**STANDARD CONTRACTUAL CLAUSES 2021/914**

**MODULE ONE: Transfer Controller to Controller**

**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 these Clauses.

**Clause 2**

**Effect and invariability of the Clauses**

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

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

**Clause 3**

**Third-party beneficiaries**

(a) 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 8.5 (e) and Clause 8.9 (b)

*[iii) not applicable]*

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

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.

**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. 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**. It may only process the personal data for another purpose:

i) where it has obtained the data subject’s prior consent;

ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2. Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to **Clause 10**, the data importer shall inform them, either directly or through the data exporter:

i) of its identity and contact details;

ii) of the categories of personal data processed;

iii) of the right to obtain a copy of these Clauses;

iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to **Clause 8.7**.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3. Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4. Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

**8.5. 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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.

(b) The Parties have agreed on the technical and organisational measures set out in **Annex II.** The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to **Clause 13**. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6.** **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 or offences (hereinafter ‘sensitive data’), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7. Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i) it 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 with respect to the processing in question;

iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

**8.8.** **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

**8.9.** **Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

***[Clause 9 not applicable]***

**Clause 10**

**Data subject rights**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in **Annex I**; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to **Clause 8.7**; and provide information on the right to lodge a complaint with a supervisory authority in accordance with **Clause 12(c)(i)**;

ii) rectify inaccurate or incomplete data concerning the data subject;

iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter ‘automated decision’), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

**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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex I.C**, shall act as competent supervisory authority.

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

**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;

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.

**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.

**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 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.

**ΑΝΝΕΧ I**

**A. LIST OF PARTIES**

**Data exporter Number** Please click here to add a text.**:**

Name: Please click here to add a text.

Address: Please click here to add a text.

Contact person’s name, position and contact details: Please click here to add a text.

Activities relevant to the data transferred under these Clauses: Please click here to add a text.

Where applicable, of its/their data protection officer and/or representative in the European Union: Please click here to add a text.

|  |  |
| --- | --- |
| Role: Controller  Date: Please click here to add a text.  First and Last Name (written out in full):  Please click here to add a text. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature |

**Data importer Number** Please click here to add a text.**:**

Name: Please click here to add a text.

Address: Please click here to add a text.

Contact person’s name, position and contact details: Please click here to add a text.

Any contact person with responsibility for data protection: Please click here to add a text.

Activities relevant to the data transferred under these Clauses: Please click here to add a text.

Where applicable, of its/their data protection officer and/or representative in the European Union: Please click here to add a text.

|  |  |
| --- | --- |
| Role: Controller  Date: Please click here to add a text.  First and Last Name (written out in full):  Please click here to add a text. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature |

**B. DESCRIPTION OF TRANSFER**

**Categories of data subjects whose personal data is transfered**

Customers  Event participants

Relatives of staff  Potential customers

Visitors  Applicants

Employees  Business partners

Apprentices  Suppliers

Communication participants  Trainees

Service providers  Consultants

Students  Authorized Agents

Shareholders  Contact Persons

Subscribers

Other. Please specify: Please click here to add a text.

**Categories of personal data transfered**

Names  Factors specific to the physical identity

Identification number  Factors specific to the physiological identity

Location data  Factors specific to the genetic identity

Online identifier  Factors specific to the mental identity

Factors specific to the economic identity

Factors specific to the cultural identity

Factors specific to the social identity

Customer data  Data of event participants

Data of relatives of staff  Data of potential customers

Data of visitors  Data of applicants

Data of employees  Data of business partners

Data of apprentices  Data of suppliers

Data of communic. participants  Data of trainees

Data of service providers  Data of consultants

Data of students  Data of authorized agents

Data of shareholders  Data of contact persons

Data of subscribers

Other. Please specify: Please click here to add a text.

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

**Sensitive data transferred**

Racial Origin  Ethnic Origin

Political opinions  Religious beliefs

Philosophical beliefs  Trade union membership

Genetic data  Biometric data

Data concerning health  Data concerning sex life

Data concerning sexual orientation  Data relating to criminal convictions

Data relating to criminal offences

Please click here to add a text.

**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: Please click here to add a text.

**Frequency of transfer:**

The data is transferred on a one-off.

The data is transferred on a continuous basis.

Other. Please specify: Please click here to add a text.

**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

Please click here to add a text.

**Purpose(s) of the data transfer and further processing**

Please click here to add a text.

