**STANDARD CONTRACTUAL CLAUSES 2021/915 BETWEEN CONTROLLERS AND PROCESSORS**

**Clause 1**

**Purpose and scope**

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with:

[ ]  Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

[ ]  Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018on 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.

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

**Clause 2**

**Invariability of the Clauses**

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

**Clause 3**

**Interpretation**

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

**Clause 4**

**Hierarchy**

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

 **Clause 5**

**Docking clause**

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

[ ]  **Include this Clause!** **(Note: If you do not tick this click-box, the clause will not be included!)**

**Clause 6**

**Description of the processing(s)**

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

 **Clause 7**

**Obligations of the Parties**

**7.1. Instructions**

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor’s opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

**7.2. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

**7.3. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

**7.4. Security of processing**

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

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

**7.5. Sensitive data**

If the processing 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 (“sensitive data”), the processor shall apply specific restrictions and/or additional safeguards.

**7.6.** **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller’s request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

**7.7.** **Use of sub-processors**

(a)

[ ]  PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller’s prior specific written authorisation. The processor shall submit the request for specific authorisation at least Please click here to add a text. prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

[ ]  GENERAL WRITTEN AUTHORISATION: The processor has the controller’s general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least Please click here to add a text. in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor’s obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfill its contractual obligations.

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

**7.8.** **International transfers**

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

**Clause 8**

**Assistance to the controller**

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects’ requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller’s instructions

(c) In addition to the processor’s obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a ‘data protection impact assessment’) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in

[ ]  Article 32 of Regulation (EU) 2016/679/

[ ]  Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

**Clause 9**

**Notification of personal data breach**

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

**9.1.** **Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to

[ ]  Article 33(3) of Regulation (EU) 2016/679

[ ]  Article 34(3) of Regulation (EU) 2018/1725

shall be stated in the controller’s notification, and must at least include:

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to

[ ]  Article 34 of Regulation (EU) 2016/679

[ ]  Article 35 of Regulation (EU) 2018/1725

with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

**9.2.** **Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under

[ ]  Articles 33 and 34 of Regulation (EU) 2016/679

[ ]  Articles 34 and 35 of Regulation (EU) 2018/1725

**Choose the suitable OPTION! (Note: You need to tick one of both click-boxes!)**

**Clause 10**

**Non-compliance with the Clauses and termination**

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

**ANNEX I**

**List of parties**

**Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller’s data protection officer]**

**Controller 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.

Where applicable, the controller’s data protection officer Please click here to add a text.

|  |  |
| --- | --- |
| Accession date: Please click here to add a text. First and Last Name (written out in full):Please click here to add a text.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature |

Processor(s): **[Identity and contact details of the processor(s) and, where applicable, of the processor’s data protection officer]**

**Processor 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.

Where applicable, the processor’s data protection officer Please click here to add a text.

|  |  |
| --- | --- |
| Accession date: Please click here to add a text. First and Last Name (written out in full):Please click here to add a text.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature |

**ANNEX II**

**Description of the processing**

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

[ ]  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 processed**

[ ]  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 processed (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 processed**

[ ]  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.

**Nature of the 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) for which the personal data is processed on behalf of the controller**

Please click here to add a text.

**Duration of the processing**

[ ]  The data is processed on a one-off.

[ ]  The data is processed on a continuous basis.

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

**For processing by (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.

**ANNEX III**

**Technical and organisational measures including technical and organisational measures to ensure the security of the data**

**EXPLANATORY NOTE:**

**The technical and organisational measures need to be described concretely and not in a generic manner.**

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

**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

[x]  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.

**ANNEX IV**

**List of sub-processors**

**EXPLANATORY NOTE:**

**This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).**

The controller has authorised the use of the following sub-processors:

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.

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

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

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

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Please click here to add a text.