss Federal Data Protection and Information Commissioner will be the sole or, if both the FADP and the GDPR apply to such transfer, one of the competent data protection authorities under the EU Standard Contractual Clauses;

(4) the terms used in the EU Standard Contractual Clauses that are defined in the FADP will be construed to have the meaning of the FADP; and

(5) where the FADP protects legal entities as data subjects, the EU Standard Contractual Clauses will apply to data relating to identified or identifiable legal entities.

(b) **United Kingdom**. In relation to Personal Data that is protected by the GDPR as incorporated into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the EU Standard Contractual Clauses are interpreted as follows:

(1) "Third Country" will be interpreted as any country, organization, or territory that is not acknowledged as providing an adequate level of protection of personal

data pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(2) from 21 September 2022, the "EU Standard Contractual Clauses" will be interpreted as the "International Data Transfer Addendum to the EU Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**") and will apply completed as follows:

(A) the EU Standard Contractual Clauses, completed as set out above in Sections 8.2 and 8.3 (as applicable), will also apply to transfers of such Personal Data, subject to (B) below;

Tables 1 to 3 of the UK Addendum will be deemed completed with the relevant information from the EU Standard Contractual Clauses, completed as set out above at Sections 8.2 and 8.3 (as applicable), and the option "importer" will be deemed selected in Table 4. The start date of the UK Addendum (as set out in Table 1) will be the effective date of this DPA.

8.5 **Relation of the Standard Contractual Clauses to the Agreement**. Nothing in the Agreement will be construed to prevail over any conflicting clause of the EU Standard Contractual Clauses. For the avoidance of doubt, the audit and Subprocessor rules in this DPA also apply in relation to the EU Standard Contractual Clauses.

9. **Documentation; Records of Processing.** If required under Data Protection Law, each Party is responsible for complying with its obligation to maintain records of processing. Each Party will reasonably assist the other Party in such requirements, including by providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), to enable the other party to comply with any such obligations. Where Customer acts as a Processor, Qualtrics shall refer to Customer's Controllers listed at io.italia.it/enti/ and to other categories of controllers as notified from time to time to Qualtrics.

10. **Government Access Requests**. Qualtrics will only comply with binding orders of governmental entities that have jurisdiction over Qualtrics or as otherwise required by law. In such cases, Qualtrics will (i) give Customer reasonable written notice to allow Customer to seek a protective order or other appropriate remedy (except to the extent that compliance with the foregoing would cause Qualtrics to violate a court order or other legal requirement), (ii) disclose only such information as is required by the governmental entity or otherwise required by law, and (iii) use commercially reasonable efforts to obtain confidential treatment for any confidential information so disclosed.

qualtrics XM

Schedule 1a
EU Standard Contractual Clauses
Module 2
Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue

[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.

of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  (iii) Clause 9(a), (c), (d) and (e);
  (iv) Clause 12(a), (d) and (f);
  (v) Clause 13;
  (vi) Clause 15.1(c), (d) and (e);
  (vii) Clause 16(e);
  (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

[Intentionally removed]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the

European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

(a) 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 in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

Clause 13
Supervision

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(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).

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

[4] 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.

contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Regulation (EU) 2016/679.

Clause 17

Governing law

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 Italy.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Rome, Italy.
(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.

qualtrics XM

Schedule 1b
EU Standard Contractual Clauses
Module 3
Processor to Processor

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) ([5]) 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.

---

[5] 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.

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8.1(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;
  (vi) Clause 15.1(c), (d) and (e);
  (vii) Clause 16(e);
  (viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

[Intentionally removed]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data 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 ([6]).

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

[6] 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.

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 ([7]) (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.

---

[7] 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.

(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

(a) 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 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. ([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 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

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

notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter 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.

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

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

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

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

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

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

State law.

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([9]);

(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.

[9] 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.

(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). 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, 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 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

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.

The data exporter shall forward the notification to the controller.

(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.). The data exporter shall forward the information to the controller.

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

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

15.2 Review of legality and data minimization

(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. 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 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) 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

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 Italy.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Rome, Italy.

(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.

