

## DATA PROCESSING AGREEMENT

based on the standard contractual clauses of the Commission according to  
ART. 28 (7) GDPR

- hereinafter also referred to as the „Agreement“ -

## TABLE OF CONTENTS

<b>SECTION I – General Provisions</b>	<b>3</b>
Clause 1 – Purpose and scope	3
Clause 2 – Invariability of the Clauses	3
Clause 3 – Interpretation	3
Clause 4 – Hierarchy	3
Clause 5 – Docking clause - Optional	Error! Bookmark not defined.
<b>SECTION II – OBLIGATIONS OF THE PARTIES</b>	<b>4</b>
Clause 6 – Description of processing(s)	4
Clause 7 – Obligations of the Parties	4
7.1. Instructions	4
7.2. Purpose limitation	4
7.3. Duration of the processing of personal data	4
7.4. Security of processing	4
7.5. Sensitive data	4
7.6. Documentation and compliance	5
7.7. Use of sub-processors	5
7.8. International transfers	6
Clause 8 – Assistance to the controller	6
Clause 9 – Notification of personal data breach	7
9.1. Data breach concerning data processed by the controller	7
9.2. Data breach concerning data processed by the processor	7
<b>SECTION III – FINAL PROVISIONS</b>	<b>9</b>
Clause 10 – Non-compliance with the Clauses and termination	9
<b>Annex I – Supplementary provisions</b>	<b>10</b>
Clause 11 - General Provisions	10
Clause 12 - Special Provisions	10
Clause 13 - Special Provisions	10
<b>Annex II – List of parties</b>	<b>14</b>
<b>Annex III – Description of the processing</b>	<b>15</b>
<b>Annex IV – Technical and organisational measures</b>	<b>16</b>
<b>Annex V – List of subprocessors</b>	<b>17</b>

## SECTION I – General Provisions

### 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, in the following: GDPR).
- (b) The controllers and processors listed in **Annex II** have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR.
- (c) These Clauses apply to the processing of personal data as specified in **Annex III**.
- (d) **Annexes I to V** are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR.

### Clause 2 – Invariability of the Clauses

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

### Clause 3 – Interpretation

- (a) Where these Clauses use the terms defined in the GDPR, 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 the GDPR.
- (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

- (a) In the event of a contradiction between this Data Processing Agreement and the provisions of any related agreements between the Parties existing or subsequently entered into or concluded (such agreements hereinafter also referred to as "**Principal Agreement**"), the provisions of this Data Processing Agreement shall prevail.
- (b) In the event of a conflict between the supplementary clauses in **Annex I** and other provisions of this Data Processing Agreement, the other provisions of this Data Processing Agreement shall take precedence over the supplementary clauses in **Annex I**.

## **SECTION II – OBLIGATIONS OF THE PARTIES**

### **Clause 6 – Description of 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 III**.

### **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 the GDPR 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 III**, 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 III**.

#### **7.4. Security of processing**

- (a) The processor shall at least implement the technical and organisational measures specified in **Annex IV** 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 the GDPR. 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) **OPTION 1: 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 [SPECIFY TIME PERIOD] 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 V. The Parties shall keep Annex V up to date.
- (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 the GDPR.
- (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 fulfil 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 fulfil 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 the GDPR.
- (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 the GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, 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 GDPR.
- (d) The Parties shall set out in **Annex IV** 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 GDPR, 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) GDPR, shall be stated in the controller's notification, and must at least include:
  - (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 GDPR, 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.

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

- (a) 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:
  - (1) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
  - (2) the details of a contact point where more information concerning the personal data breach can be obtained;
  - (3) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

- (b) 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) 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 GDPR.



## SECTION III – FINAL PROVISIONS

### Clause 10 – Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of the GDPR, 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 the GDPR;
  - (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 the GDPR.
- (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 – Supplementary provisions

### Clause 11 - General Provisions

- (a) **Scope:** The clauses contained in this Agreement shall apply to all services involving processing of personal data by the Processor on behalf of the Controller within the meaning of Art. 28 GDPR.
- (b) **Form:** Any amendments or additions to this Agreement shall be made at least in text form and must expressly state that they amend and/or add to these provisions. This also applies to a waiver of this text form requirement. Insofar as this Agreement stipulates the written form, the written form as defined by Sect. 126b of the German Civil Code ("*Bürgerliches Gesetzbuch*", "*BGB*") shall be sufficient.
- (c) **Choice of law:** This Agreement is subject to German law.
- (d) **Place of jurisdiction:** The place of jurisdiction shall be Germany.

