

## **Data Processing Agreement under Art. 28 und 29 of Regulation (EU) 2016/679**

between

### **Controller**

subsequently called as „Controller“  
and

#### **1. PlanRadar GmbH**

FN 400573 d  
Schottenring 16, DG 1  
1010 Vienna  
Austria

and

#### **2. PlanRadar SOFTWARE S.R.L.**

17-19A Ploiești Str., Ground Floor, Ap. 45  
400157 Cluj-Napoca  
Romania

collectively called as “Processors” or “Joint processors”, each individually called as the „Processor“, and together with the Controller referred as the “Parties”

### ***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.
- (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.
- (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.
- (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.

## ***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.

## ***3. Interpretation***

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 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 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 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

## ***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.

## ***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.

## SECTION II – OBLIGATIONS OF THE PARTIES

### ***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 II.

### ***7. Obligations of the Parties***

#### **7.1. Instructions**

- (a) The joint processors shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which any of the processor is subject. In this case, each 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 joint processors shall immediately inform the controller if, in either processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

#### **7.2. Purpose limitation**

The joint processors 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 joint processors shall only take place for the duration specified in Annex II.

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

- (a) The joint processors 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 joint processors 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. Each 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 joint processors 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 joint processors shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The joint processors 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. At the controller's request, the joint processors 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 joint processors.
- (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 joint processors 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) Neither 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 processors shall submit the request for specific authorisation at least 4 weeks 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.
- (b) Where either 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 processors in accordance with these Clauses. Each processor shall ensure that the sub-processor complies with the obligations to which either processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

- (c) At the controller's request, each 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, each processor may redact the text of the agreement prior to sharing the copy.
- (d) The joint processors shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. Each processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The joint processors shall agree a third party beneficiary clause with the sub-processor whereby - in the event that either 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 joint processors 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 either processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
- (b) The controller agrees that where either 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 processors 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.

#### **8. Assistance to the controller**

- (a) Each 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) Each 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), each processor shall comply with the controller's instructions
- (c) In addition to the processors' obligation to assist the controller pursuant to Clause 8(b), the processors 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 processors:
  - (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 processors become aware that the personal data it is processing is inaccurate or has become outdated;
  - (4) the obligations in Article 32 Regulation (EU) 2016/679.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processors are required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

### ***9. Notification of personal data breach***

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

#### **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 joint processors 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) Regulation (EU) 2016/679/, 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 Regulation (EU) 2016/679, 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 joint processors**

In the event of a personal data breach concerning data processed by the joint processors, each processor shall notify the controller without undue delay after either 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 joint processors when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## **SECTION III – FINAL PROVISIONS**

### ***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 joint processors are in breach of its obligations under these Clauses, the controller may instruct either processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. Each 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 either 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) either 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) either 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) Each 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 joint processors 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, each processor shall continue to ensure compliance with these Clauses.

**Vienna, date** \_\_\_\_\_

**Place, date** \_\_\_\_\_

**For PlanRadar GmbH  
and PlanRadar SOFTWARE S.R.L.**

**For Controller**

## ANNEX I LIST OF PARTIES

### **Controller(s):**

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

### **Processor(s):**

1. PlanRadar GmbH

FN 400573 d

Kärtner Ring 5-7

1010 Vienna

Austria

2. PlanRadar SOFTWARE S.R.L.

17-19A Ploiești Str., Ground Floor, Ap. 45

400157 Cluj-Napoca

Romania

Contact person's name, position and contact details:

Name and contact data of the data protection officer: Constantin Köck,

[c.koeck@planradar.com](mailto:c.koeck@planradar.com)

## **ANNEX II: DESCRIPTION OF THE PROCESSING**

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

- The users of the PlanRadar software-as-a-service solution, who have been invited to the projects by the Controller (e.g. customers, subcontractors, employees)

### *Categories of personal data processed*

- Communication data (e-mail address, optional telephone number)
- Contract data (name, e-mail, company)
- Ticket information (creator, creation date, modification date, voice memo)

### *Nature of the processing*

- Depending on the user's needs, the processing includes the collection, recording, organisation, classification, storage, adaptation or alteration, retrieval, consultation, use, transmission, alignment or combination, restriction, or deletion of data.