Schedule 2 Description of the Processing

This Schedule 2 applies to describe the processing of Personal Data for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

List of Parties

Data exporter(s)
Name: PagoPA S.p.A.
Address: Piazza Colonna 370, CAP 00187, Roma, Italy (seat) - Via Sardegna 38, CAP 00187 (HQ)
Contact person's name, position and contact details: Maurizio Fatarella, General Manager, dpo@pagopa.it
Activities relevant to the data transferred under these Clauses: provision of Cloud Service(s) by importer to exporter as set out in Section 8.1 of the DPA and in Section 1.4 of this Schedule 2.
Signature and date:

MAURIZIO FATARELLA
30.11.2023 15:01:25 GMT+01:00

Role: controller (Module 2) or processor (Module 3)

Data importer(s)
Name: Qualtrics LLC
Address: 333 West River Park Drive, Provo, Utah 84604, United States
Contact person's name, position and contact details: Rachael McChrystal, privacy@qualtrics.com
Activities relevant to the data transferred under these Clauses: provision of Cloud Service(s) by importer to exporter as set out in Section 8.1 of the DPA and in Section 1.4 of this Schedule 2.
Signature and date:

DocuSigned by:
Mark Creer
F3B7DF9FFCA34AF...

December 5, 2023

Role: processor (Module 2) or (sub)processor (Module 3)

1. **Description of Transfer.**

1.1. **Data Subjects.** Unless otherwise indicated by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners and end users of the exporter

1.2. **Data Categories.** The transferred Personal Data concerns the following categories of data: Customer determines the categories of data or data fields that may be transferred per Cloud

Service subscribed. Categories of personal data include navigation, diagnostic and usage data related to the exporter's services and products, unique identifiers and other Personal Data the exporter may submit through the Cloud Service(s) the extent of which is determined and controlled by the exporter in its sole discretion as applicable to fulfill the purpose.

1.3. Special Data Categories (where applicable).

(a) The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("Sensitive Data"). Qualtrics has taken Technical and Organizational Measures as set out in Schedule 3 to ensure a level of security appropriate to protect also Sensitive Data.

(b) The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

(1) training of personnel;

(2) encryption of data in transit and at rest;

(3) system access logging and general data access logging.

In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

1.4. Purposes of the Data Transfer and Further Processing; Nature of the Processing.

The transferred Personal Data is subject to the following processing activities in accordance with Section 8.1. of the DPA as strictly necessary to provide the Cloud Service and related support to Customer, or as otherwise requested by Customer:

1. use of Personal Data to set up, operate, monitor, and provide the Cloud Service (including operational and technical support);
2. continuous improvement of service features and functionalities provided as part of the Cloud Service;
3. provision of support and/or professional services;
4. communication to Authorized Users;
5. storage of Personal Data in dedicated data centers (multi-tenant architecture), as long as data centers are located in jurisdiction selected by exporter under the Partner in an Order Form;
6. release, development, and upload of any fixes or upgrades to the Cloud Service;
7. back up and restoration of Personal Data stored in the Cloud Service;
8. computer processing of Personal Data, including data transmission, data retrieval, and data access;
9. network access to allow Personal Data transfer;
10. monitoring, troubleshooting, and administering the underlying Cloud Service infrastructure and database;
11. security monitoring, network-based intrusion detection support, and penetration testing; and
12. execution of instructions of Customer in accordance with the Agreement.

For the avoidance of any doubt, "as necessary to provide the Cloud Service" as referenced anywhere throughout the Agreement (including any attachment thereto, including the Cloud Security and Privacy Framework) must be interpreted in light of Section 8.1. of the DPA and this section (Purposes of the Data Transfer and Further Processing; Nature of the Processing.) of this Schedule 2 (Description of the Processing).

The purpose of the transfer is to provide and support the Cloud Service. Qualtrics and its Subprocessors may support the Cloud Service data centers remotely. Qualtrics and its Subprocessors provide support when Customer submits a support ticket as further set out in the Agreement.

Additional description in respect of the EU Standard Contractual Clauses:
The purpose of the transfer is to provide and support the relevant Cloud Service. Qualtrics and its Subprocessors may provide or support the Cloud Service remotely.

1.5 For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: as set out in Schedule 4 (Subprocessors)

1.6 The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): Personal Data will be transferred on an ongoing basis for the duration of the Agreement.