### Clause 12 – NOT USED

### Clause 13 - Special Provisions

- (a) **Contractual penalty:** For each case of culpable infringement of the provisions of this Agreement and/or the applicable data protection provisions by the Processor, its legal representatives, subcontractors, employees or its agents, the Processor undertakes to pay an appropriate contractual penalty. The amount shall be determined by the Controller at its reasonable discretion and, in the event of a dispute, shall be subject to review by the competent court at the Controller's registered office. This shall be without prejudice to the establishment of further claims for damages or release, whereby any contractual penalty paid by the Processor to the Controller in accordance with its obligation under this paragraph shall be set off against any damages payable by the Processor to the Controller on account of the same breach of duty.
- (b) **Liability:**
  - (1) The Processor shall be liable to the Controller in accordance with the statutory provisions. Any limitations or restrictions of liability of the Parties under the Principal Agreement or other contractual agreements shall not apply in this respect.
  - (2) The Processor shall also be liable in case its employees or agents are in breach of data protection provisions and/or process personal data against or without instructions from the Processor.
  - (3) The Processor's liability towards the Controller shall also extend to any fines imposed on the Controller, insofar as such fines are attributable to the culpable breach of one of the Processor's obligations under data protection law by the Processor, its employees or its agents. If, as a result of such a breach of obligation, an order imposing a fine on the Controller becomes final, the Processor shall indemnify the Controller, and hold the Controller harmless, from the fine imposed, with the amount of such release determined in accordance

with the internal proportion of liability in relation between the Parties. The proportion of the fine to be borne by the Processor shall depend on its share of responsibility for the breach sanctioned by the fine. In any event, the aforementioned liability on the part of the Processor shall be subject to the condition precedent that the Controller notifies the Processor in writing without undue delay of any such case, does not acknowledge the alleged breach, and conducts any judicial or extrajudicial dispute, including any out-of-court settlement, only in consultation with the Processor. The Processor may in particular request that the Controller have any fine notices judicially reviewed by all available competent bodies, in which case the Processor shall be obligated to indemnify the Controller, and hold the Controller harmless, from the legal costs incurred in the amount of the statutory fees.

- (4) The Processor shall indemnify the Controller, and hold the Controller harmless, from any claims for damages by data subjects in connection with a breach of data protection provisions which they assert against the Controller, insofar as such claims are based on the fact that the Processor has breached obligations specifically directed to it as a Processor or has processed personal data on the Controller's behalf without or contrary to an instruction from the Controller. The provisions in the above 0(b)(3) Sentence 4 and 5 of this Annex I shall apply accordingly.

(c) **Persons Authorised to Issue Instructions**

Insofar as the Controller deems it necessary, it shall designate in writing to the Processor those persons (including their respective contact details) who shall be exclusively authorised on its side to issue processing instructions to the Processor in accordance with the provision in Clause 7(1)(a) of this Agreement. Insofar as the Controller makes use of this right, only instructions from these persons and via the communication channels determined by the Controller shall be legally binding within the meaning of the provision in Clause 7(1)(a) of this Agreement. The Controller shall notify the Processor of any changes with regard to the persons authorised to issue instructions on the part of the Controller or their respective contact details.

(d) **Location of Data Processing**

- (1) The processing of personal data on behalf of the Controller off of the Processor's business premises shall only be permitted with the written consent of the Controller.
- (2) The processing and use of the personal data shall be performed exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another contracting state of the European Economic Area. This shall also apply to any data backups by the Processor. This shall not affect the provision in Clause 7(8) of this Agreement.

(e) **Monitoring Obligations**

- (1) The Processor undertakes to ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller is processed exclusively in accordance with this Agreement, any Principal Agreement as well as the Controller's processing instructions issued on the basis of this Agreement.
- (2) The Processor shall structure its enterprise and its business processes in such a way that the data, which it processes on the Controller's behalf, is secured to the necessary extent and

protected against unauthorised disclosure to and access by any third parties. The Processor shall agree in advance with the Controller on any changes in the organisation of the data processing on behalf of the Controller which are relevant to the security of the data.