### *Purpose(s) for which the personal data is processed on behalf of the controller*

- To provide the PlanRadar software-as-a-service solution for construction documentation, task and defect management, in particular to simplify documentation and communication in construction and real estate projects. For this purpose, the user can process data on projects, tasks, individual work steps and the respective persons involved via the cloud-based software.

### *Duration of the processing*

- The duration of the processing shall be governed by the main contract. In addition, the controller may terminate the contract in accordance with clause 10.

### *For processing by (sub-)processors:*

- The storage of data in the cloud (Cloud Hosting) is carried out by sub-processor (see Annex IV). The duration of the processing depends on the main contract.

**ANNEX III - TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**A. Entrance control**

*The aim is to protect access to data processing facilities where personal data is processed or used from unauthorized individuals.*

| <b>Measure</b>                                | <b>Description</b>  |
|---|---|
| Alarm systems                                 | The alarm systems for securing a building against break-ins and other criminal activities are in place. In the event of an alarm-triggering incident, an immediate notification is sent to a central security center.   |
| Data centers*                                 | The data centers, servers, and host software systems are locked in unassuming buildings. They are secured through physical security measures to prevent unauthorized access, both outside the premises (via fences and walls) and within the buildings.   |
| Alarm systems at server locations*            | Access to server locations is secured by alarm systems that trigger an alert when the door is compromised.  |
| Automatic access control at server locations* | Access to server locations is managed through electronic access controls that trigger an alarm if the door is tampered with or held open.   |
| Chip cards and expense control                | Security against unauthorized entry is maintained with chip cards. An official chip card handover sheet must be signed by every employee. Chip cards must not be given to other persons.  |
| Visitor record                                | Visitors must always identify themselves, and they are always accompanied by the employees.   |
| Visitor record at server locations*           | Visitors are required to identify themselves and go through the registration process, and they are continuously accompanied by authorized personnel. Access authorization is granted by an authorized person and revoked within 24 hours after an employee or supplier record has been deactivated. |
| Porter/guard                                  | Porter and security services monitor access to the building.  |

|  |   |
|--|---|
| Porter/guard at server locations *       | Porter and security services monitor access to the building and sensitive areas. Trained security personnel guard the data centers and the surrounding area 24/7. |
| Video surveillance                       | Video monitoring has been implemented throughout the building to oversee access control.  |
| Video surveillance at server locations * | Access to sensitive areas at data centers is monitored through video surveillance.  |

## B. Access control

*The goal is to prevent unauthorized individuals from using data processing systems.*

| <b>Measure</b>                 | <b>Description</b>   |
|--------------------------------|--|
| User rights at data centers*   | Each user is provided with a unique ID to ensure that all system components can only be accessed by authorized users and administrators. The creation, deletion, and modification of user IDs, login credentials, and other identification features are logged along with a timestamp.   |
| User profiles                  | User accounts are initially provisioned with the least access rights; periodic reviews of assigned permissions, especially for administrative user accounts, are conducted.  |
| User profiles at data centers* | User access is only enabled once the HR department creates a corresponding record in the HR system. The principle of least privilege on a 'need-to-know' basis is followed. The granted access rights to IT systems are subject to quarterly review by authorized personnel. Access permissions are promptly revoked when they are no longer necessary for the user's tasks. |
| Password assignment            | Passwords/passphrases for initial login are comprised of a unique value and must be changed immediately after the first use.   |

|   |   |
|---|---|
| Authentication                                  | Authentication is secured by username and password. In addition, multi-factor authentication has been introduced, which is based on at least two of the following factors (PIN codes or biometric features).  |
| Password-Policy                                 | Security measures include the implementation of automatic account lockouts after repeated failed login attempts and the activation of two-factor authentication for particularly important accounts.  |
| Password-Policy at data centers*                | User passwords must be changed at least every 90 days. Only complex passwords are allowed. Changing the password through simple password variations, such as altering a single character, is not permitted.   |
| Clean-Desk/Clear-Screen-Policy                  | All employees are instructed to store all documents and materials in lockable cabinets or drawers when leaving their workplace. Automatic locking mechanisms for computers/laptops/notebooks when leaving the workspace or during periods of inactivity. Paper documents containing confidential information are shredded or properly disposed of. Chip cards and other physical access methods are securely stored and not openly visible. |
| WLAN policy                                     | Visitors may only use the dedicated guest-WiFi. Employees must not reveal or give visitors access to the main WLAN-network.   |
| Intrusion Detection/Intrusion Prevention System | Early attack detection, vulnerability identification, safeguarding critical resources, logging and reporting, as well as regular updates and maintenance, are all in place.   |
| Firewalls                                       | Hardware- and software firewalls are deployed and serve as essential elements to protect your network from unauthorized access, cyber threats, and potential security breaches.   |
| Hardware firewall at data centers*              | Antivirus software has been deployed, featuring both an email filter and malware detection capabilities.  |
| Software firewall at data centers*              | Firewall devices have been set up to limit access to the data processing environment and bolster the security of the computing clusters.  |

