DATA PROTECTION TERMS & CONDITIONS

("DPA")

Version Date: 06.07.2022

PLEASE READ AND CONFIRM FIELDCODE DATA PROTECTION TERMS AND CONDITIONS (THE "DPA"). THIS DOCUMENT WILL HAVE BEEN DEEMED ACCEPTED BY THE CUSTOMER ONCE CLICKED ON "ACCESS NOW" OR SIMILAR AS SET FORTH HEREIN.

1 / INTERPRETATION

A. Fieldcode Germany GmbH with its principal place of business at Am Stadtpark 2 DE – 90409 Nürnberg shall be considered as "Data Processor" under this DPA and the Customer shall be considered as "Data Controller".

B. This DPA sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller. Data Processor's processing of personal data shall take place for the purposes of fulfilment of the Parties' agreement for license to the Customer for use of and access to the ticketing system for management of field services provided by Fieldcode ("Fieldcode Software"), if concluded between Customer and Fieldcode by accepting the GT&Cs at https://www.fieldcode.com/en/informations/legal.

C. Structure:
   a. Detailed information about the processing of personal data under this DPA is included in Appendix A to this DPA.
   b. Technical and organization measures of Data Processor are included in Appendix B to this DPA.
   c. Standard Contractual Clauses by European Commission for data transfer to third countries are included in Appendix C to this DPA.
   d. Privacy Policy of Fieldcode is available at https://fieldcode.com/en/informations/privacy-policy.

D. This DPA has been designed to ensure the Parties' compliance with Article 28, subsection 3 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("General Data Protection Regulation" or "GDPR" or "Data Protection Laws") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Any capitalised terms and words, unless otherwise defined herein, shall have the meaning as specified in the General Data Protection Regulation.

2 / DATA CONTROLLER AND DATA PROCESSOR

A. Data Controller shall be responsible to third parties (including the data subject) for ensuring that the processing of personal data takes place in accordance with and under the governance of the General Data Protection Regulation. Data Controller shall therefore have both the right and obligation to make decisions about the purpose and means of the processing of personal data. Data Controller is responsible for ensuring that the access and the processing with which Data Processor is entrusted, is legally permissible.

B. Data Processor shall be permitted to process personal data based on instructions from the Data Controller and as required under EU or Member State law, to which Data Processor is a subject. In

case of the latter, Data Processor shall inform Data Controller of this legal requirement prior to processing, unless the relevant law prohibits the provision of such information based on important grounds of public interest, as described in the Article 28, subsection 3 (a) GDPR.

C. Data Processor shall rectify, erase and restrict processing of personal data as instructed by Data Controller and in accordance with this DPA.

D. Data Processor shall immediately inform Data Controller in writing if, in the opinion of Data Processor, the instructions of Data Controller are noncompliant with the General Data Protection Regulation or any other data protection regulations within EU or Member State law. Data Processor shall not be responsible for any personal data beyond what is agreed under this DPA and shall not be liable for results of any access granted to the personal data that has not been explicitly agreed under this DPA.

3 / SECURITY

A. Data Processor shall ensure and perform all the steps, as applicable and required by the Article 32 of the General Data Protection Regulation. Consequently, Data Controller and Data Processor respectively shall maintain appropriate technical and organisational measures to ensure a level of security, taking into the account the current level, implementation costs and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

B. In accordance with Section 3(A) above, Data Processor shall perform an appropriate risk assessment and thereafter implement measures to ensure a level of security reflective of such risk, which may (as the case may be) include: (i) ensuring pseudonymisation and encryption of personal data; (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a security incident and/or any other system issues; (iv) maintaining a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures; and (v) ensuring an appropriate segregation of personal data from other databases, if any.

C. In order to achieve the following, Data Processor shall maintain the level of security and the measures as specified in the Appendix B to this DPA "Fieldcode Operational and Technical measures".

4 / OBLIGATIONS OF DATA PROCESSOR

A. Data Processor, as possible and applicable to the nature of the processing, shall support Data Controller, in accordance with its operational and technical measures specified in Appendix B to this DPA, in the fulfilment of Data Controller's obligations to respond to requests for the exercise of data subjects' rights pursuant to Chapter 3 of the General Data Protection Regulation. Such assistance may (as the case may be) include:

   a. notification obligation when collecting personal data from the data subject

   b. notification obligation regarding rectification or erasure of personal data or restriction of processing

c. ensuring the rights of the data subject such as: right of access, right of rectification, right to erasure ("the right to be forgotten"), right to restrict processing, right to data portability, right to object, and right to object to the result of automated individual decision-making, including profiling.

