giz

STANDARD CONTRACTUAL CLAUSES 2021/914

MODULE TWO: Transfer Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these 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) 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 contractual clauses ('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 Clauses.

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

a) The data subjects can enforce against the data exporter and/or data importer these Clauses, 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 other 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 hereunder.

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational 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 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[1] (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;

[1] 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.

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

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

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

8.9. Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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[2]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[3] at no cost to the data subject. It shall inform the data subjects, in the

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

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

manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

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

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

[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.

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

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 Germany.

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

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

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

Data exporter:

Company Name: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Address: KG 541 St, Kigali, Rwanda

Contact person's name, position and contact details: Ariane Nayituliki, Digital Advisor, ariane.nayituliki@giz.de / Ayaan Jama, Digital Advisor, ayaan.jama@giz.de

Activities relevant to the data transferred under these Clauses: Data collection and data transfer to GIZ as part of the support to the implementation of results-based monitoring of two GIZ projects.

Role: ☒ Controller

_____

Signature and date

Data importer:

Company Name: Please specify

Address: Please specify

Contact person's name, position and contact details: Please specify

Any contact person with responsibility for data protection: Please specify

Activities relevant to the data transferred under these Clauses: Please specify

Role: ☒ Processor

_____

Signature and date

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

☐ Employees of GIZ including applicants
☐ Subscribers of e.g. magazines and newsletters
☐ External participants in events
☐ Participants in surveys
☐ Visitors to the premises of GIZ
☐ Visitors to websites
☐ Service Provider / Supplier
☐ Contact persons of partner institutions
☐ Representatives of official bodies and government representatives
☐ Students/Scholarship holders
☐ Other: Please specify: Participants in training

……..

Categories of personal data transferred:

☒ Personal Master Data (Name, date of birth)
☒ Address data
☒ Contact- and communication data (e.g. telephone, e-mail etc.)
☐ Qualification data (e.g. career history, CV, qualification etc.)
☒ Employee data (wages and salaries, bank account, tax information etc.)
☐ Billing and payment data
☐ User data (browsing data, IP addresses, cookies, login data etc.)
☐ Photo and sound recordings
☐ Travel and location data
☐ Special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 (e.g. data concerning health, biometric data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning a natural person's sex life or sexual orientation). Please specify
☐ Other: Please specify

……

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

Applied restrictions or safeguards

☒ Strict purpose limitation
☐ Access restrictions
☐ Access only for staff having followed specialised training

☐ Keeping a record of access to the data
☐ Restrictions for onward transfers
☐ Additional security measures. Please specify:
……..
Frequency of transfer:

☒ The data is transferred on a one-off.
☐ The data is transferred on a continuous basis.
☐ Other: Please specify .

……..

Nature of processing

☒ Collection ☐ Adaptation ☐ Disclosure by transmission
☐ Restriction ☐ Recording ☐ Alteration
☐ Dissemination ☐ Erasure ☐ Organisation
☐ Retrieval ☐ otherwise making available ☐ Destruction
☐ Structuring ☐ Consultation ☐ Alignment
☒ Storage ☐ Use ☐ Combination
☐ Other: Please specify

……

Purpose(s) of the data transfer and further processing

The data transfer and further processing by the data importer is part of the support to the implementation of results-based monitoring activities of two GIZ projects. The data transfer and further processing shall allow for effective project monitoring, steering and impact measurement.

……

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

☒ The data is retained for a short time.
☐ The data is retained for a longer period.
☐ The criteria for determining the retention period results from main contract.
☐ The statutory retention period is used to determine the retention period.
☐ Other. Please specify:

……

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

……

C. COMPETENT SUPERVISORY AUTHORITY

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

☒ Germany - Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

ANNEX II

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

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

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

The following checklist, which contains a large number of possible technical and organisational measures, can be used for presentation. The checklist is not exhaustive and must be supplemented by the contractor for each individual case, if necessary. In order to ensure the concrete description, explanations must be inserted in each case. The presentation and description of the technical and organisational measures implemented by the contractor can alternatively also be made in a separate document.