### C. Admittance control

*The intention is to ensure that authorized users of a data processing system can exclusively access data for which they have access permissions, and that personal data cannot be read, copied, altered, or removed without authorization during processing, use, and after storage.*

| <b>Measure</b>        | <b>Description</b>   |
|-----------------------|--|
| Anti-Virus-Software   | Access control, ensuring protection against unauthorized system usage, is fortified by antivirus software. The software performs a daily check for updates.  |
| Disk encryption       | Protection against unauthorized system usage is ensured through the encryption of data storage devices.  |
| Authorization concept | The principles of "Least Privilege," "Need-to-Know," and "Segregation of Duties" are upheld.   |
| System administrator  | Regular review of the granted permissions, particularly for administrative user accounts, is in place. The number of administrators is kept to the "essential" minimum. Unauthorized reading, copying, modification, or deletion within the system is strictly prohibited. |
| Access recording      | Recording of all access; captures data such as the username, access timestamp, access type, and other relevant information.  |
| Retention periods     | The data retention periods are either legally mandated or established based on data protection regulations.  |

### D. Input control

*The purpose is to ensure that it can be retrospectively verified and determined whether and by whom personal data in data processing systems has been entered, modified, or removed.*

| <b>Measure</b>                            | <b>Description</b>  |
|---|---|
| Processing register                       | The processing register has been created and is regularly reviewed.                                   |
| Input, modification, and deletion of data | Recording the input, modification, and deletion of data, tamper-evident email archiving, retention of |

|                        |  |
|------------------------|--|
|                        | forms from which data has been transferred to automated processing, traceability of data input, modification, and deletion through individual usernames (not user groups). |
| Protocol and log files | The determination of whether and by whom personal data has been entered, altered, or removed from data processing systems. Log and protocol files are secured.             |

### E. Disclosure control

*The intention is to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while stored on data carriers, and that, if necessary, it can be verified and determined.*

| Measure   | Description  |
|---|--|
| Pseudonymization  | Identifiers are used, where possible, instead of names.  |
| Dedicated lines or VPN tunnels                          | Access to production data is restricted to whitelisted IP addresses (access via Virtual Private Networks (VPN) or office network with dedicated line).   |
| Prevention of unauthorized copying at data centers*     | Employees are not allowed to connect personal electronic devices to information systems.   |
| Data encryption   | Unauthorized reading, copying, modification, or removal during electronic transmission or transport is prevented through the use of encryption. All data is encrypted, both during storage (Encryption at Rest) and during transmission (Encryption in Transit). |
| Deletion policy   | Deletion deadlines, applied to both data itself and metadata like log files, are in place. The data remains available for download for 30 days after the termination of the main contract and is afterwards, if permitted by law, irrevocably deleted.           |
| Recording the destruction process                       | Recording of destruction relates to documenting and recording of all processes that involve the disposal, deletion, or destruction of data.  |
| Decommissioning of storage devices in the data centers* | When a storage device reaches the end of its lifespan, all retired magnetic storage devices are demagnetized   |

|  |   |
|--|---|
|  | and physically destroyed in accordance with industry standards and applicable data protection laws. |
|--|---|

### F. Order control

*The goal is to ensure that personal data processed on behalf of data controller can only be processed in accordance with the instructions.*

| Measure   | Description  |
|---|--|
| Data confidentiality                                  | Regular employee training is implemented to ensure standard processes during employee transitions or departures.   |
| Written instructions                                  | Clear contract formulation; no data processing takes place without clear instructions from the data controller as per Art. 28 GDPR.  |
| Data destruction upon the termination of the contract | Deletion deadlines for both data itself and metadata like log files are in place. The destruction of data upon the termination of the contract is ensured.   |
| Sub-processor   | Strict selection of sub-processors (ISO certification, ISMS) and ensuring that the technical and organizational measures are also adhered to by the sub-processor through the data processing agreement. |