B. Data Processor shall support Data Controller in ensuring compliance with Data Controller's obligations stipulated by the Articles 32 - 36 of the General Data Protection Regulation as applicable to the nature of the processing, scope of this DPA and the data made available to Data Processor.

C. In accordance with Section 3(C) above, Data Processor shall, as possible and applicable to the nature of the processing and the scope of this DPA, support Data Controller in Data Controller's compliance with:

a. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing in accordance with Section II above and Appendix B to this DPA,

b. the obligation to communicate the personal data breach to the data subject when such breach is likely to result in a high risk to the rights and freedoms of natural persons,

c. the obligation to report personal data breach to the applicable supervisory authority without undue delay and, if possible, within seventy-two 72 hours after the discovery of such breach by Data Processor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons,

d. the obligation to carry out a data protection impact assessment, in case a category of data subjects and/or a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, and

e. the obligation to consult with the applicable supervisory authority prior to processing in case it is required due to high risk of processing being demonstrated via the respective data protection impact assessment.

5 / SUB-PROCESSORS

A. In the event of general written consent to utilize sub-processors in accordance with Article 28 subsection 2 of General Data Protection Regulation, Data Processor shall inform Data Controller of any planned changes with regard to additions to or replacement of sub-processors.

B. In case of Data Processor receiving the written authorisation to use a sub-processor, Data Processor shall ensure that such sub-processor is subject to the same or reasonably similar (as the case may be) data protection obligations as those specified in this DPA under EU law or the national law of the Member States.

6 / THIRD COUNTRY TRANSFER

A. Data Processor shall be permitted to process personal data through transfer of personal data to third countries or international organisations, only if instructed by Data Controller or in case such processing is required under EU or Member State law to which Data Processor is subject. In case of the latter, Data Processor shall inform Data Controller of such legal requirement prior to processing

and the transfer, unless such law prohibits the provision of such information based on important grounds of public interest, in accordance with Article 28, subsection 3 (a) GDPR.

B. Unless otherwise indicated by the instructions or approval of Data Controller or unless otherwise required under the License Agreement or geographical scope of the License, Data Processor shall not (i) disclose personal data to Data Controller in a third country or in an international organisation; or (ii) assign the processing of personal data to a sub-processor in a third country.

C. In case a transfer to a third country should be required in order to perform the services as agreed between the parties, the parties agree to enforce Standard Contractual Clauses, as attached to this DPA in Appendix C, in order to ensure an adequate level of protection for the personal data prior the planned transfer, unless the transfer is based on an adequacy decision by the European Commission as set forth in Article 45 GDPR.

7 / PERSONAL DATA BREACH

A. Upon knowledge of a personal data breach at the Data Processor's facilities or systems or a sub-processor's facilities, Data Processor shall notify Data Controller, without undue delay. In any case, Data Processor shall notify Data Controller within forty-eight (48) hours after Data Processor has discovered the breach in order to enable Data Controller to comply with its obligations stipulated in the General Data Protection Regulation.

B. According to Section 3 of this DPA, Data Processor shall – as applicable to the nature of the processing and the means available – assist Data Controller in the reporting of the breach to the supervisory authority.

C. In furtherance to Section 4(B) above, Data Processor may be required to support Data Controller in obtaining the information listed below which, as stipulated by the Article 33, subsection 3 of the General Data Protection Regulation, shall be included in Data Controller's report to the supervisory authority:

   a. The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and their categories along with the approximate number of affected personal data records;
   b. Probable consequences of a personal data breach; and
   c. Measures, which have been undertaken or are planned to be undertaken to manage and remedy the personal data breach, including, if applicable, measures to limit the potential damage.

8 / CONTACT INFORMATION

In case of any required assistance, instruction or information/notifications, as described herein, and in the General Data Protection Regulation, Data Controller will be able to contact Data Processors through the Data protection Officer as described below.