**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: Please click here to add a text.

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

**Subject matter of (sub-) processing:** Please click here to add a text.

**Nature of (sub-) processing:** Please click here to add a text.

**Duration of (sub-) processing:** Please click here to add a text.

**C. COMPETENT SUPERVISORY AUTHORITY**

Austria - Österreichische Datenschutzbehörde

Belgium - Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)

Bulgaria - Commission for Personal Data Protection

Croatia - Croatian Personal Data Protection Agency

Cyprus - Commissioner for Personal Data Protection

Czech Republic - Office for Personal Data Protection

Denmark - Datatilsynet

EDPS - European Data Protection Supervisor

Estonia - Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)

Finland - Office of the Data Protection Ombudsman

France - Commission Nationale de l'Informatique et des Libertés - CNIL

Germany - Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Germany - Baden-Württemberg - Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit

Germany - Bayern - Landesamt für Datenschutzaufsicht

Germany - Bayern - Der Bayerische Landesbeauftragte für den Datenschutz

Germany - Berlin - Berliner Beauftragte für Datenschutz und Informationsfreiheit

Germany - Brandenburg - Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Germany - Bremen - Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Germany - Hamburg - Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Germany - Hessen - Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

Germany - Mecklenburg-Vorpommern - Der Landesbeauftragte für Datenschutz und Informationsfreiheit

Germany - Niedersachsen - Die Landesbeauftragte für den Datenschutz Niedersachsen

Germany - Nordrhein-Westfalen - Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Germany - Rheinland-Pfalz - Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit

Germany - Saarland - Unabhängiges Datenschutzzentrum Saarland

Germany - Sachsen - Der Sächsische Datenschutzbeauftragte

Germany - Sachsen-Anhalt - Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Germany - Schleswig-Holstein - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Germany - Thüringen - Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Greece - Hellenic Data Protection Authority

Hungary - Hungarian National Authority for Data Protection and Freedom of Information

Ireland - Data Protection Commission

Italy - Garante per la protezione dei dati personali

Latvia - Data State Inspectorate

Lithuania - State Data Protection Inspectorate

Luxembourg - Commission Nationale pour la Protection des Données

Malta - Office of the Information and Data Protection Commissioner

Netherlands - Autoriteit Persoonsgegevens

Poland - Urząd Ochrony Danych Osobowych (Personal Data Protection Office)

Portugal - Comissão Nacional de Proteção de Dados - CNPD

Romania - The National Supervisory Authority for Personal Data Processing

Slovakia - Office for Personal Data Protection of the Slovak Republic

Slovenia - Information Commissioner of the Republic of Slovenia

Spain - Agencia Española de Protección de Datos (AEPD)

Sweden – Integritetsskyddsmyndigheten

**ANNEX II**

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

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 technical and organizational security measures already pre-checked are the minimum standard required by the Controller. If you have not implemented these technical and organizational security measures, please inform the Controller immediately. Additionally, you shall add all additional technical and organizational security measures taken by you!**

1. **Measures of pseudonymization and encryption of personal data**

☒ Pseudonymisation of personal data that are  Pseudonymisation policy

no longer needed in plain text  Encryption of data carriers

Pseudonymisation of data in test systems ☒ Encryption of websites (SSL)

Encryption of databases ☒ Encryption of e-mail (TLS 1.2 or 1.3)

Encryption of passwords and keys  Encryption of mobile devices

Please click here to add a text.

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

☒ Confidentiality agreements with employee’s ☒ NDA´s with third parties

☒ Data Protection agreements with employee’s  External storage / external backup server

Support agreements with third parties  Data outsourcing agreements

Use of certified Microsoft Cloud  Use of certified Google Cloud

Use of certified Amazon Cloud  Use of other certified cloud provider

☒ Firewall ☒ Anti-Virus

☒ Regular backups  Redundant systems

Monitoring of systems and services  RAID storage systems

Network attached storage (NAS)  Maintenance contracts

Regular IT incident tests  In-house storage of copies / backups

Uninterruptible Power Supply (UPS)  Fire and smoke detection systems

Devices for monitoring temperatures  Firefighting equipment

Alarm warning in the event of unauthorized access  Use of load balancing

Please click here to add a text.

1. **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 whole system  Storage on several and different devices

Creation of a data backup concept ☒ Regular test of backup and recovery

Hardware support and services contracts  Emergency preparedness concept

Storage of outsourced data backup ☒ Regular training of IT staff

Please click here to add a text.

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

☒ In-house checks ☒ Regular review of processes by IT

☒ Regular audits (e.g. by the DPO  Regular check of processing activity records

TOM audit by the DPO  Regular tests/checks of employees

Execution of data protection impact assessments  Review of privacy by design / default

Implementation of a data protection management system (DPMS) / data protection handbook

Please click here to add a text.

1. **Measures for user identification and authorisation**

Two-Factor-Authentication ☒ Authentication with username / password

Separation of test and productive system user roles ☒ Regular checks of authorisations

BIOS passwords  Creation of user profiles

Mobile Device Management Policy  Creation of an authorisation concept

☒ Password guideline ☒ Limitation of the number of administrators

Identification of new employees by HR department  Separation of user roles

Automatic locking mechanisms  Third party identification with IDs

☒ Management of rights by system administrator ☒ Differentiation between authorisations

Please click here to add a text.

1. Measures for the protection of data during transmission

☒ Use of encryption technologies  VPN

☒ Logging of activities and events  Transport over a private cloud

Documentation of recipients of data ☒ Encryption of email (TlS 1.2 or 1.3)

Verification of the recipient’s identity ☒ Use of company internal / restricted drives

Physical transport: safe transport containers  Careful selection of transport staff

Please click here to add a text.