1. Measures of pseudonymization and encryption of personal data

☐ Pseudonymisation of personal data no longer required in clear text
☐ Pseudonymisation Policy
☐ Encryption of data carriers
☐ Pseudonymisation of test system data
☐ Encryption of websites (SSL)
☐ Encryption of database
☐ Email encryption (TLS 1.2 or 1.3)
☐ Encryption of passwords and keys
☐ Encryption of mobile devices
☐

Explanation:

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

☐ Non-disclosure agreement with employees
☐ Employees´ data protection obligations
☐ Non-disclosure agreement with third parties
☐ External storage / backup server
☐ Support contracts with third parties
☐ Data outsourcing agreements
☐ Utilization of certified cloud provider
☐ Firewall
☐ Anti-virus software
☐ Regular data backups
☐ Redundant systems
☐ Monitoring of systems and services
☐ RAID systems
☐ Devices for monitoring temperatures ☐ Firefighting equipment
☐ Network Attached Storage (NAS)
☐ Maintenance agreement
☐ Regular IT incident tests
☐ Internal storage of copies / backups
☐ Uninterruptible Power Supply (UPS),
☐ Fire and smoke alarm systems
☐ Devices for monitoring temperatures
☐ Firefighting equipment
☐ Alarm warning in case of unauthorized access
☐ Load balancing
☐

Explanation:

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

☐ Regular backups of the entire system
☐ Storage on multiple systems
☐ Data backup concept
☐ Regular test backup/recovery
☐ Hardware support and maintenance agreement
☐ Concept for emergency preparedness

☐ Outsourced data backup
☐ Regular training of IT staff
☐

Explanation:

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

☐ Internal controls
☐ Order or contract control (careful selection of contractors, clear contract design, etc.)
☐ Regular review of IT processes
☐ Regular audits (e.g. by data protection officer)
☐ Regular review of procedures
☐ Audit of technical and organisational measures by data protection officer
☐ Regular checks of employees
☐ Conducting data protection impact assessments
☐ Check of privacy by design and by default
☐ Data protection management system / data protection manual
☐

Explanation:

5. Measures for user identification and authorisation

☐ Two-factor authentication
☐ Authentication with username / password
☐ Separation of roles between test and production system
☐ Regular assessment of authorizations
☐ BIOS passwords
☐ Permission management
☐ Mobile Device Management Policy
☐ User profiles
☐ Password policy
☐ Limitation the number of admins
☐ Identification of new employees
☐ Separation of user roles
☐ Automatic locking mechanisms
☐ Identification of external person with ID cards
☐ Management of rights by an admin
☐ Differentiation between permissions
☐

Explanation:

6. Measures for the protection of data during transmission

☐ Utilisation of encryption technologies
☐ Virtual Private Network (VPN)
☐ Logging of activities and events
☐ Transport via private cloud
☐ Documentation of data recipients
☐ Email encryption (TLS 1.2 or 1.3)
☐ Verification of the identity of the recipients
☐ Utilisation of non-public drives
☐ Physical transport: secure transport containers
☐ Careful selection of transport personnel
☐

Explanation:

7. Measures for the protection of data during storage

☐ Encryption of data carriers
☐ Data classification
☐ Permission management
☐ Limitation of access
☐ Logging of actions and events
☐ Security doors
☐ Limitation the number of admins
☐ Magnetic or chip cards
☐ Anonymization of data
☐ Pseudonymization of data
☐ Secure storage of data carriers
☐ Firewall
☐

Explanation:

8. Measures for ensuring physical security of locations at which personal data are processed
☐ Alarm system

☐ Facility security services and/or entrance security staff
☐ Protection of building shafts
☐ Logging of visitors
☐ Automatic access control
☐ Careful selection of cleaning staff
☐ Careful selection of security staff
☐ Magnetic or chip cards
☐ Locking system with code lock
☐ Obligation to wear authorization cards
☐ Manual locking system
☐ Concept of access
☐ Biometric entrance barrier
☐ Lockable server cabinets
☐ Video surveillance of the entrances
☐ Doors with a knob on the outside
☐ Light barriers / motion detectors
☐ Visitors: Only accompanied by employees
☐ Safety locks
☐ Bell system with camera
☐ Key issuance procedure
☐

Explanation:

9. Measures for ensuring events logging

☐ Use of automatic logging
☐ Creation of incident reports
☐ Notification with real-time alarm
☐ Application-level logging
☐ Automatic review of logs
☐ Synchronization of system clocks
☐ Regular manual review of logs
☐ Automatic consolidation of incidents
☐ Logs are stored in the application and automatically sent to another location
☐