Data Processor [Data Protection Officer]:

Stefan Hofbeck

dataprotection@fieldcode.com

9 / MISCELLANEOUS

A. This DPA shall become effective on the date of the acceptance of this DPA by the Customer.

B. Data Controller acting in good faith shall be entitled to request the amendment to this DPA if changes to the law or inexpediency of the provisions contained herein require such amendment. Each Party may by at least thirty (30) calendar days' prior written notice to the other Party, request in writing any variations to this DPA if they are required as a result of any change in any Data Protection Laws to allow processing of Customer personal data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (a) the Parties shall use commercially reasonable efforts to accommodate such required modification; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Data Processor to protect the Data Processor against additional risks, or to indemnify and compensate Data Processor for any further steps and costs associated with the variations made herein at Customer's request.

C. This DPA may be terminated according to the terms and conditions of the GT&Cs and or separate Individual Agreement with the Customer, if any.

D. This DPA shall remain in force until the termination of the processing and fulfilment of the Section 8(E) by Data Processor and any sub-processors which shall last until the earlier of (i) completion of processing by Data Processor; or (ii) termination of the License between the Parties.

E. On termination of the processing activities described herein, Data Processor shall, at Data Controller's discretion, erase or return all personal data to the Data Controller and shall erase existing copies unless EU law or Member State law requires storage of the personal data or one (1) copy retention for archival purposes.

Appendix A – Details of the processing of personal data

I. **Purpose of the processing**

The purpose of processing of personal data on behalf of Data Controller is:

Processor shall process personal data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) processing for Data Controller as part of its provision of the services; (iii) processing to comply with Data Controller's reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the processing shall be performed; (iv) processing as required under the laws applicable to Data Processor, and/or as required by a court of competent jurisdiction or other competent governmental authority, provided that Data Processor shall inform Data Controller of the legal requirement before processing, unless such law or order prohibit such information on important grounds of public interest.

II. **Nature of the processing**

The processing of personal data on behalf of Data Controller shall mainly pertain to:

Storing Data Controller's data within Data Processors system (Fieldcode Software) to provide the appropriate License under License Agreement.

III. **Types of personal data**

The processing of personal data shall include the following types of personal data about data subjects:

Data Controller:

i. User Name
ii. Email address
iii. Telephone number

Customer may submit further personal data in order to use the services of Fieldcode as offered and agreed within the Agreement, the extent of which is determined and controlled by Customer in its sole discretion.

IV. **Categories of data subjects**

The Processing includes the following categories of data subjects:

Customer may submit Personal Data to the Fieldcode Software which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Employees, agents, advisors, freelancers of Customer (who are natural persons)

- Prospects, customers, business partners and vendors of Customer (who are natural persons)

- Employees or contact persons of Customer's prospects, customers, business partners and vendors

- Any other third party individual with whom Customer decides to communicate through the Services

No special categories of data subject are process under this DPA, unless otherwise specified in the Privacy Policy of Fieldcode.

V. **Duration of processing**

Subject to any section of the DPA and/or the Agreement dealing with the duration of the processing and the consequences of the expiration or termination thereof, Data Processor will process personal data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Appendix B
TECHNICAL AND ORGANIZATION MEASURES OF DATA PROCESSOR

All existing technical and organizational measures are reviewed with regard to their compliance to "privacy by design/privacy by default" according to Art. 25 GDPR on a regular base. The customer specific requirements for data protection are taken into account when implementing new projects/contracts and if necessary, adapted to the specifications in accordance with the projectbased IT system.
The measures that need to be taken in terms of data protection law are implemented at Fieldcode as follows:

Physical Access Control (Entry Control)

Access to the premises of Fieldcode is only possible for authorized persons (employees). • Any access to the building is only possible with the RFID employee ID card or individual access control through an employee at the reception.
• Access to the offices and the floors is only possible via RFID employee ID card or accompanied by Fieldcode employee (visitor badge registered at the reception).
• Server rooms and IT admin offices have been defined as high security areas and are secured by a separate physical lock and via RFID system. All accesses are protocolled / ISO is informed before entering.
• Entry points to server rooms / hallways which lead to server rooms are being surveilled by CCTV.
• Buildings which host our mirrored data centers are physically controlled by an external security company outside of business hours.
• Physical key management including protocols for handing out and handing in is in effect.
Third parties are signing a Non Disclosure Agreement when entering high security areas. They are escorted by Fieldcode staff when performing work in the data center.