- (3) The Processor shall confirm in writing or in text form that it has designated a data protection officer in accordance with Art. 37 GDPR and, if applicable, in accordance with Sect. 38 of the German Federal Data Protection Act (BDSG), and that it monitors compliance with the provisions on data protection and data security with due involvement of the data protection officer.

If the Processor is not subject to the provisions of Art. 37 GDPR and Sect. 38 BDSG, or not obliged to designate a data protection officer, it shall name a reliable contact person to monitor compliance with data protection and data security regulations and to act as a contact person for enquiries relating to data processing. The Processor shall notify the Controller of the name and contact details of its data protection officer or, respectively, the contact person as well as of any changes thereto in writing or in text form without undue delay.

- (f) **Records of Processing Activities:** As regards the Controller's establishment and maintenance of the records of processing activities pursuant to Art. 30 GDPR, the Processor shall support the Controller and make the necessary information available in an appropriate manner. Pursuant to Art. 30(2) GDPR, the Processor shall also maintain its own records of all processing activities carried out on behalf of the Controller.
- (g) **Assistance with Data Subject Requests:** In addition to Clause 8(b), the Processor shall provide all cooperation and assistance (in particular by way of providing pertaining information) required thereunder without undue delay and in such a timely manner as to enable the Controller to fulfil its obligations to comply with data subject rights in a timely manner. To the extent that the processed data is the subject of a request for data portability under Art. 20 GDPR, the Processor shall also be obliged to provide the data records concerned to the Controller without undue delay in a structured, commonly used and machine-readable format.
- (h) **Notification Obligations:**
- (1) The obligation for the Processor to notify the Controller without undue delay in the event of a personal data breach involving the data processed by the Processor (Clause **Error! Reference source not found.**) shall also apply in particular to breaches which have occurred in the course of the processing by persons employed by the Processor or by other third parties entrusted with the processing. The notification obligation shall also apply in the event of indications suggesting a potential breach of the security of the personal data processed on the Controller's behalf as well as in the event of breaches of the provisions made in the Principal Agreement and the agreements and / or of the instructions issued by the Controller.
- (2) The obligation for the Processor to notify the Controller without undue delay in the event of a personal data breach involving the data processed by the Processor (Clause **Error! Reference source not found.**) shall include the obligation

for piecemeal notification. Partial notifications must therefore also be made without undue delay.

- (3) If access to the data which the Controller has transmitted to the Processor for data processing is jeopardised by third-party measures (e.g. measures taken by an insolvency administrator, confiscation by tax authorities, etc.), the Processor shall inform the Controller of this without undue delay.
- (4) **Forwarding of data subject requests:** If a data subject contacts the Processor directly to request access to their personal data, as specified in **Annex III** to this Agreement, or to have such data rectified, erased, or its processing restricted, the Processor shall forward this request to the Controller without undue delay upon receipt.
- (5) **Monitoring by the supervisory authority:** The Processor shall inform the Controller of any monitoring measures implemented by the supervisory authority, insofar as the measures may involve data processing that the Processor performs for the Controller.
- (i) **Confidentiality Agreement:** The Processor shall also obligate its employees, in accordance with the requirements of the Controller, to comply with any mandatory statutory confidentiality obligations applicable to the Controller. The Processor shall provide the Controller, upon request, with appropriate proof of compliance with this obligation as well as with its obligation under Clause **Error! Reference source not found.** Sentence 2 of this Agreement.
- (j) **Defence of the Right of Retention:** Any defence of the right of retention pursuant to Sect. 273 of the German Civil Code (BGB) with regard to the data processed and the associated data carriers shall be excluded.
- (k) **Documentation of Data Erasure:** The erasure of data after termination of the data processing on the Controller's behalf (see **Error! Reference source not found.** of this Agreement) in accordance with the data protection and data security provisions shall be documented by the Processor and confirmed to the Controller upon request by submitting the deletion log.

## Annex II – List of parties

**Controller #1** : *[Name and contact details of the Controller(s) and, if applicable, of the Controller's data protection officer]*

- Name: SEFE Securing Energy for Europe GmbH
- Address: Markgrafenstrasse 23, 10117 Berlin, Germany
- Contact details of the Data Protection Office / Data Protection Officer: [dataprivacy@sefe.eu](mailto:dataprivacy@sefe.eu)
- 

**Processor #1**: *[Name and contact details of the Processor(s) and, if applicable, of the Processor's data protection officer]*

- Name: [...]
- Address: [...]
- Name, role and contact details of the contact person: [...]
- 

[...]