1.7 The period for which personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data will be retained for the duration of the Agreement and subject to Section 5 of the DPA, unless otherwise required by applicable law. Retention from Subprocessors is set out in Schedule 4 (Subprocessors).

2. Competent Supervisory Authority

In accordance with Clause 13 of the EU Standard Contractual Clauses the competent supervisory authority is the Italian Data Protection Authority (Garante per la protezione dei dati personali)

Schedule 3 Technical and Organizational Measures

This Schedule 3 describes the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

Qualtrics will apply and maintain the Technical and Organizational Measures described in this Schedule 3 and as detailed in the Cloud Security and Privacy Framework attached herein, as updated from time to time by Qualtrics.

To the extent that the provisioning of the Cloud Service comprises SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 3 describe the measures and safeguards that have been taken to fully take into consideration the nature of the personal data and the risks involved.

1. TECHNICAL AND ORGANIZATIONAL MEASURES

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings, or rooms where data processing systems that process or use Personal Data are located.

Measures:

- Qualtrics protects its assets and facilities using the appropriate means based on the Qualtrics security policy.
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas, and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems, and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Qualtrics buildings must register their names at reception and must be accompanied by authorized Qualtrics personnel.
- Qualtrics employees and external personnel must wear their ID cards at all Qualtrics locations.

Additional measures for Data Centers:

- All data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms, and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- Qualtrics and all third-party data center providers log the names and times of authorized personnel entering Qualtrics' private areas within the data centers.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed through defined processes according to the Qualtrics security policy.
- All personnel access Qualtrics' systems with a unique identifier (user ID).
- Qualtrics has procedures in place so that requested authorization changes are implemented only in accordance with the Qualtrics security policy (for example, no rights are granted without authorization). In case personnel leave the company, their access rights are revoked.
- Qualtrics has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. For domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Qualtrics uses up–to-date antivirus software at access points to the company network (for email accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Qualtrics' corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. No Backdoors Persons entitled to use data processing systems gain access only to Personal Data that they have a right to access, and Personal Data must not be read, copied, modified, or removed without authorization in the course of processing, use, and storage. In addition to the foregoing, Qualtrics has not purposefully built – and undertakes not to purposefully build, for the duration of the Agreement and for the services provided to Customer - any backdoors or other methods into its Cloud Services with the aim of allowing third parties, including government authorities, to circumvent its security measures to gain access to Customer Data.

Measures:

- As part of the Qualtrics security policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require to fulfill their duty. Qualtrics uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Qualtrics security policy.
- All production servers are operated in the data centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, Qualtrics conducts internal and external security checks and penetration tests on its IT systems.
- A Qualtrics security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified, or removed without authorization during transfer. If data carriers are physically transported, adequate measures are

implemented at Qualtrics to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over Qualtrics internal networks is protected according to the Qualtrics security policy.
- When data is transferred between Qualtrics and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network-based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Qualtrics-controlled systems (e.g., data being transmitted outside the firewall of the Qualtrics data center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified, or removed from Qualtrics' data processing systems.

Measures:

- Qualtrics only allows authorized personnel to access Personal Data as required in the course of their duty.
- Qualtrics has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Qualtrics or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- Qualtrics uses controls and processes to monitor compliance with contracts between Qualtrics and its customers, subprocessors, or other service providers.
- As part of the Qualtrics security policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- All Qualtrics employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Qualtrics' customers and partners.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Qualtrics employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- Qualtrics uses uninterrupted power supplies (e.g., UPS, batteries, generators, etc.) to protect power availability to the data centers.
- Qualtrics has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business-critical services as further set out in the Documentation or incorporated into the EULA Acceptance Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Measures:

- Qualtrics uses the technical capabilities of the deployed software (e.g., multi- tenancy, system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.

1.9 Data Integrity Control. Personal Data will remain intact, complete, and current during processing activities.

Measures:

Qualtrics has implemented a multi-layered defense strategy as a protection against unauthorized modifications. In particular, Qualtrics uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

Schedule 4
Subprocessors

Schedule 4 is under refinement and will be incorporated into and form part of this DPA once finalized upon agreement by the Parties.

Schedule 5
Usage Data information

Schedule 5 is under refinement and will be incorporated into and form part of this DPA once finalized upon agreement by the Parties.