1. Measures for the protection of data during storage

Encryption of data carriers  Data classification

Creation of an authorisation concept  Limitation of access

☒ Logging of actions and events  Security doors

☒ Limitation of the number of administrator’s  Key card / RFID access

Anonymisation of data  Pseudonymisation of data

Secure storage of data carriers ☒ Firewall

Please click here to add a text.

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

Alarm system  Control of persons at the porter

Protection of building shafts  Logging of visitors

Automatic access control system  Careful selection of cleaning staff

Chip cards, transponders  Careful selection of security personnel

Locking system with code lock  Obligation to wear authorisation IDs

☒ Manual locking system  Access concept

Biometric access lock  Lockable server cabinets

Video surveillance of entrances  Doors with a knob on the outside

Light barriers / motion detectors  Visitors: Only accompanied by employees

☒ Security locks  Bell system with camera

☒ Key control  Offices have door locks

Please click here to add a text.

1. **Measures for ensuring events logging**

Use of automatic logging solutions  Event report generation

Notification policy with real time alert ☒ Logging activated on application level

Automatic checks of logs  Systems clocks synchronization

☒ Regular manual checks of logs  Automatic consolidation of event logs

Logs are stored within the application and automatically send to a remote location

Please click here to add a text.

1. **Measures for ensuring system configuration, including default configuration**

Configuration management policy exists ☒ Configuration change control process

☒ Data protection by default is observed  Standard review of default configurations

DPO is involved in configuration  Definition of standard configurations

IT security officer is involved in configuration ☒ Configuration only by system administrator

Logging of changes in configuration ☒ Regular training of IT staff

Observation of manufacturer’s recommendations

Please click here to add a text.

1. **Measures for internal IT and IT security governance and management**

☒ IT security policy IT administration policy

Regular compliance audits and reviews  IT asset register

☒ Training of employees on data security  Periodic system testing and evaluation

☒ IT team with clear roles and responsibilities  Incident management and response policy

Risk assessment and risk management measures at all stages and levels

Please click here to add a text.

1. **Measures for certification/assurance of processes and products**

Implementation of ISO 9001 - Quality Management

Implementation of ISO 27001 - Information Security Management

Implementation of ISO 27701 - Privacy Information Management

GDPR Certification – Data Protection Management

☒ Clear overview of the provisions applicable to the provided products/services/processes

Identification of industry-related standards

☒ Regular internal and/or external audits

☒ Assignment of audit responsibilities to certified experts

Regular check for new prerequisites and renewal of certificates

Please click here to add a text.

1. **Measures for ensuring data minimization**

☒ Identification of the purpose of processing

☒ Assessment of a link between processing and purpose

Assessment of the amount and quality of the data processed in relation to the purpose

☒ Identification of the applicable retention periods for each data category

☒ Secure erasure of the data after expiration of the retention period

Please click here to add a text.

1. **Measures for ensuring data quality**

Data profiling and classification  Control/check of incoming or new data

☒ Logging of entry and modification of data ☒ Assignment of rights for data entry

Storage of logs ☒ Traceability of entry, modification of data by  Avoidance of duplicated data individual user names (not user groups)

Identification of requirements for data types  Application of measures for data quality

Please click here to add a text.

1. **Measures for ensuring limited data retention**

Retention policy defining responsibilities and roles  Separation of data by retention periods

DPO advises on data retention periods ☒ Regular training on retention periods

☒ Regular audit and assessment of retained data

Please click here to add a text.

1. **Measures for ensuring accountability**

☒ Provision of training / awareness rising ☒ Regular controls and checks

Assembly of a data protection team  Guidance and support for employees

☒ Appropriate policies on data protection ☒ Conclusion of SCCs

Conclusion of joint controllership agreements  Answer of data subject’s requests

Transparency document (Art. 13 / 14 GDPR) ☒ Use of secure data erasure

Legal basis for processing exists for all activities ☒ Documented privacy policy

Audit reports and measures taken are documented  Proper involvement of DPO

Specific consent procedure / maintaining of consent records

Please click here to add a text.

1. **Measures for allowing data portability and ensuring erasure**

☒ Personal data is stored in a structured format ☒ Monitoring of legal deadline ensured

Transmission with end-to-end encryption ☒ Observation of retention periods

☒ Establishment of data portability process ☒ Proper handling of data subject requests

☒ Secure data erasure ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure certificate).

☒ Secure data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data destruction certificate).

Please click here to add a text.

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

Standard Contractual Clauses (SCCs) are signed or agreed on

Implementation of ISO 9001 - Quality Management on (sub-) processor level

Implementation of ISO 27001 - Information Security Management on (sub-) processor level

Implementation of ISO 27701 - Privacy Information Management on (sub-) processor level

GDPR Certification – Data Protection Management on (sub-) processor level

☒ Secure data erasure ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure certificate).

☒ Secure data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data destruction certificate).

☒ Contractually agreed on effective control rights

☒ Contractually agreed on provision of assistance to the controller

Please click here to add a text.