...

## Annex III – Description of the processing

### *Object of the data processing on the Controller's behalf:*

The Processor may process personal data on behalf of the Controller for the purpose of delivering the Services, specifically:

- System Integration Services: Including the design, configuration, and implementation of integrated IT systems across the Controller's business units and third-party platforms.
- Application Development Services: Including the design, coding, testing, deployment, and enhancement of bespoke software applications used by the Controller and its business Clients.
- Application Maintenance Services: Including ongoing support, bug fixing, performance optimization, and updates to existing applications.
- Quality Assurance Services: Including the planning and execution of testing activities to ensure software reliability, functionality, security, and compliance with agreed standards and requirements.
- 

These services are intended to support the Controller's business operations in the energy sector, including customer management, billing, analytics, and operational efficiency.

The Processor shall, where applicable, capture under each Individual Contract, details of any personal data due to be processed relating to such Individual Contract.

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

Data subjects whose personal data may be processed shall include, but may not be limited to:

- Employees and contractors of the Controller
- Business customers and partners of the Controller
- End users of the Controller's applications and platforms

### • *Categories of personal data processed:*

Depending on the specific services provided, the Processor may process the following categories of personal data:

- - Identification data (e.g., names, job titles, business contact details)
  - - System usage data (e.g., IP addresses, access logs, error logs)
- - Business customer data (e.g., company names, service usage, billing information)
- - Technical metadata related to application performance and user interactions

The Processor shall, where applicable, capture under each Individual Contract, details of any personal data due to be processed relating to such Individual Contract. No special categories of personal data (as defined under Article 9 of the GDPR) are intended to be processed unless explicitly agreed in writing



## **Annex IV – Technical and organisational measures**

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR and other applicable data protection laws. These measures shall include, at a minimum:

### **1. Access Control**

- Restrict access to personal data to authorised personnel only.
- Implement role-based access and least privilege principles.
- Use strong authentication mechanisms (e.g., multi-factor authentication).

### **2. Data Encryption**

- Encrypt personal data in transit (e.g., TLS/SSL) and at rest using industry-standard algorithms.
- Secure cryptographic key management practices.

### **3. Network and System Security**

- Firewalls, intrusion detection/prevention systems, and anti-malware solutions.
- Regular patching and vulnerability management.
- Segregation of environments (development, testing, production).

### **4. Data Backup and Recovery**

- Regular backups of systems containing personal data.
- Disaster recovery and business continuity plans tested periodically.

### **5. Logging and Monitoring**

- Maintain audit logs of data access and processing activities.
- Implement monitoring for suspicious or unauthorised activities.

### **6. Physical Security**

- Secure facilities with controlled access.
- Protection against theft, damage, and environmental hazards.

### **7. Personnel Security and Training**

- Confidentiality agreements for staff handling personal data.
- Regular data protection and security awareness training.

### **8. Incident Management**

- Documented procedures for detecting, reporting, and responding to data breaches.
- Notification to the Controller without undue delay.

### **9. Data Minimisation and Retention**

- Limit processing to necessary data only.



- Implement secure deletion or anonymisation at the end of retention periods.

This Annex provides a high-level framework. Detailed and specific measures (e.g., encryption standards, backup frequency, penetration testing schedules) shall be defined in Individual Contract or Schedule 3 (security).

## Annex V – List of subprocessors

The Processor currently has engaged the following other processors in its fulfilment of the data processing, and the Controller hereby agrees to their commissioning.

To the extent the data processing takes place outside the European Economic Area or that data is accessed from outside the European Economic Area, the following overview must also list the measures and safeguards which ensure an appropriate level of data protection during processing in accordance with Art. 44 ff. GDPR (e.g. EU standard contractual clauses, BCR or EU Commission adequacy decision).

Company name and registered office (address)	Role/activity and nature of data processing	Categories of data processed	Location(s) of data processing (including by remote access)	Measures and safeguards for transfers to a non-EEA member state without adequate level of data protection
Text	Text	Text	Text	Text
Text	Text	Text	Text	Text
Text	Text	Text	Text	Text