System Access Control (Access Control)

• Any electronic access to the Fieldcode system via network is protected by a firewall technology. External access to the network is secured via VPN technology and SSL encryption.
• Access data to server systems is only known to a dedicated group of administrators. Access passwords of all employees and systems must be changed on a regular basis (automatically controlled, requirements for the password are pre-set).

Data Access Control (Intervention Control)

The data access is only possible via Fieldcode's own software solution and its access modules.
• Password protection for accessing the basic system
• Critical passwords are accessible via password-software only (2-step password protection)
• Usage of personalized "Admin-Accounts" for highly secured systems/applications
• Role-based permission concept ensures very detailed and easy to control permission levels

Employees only have access to such personal data which is required for carrying out their work. Any customer-specific requirement for data access control can be realised within Fieldcode's own system.

Transmission Control (Transfer Control)

Any electronic transmission/transfer of data is only made by means of automated projectspecifically designed interfaces within the Fieldcode system environment. Each access to existing interfaces is controlled via access rights. A stand-alone automated export of data to other systems is prevented effectively. Every user works exclusively through the Fieldcode system module via an encrypted connection which is enabled for him/her.

Input Control

Changes to HW-systems, applications and data, as well as all admin activities, are protocolled and can be reported/reviewed if needed.
A distinction is made between non-editable and editable system fields. Non-editable fields cannot be manipulated or modified by the user in the system. Any changes to editable system fields are logged by the system by saving the user, date and time. Each change is evidently deposited in the daily system backup.

Job Control (Order Control)

Every employee is bound in writing to comply with the applicable guidelines of the Federal Protection Act (BDSG neu) § 53 and to the internal Non-Disclosure Agreement. Project staff is additionally committed in writing to comply with certain job-specific regulations, if required.
Potential third party contractors are subjected to extensive checks before being assigned "Fieldcode Authorized Partner" status. Audits are conducted on site at the HAPs.

Availability Control

Availability/Integrity hazards are included in the Fieldcode Risk Analysis which is reviewed regularly by ISO and CEO. Safety measures are defined and carried out / protocolled via Business Continuity Processes.
It is ensured through system settings and procedures that personal data provided to Fieldcode is protected against accidental destruction or loss.

- The data protection policy is based on daily, weekly and monthly data backup. The various data backups are stored on physically separated storage media in different fire zones to the server system.
- Fieldcode has a non-disruptive power supply in the server and network area available. The server room is redundantly air-conditioned.
- A consistent anti-virus concept is installed up to a work place client basis. o All IT systems are password-protected.
- Personal data will exclusively be stored on safe and access restricted network drives.

Requirement/ Control of Separation

There are separate and independent IT structures for test and production systems available. Every project existing at Fieldcode is deposited in its own and separate database structures (separate order data processing). Each database instance (project) is kept in a separate table. It is being strictly distinguished and divided between inventory data (analyses, reports etc.) and usage data. The minimum principle applies, i.e. only such data is shown that is necessary for the ticket.

Organisation Control

Any irregularity in the IT infrastructures is reported via monitoring tools PRTG and/or Grafana in real-time. Automatic and/or manual correction measures will be taken thereafter. Data recovery exercises are carried out on a regular basis.

Appendix C

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 - **Purpose and scope**

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

(b) The Parties:

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

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

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

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

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

Clause 2 - **Effect and invariability of the Clauses**

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

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

Clause 3 – **Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

v. Clause 13;

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

vii. Clause 16(e);

viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

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

Clause 4 – **Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – **Hierarchy**

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

Clause 6 – **Description of the transfer(s)**

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

Clause 7 – **Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – **Data protection safeguards**

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

TRANSFER CONTROLLER TO PROCESSOR

8.1 – **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 – **Purpose limitation**

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

8.3 – **Transparency**

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

8.4 – **Accuracy**

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

8.5 – **Duration of processing and erasure or return of data**

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

8.6 – **Security of processing**

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

exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 – **Sensitive data**

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

8.8 – **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union(4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 – **Documentation and compliance**

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of

non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

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 three (3) weeks 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. 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([2]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress
(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    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.

[2] 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.

(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 INC ASE 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(12);
    iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the. 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.

SECTION IV – FINAL PROVISIONS

Clause 16 – **Non- compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    ii. the data importer is in substantial or persistent breach of these Clauses; or
    iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) 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 Nuremberg, 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.