Explanation:

10. Measures for ensuring system configuration, including default configuration

☐ Configuration management policy exists

☐ Process for changes to configurations
☐ Privacy by Default
☐ Check of the default configurations
☐ Definition of default configurations
☐ Configuration by system administrator
☐ Logging of changes to configurations
☐ Regular training of IT staff
☐

Explanation:

11. Measures for internal IT and IT security governance and management

☐ IT security guideline
☐ IT administration guideline
☐ Regular compliance audits / reviews
☐ Register of IT systems
☐ Training of employees on data security
☐ Regular system review/evaluation
☐ IT team with assigned roles/responsibilities
☐ Incident-management guidelines
☐ Risk assessment and risk management measures at all stages and levels
☐

Explanation:

12. Measures for certification/assurance of processes and products

☐ Implementation of ISO 9001 - *Quality Management*
☐ Implementation of ISO 27001 - *Information technology management system*
☐ Implementation of ISO 27701 - *Privacy Information Management System*
☐ GDPR-Certification – Data Protection Management
☐ Overview of the regulations applicable to products/services/processes
☐ Identification of industry-specific standards
☐ Regular internal and/or external audits
☐ Assignment of audit responsibilities to certified experts
☐ Regular check for new requirements and renewal of certificates
☐

Explanation:

13. Measures for ensuring data minimization

☐ Identification of the purpose of the processing
☐ Assessment of the connection between processing and purpose
☐ Assessment of the scope and quality of the data processed in relation to the purpose
☐ Identification of the applicable retention periods
☐ Secure deletion of data after expiry of the retention period
☐

Explanation:

14. Measures for ensuring data quality

☐ Data profiling and classification
☐ Control of incoming or new data
☐ Logging of the input/change of data
☐ Assignment of rights for data entry
☐ Log retention
☐ Traceability of users when entering, change of data (no user groups)
☐ Avoidance of duplicate data
☐ Identification of data requirements
☐ Application of data quality measures
☐

Explanation:

15. Measures for ensuring limited data retention

☐ Retention policy with roles
☐ Separation of data according to retention periods
☐ Regular training
☐ Regular review and evaluation of stored data
☐

Explanation:

16. Measures for ensuring accountability

☐ Training / Awareness Raising
☐ Regular checks and audits
☐ Data protection team exist
☐ Guidance and support for employees
☐ Appropriate privacy policies
☐ Conclusion of Standard Contractual Clauses (SCC)
☐ Joint Controllership Agreements
☐ Responding to requests from data subjects
☐ Transparency documents (Article 13 / 14 GDPR)
☐ Secure deletion of data
☐ Documented privacy statement
☐ Audit reports and measures are documented
☐ Proper involvement of the Data Protection Officer
☐ Specific consent procedure / keeping of consent logs
☐

Explanation:

17. Measures for allowing data portability and ensuring erasure

☐ Storage in a structured format
☐ Monitoring of statutory periods
☐ Transfer via end-to-end encryption
☐ Compliance with retention periods
☐ Enabling data portability
☐ Dealing with the rights of data subjects pursuant to Chapter 3 of Regulation (EU) 2016/679
☐ Secure data deletion ensured
☐ Secure destruction of data carriers ensured
☐

Explanation:

giz

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

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

The data exporter has authorised the use of the following sub-processors:

1. Name: Please specify

Address: Please specify

Contact person's name, position and contact details: Please specify

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

When transferring data to a third country or an international organisation: How is compliance with Chapter V of Regulation (EU) 2016/679 ensured? Please specify

2. Name: Please specify

Address: Please specify

Contact person's name, position and contact details: Please specify

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

When transferring data to a third country or an international organisation: How is compliance with Chapter V of Regulation (EU) 2016/679 ensured? Please specify

3. Name: Please specify

Address: Please specify

Contact person's name, position and contact details: Please specify

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

When transferring data to a third country or an international organisation: How is compliance with Chapter V of Regulation (EU) 2016/679 ensured? Please specify

4. Name: Please specify

Address: Please specify

Contact person’s name, position and contact details: Please specify

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

When transferring data to a third country or an international organisation: How is compliance with Chapter V of Regulation (EU) 2016/679 ensured? Please specify