### G. Availability control

*The purpose is to ensure that personal data is protected against accidental destruction or loss.*

| Measure   | Description   |
|---|---|
| Uninterruptible power supply (UPS) in data centers* | The electrical systems have been designed to ensure complete redundancy and can be maintained without affecting operations. The redundant data centers operate around the clock, seven days a week. Uninterruptible Power Supply (UPS) devices ensure continuous power supply for critical areas in the event of a power outage. Generators are also installed to provide emergency power to the entire facility when needed. |

|  |  |
|--|--|
| Air conditioning in the data centers*              | Employees and relevant systems monitor the temperature and humidity in the data centers to ensure they are maintained at suitable levels.  |
| Fire extinguishing equipment in data centers*      | Automatic fire detection and suppression facilities are in place within the data centers. The fire detection system employs smoke sensors throughout all areas of the data centers, covering mechanical and electrical infrastructure, cooling rooms, and the spaces housing the generators. |
| Theft protection in data centers*                  | Secure placement of systems to ensure protection against theft.  |
| Backup/Recovery                                    | Protection against accidental or deliberate destruction or loss through backup strategy. The data is also secured through regular testing and recovery exercises. The backup and recovery concept are regularly reviewed and adapted to changing requirements and technologies.              |
| Emergency plan                                     | The regular review of the emergency plans takes place annually, ensuring integration of business continuity management.  |
| Storage of data backups at offsite location*       | The backup system is configured georedundantly, with backups stored in different buildings and different fire zones.   |
| System landscape                                   | The production systems are designed redundantly to maintain operations.  |
| Penetration tests, testing, and release procedures | Software undergoes testing and release procedures to identify and fix errors, bugs, and vulnerabilities.   |
| Protection against malware and patch management    | Regular monitoring of security update and system vulnerability status, anti-malware software, and regular implementation of security patches and updates are in place.   |

## H. Separation Control

*The endeavor is to ensure that data collected for different purposes can be processed separately.*

| <b>Measure</b>                            | <b>Description</b>   |
|---|--|
| Logical separation                        | Separate processing of data collected for different purposes: client capability, sandboxing.   |
| Separation of production and test systems | Test and production systems are logically separated to reduce the risk of unauthorized access or unauthorized changes to the production systems. |

### **I. Cryptography and Pseudonymization**

*The purpose is to ensure that information is protected from unauthorized access and remains unaltered during transmission or storage.*

| <b>Measure</b>                                   | <b>Description</b>   |
|--|--|
| Pseudonymization                                 | If feasible for the specific data processing, the primary identifying characteristics of personal data are removed within the respective data application and stored separately. |
| Encryption of data storage devices and endpoints | The encryption of data storage devices (e.g., portable hard drives, USB sticks) and endpoints (PCs, laptops).  |

### **J. Data Protection Management**

*The aim is the appropriate assignment of central responsibilities to ensure control over the measures described above and maintain a high standard of security.*

| <b>Measure</b>             | <b>Description</b>  |
|----------------------------|---|
| Data Protection Officer    | Data Protection Officer has been designated.  |
| Data protection management | Employees are committed to confidentiality and the preservation of data secrecy, including regular employee training and awareness measures.            |
| Privacy by design/default  | The implementation of opt-out instead of opt-in and privacy by default/design is implemented to enhance user data privacy and security from the outset. |
| Certifications             | ISO 27001 Certification, along with the Statement of Applicability, provides a framework for identifying,   |

|                 |  |
|-----------------|--|
|                 | controlling, and reducing the risks associated with data security.   |
| Internal audits | Security checks at the infrastructure and application levels are conducted regularly. Annual internal audit according to ISO 27001 is performed.   |
| External audits | External audits are conducted as part of the ISO 27001 certification process.  |
| Regular review  | Procedures for reviewing, assessing, and evaluating technical and organizational measures are conducted regularly.   |
| IT security     | Incident response management, attack detection, monitoring and alerting, asset management, software management and distribution, user policies for device handling, and behavior in the use of information technology are implemented. |

**Annotation:**

The marked (\*) sections pertain exclusively to data centers of our sub-processor, Amazon Web Services, as the cloud hosting provider.

## **ANNEX IV: LIST OF SUB-PROCESSORS**

### EXPLANATORY NOTE:

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

1. Amazon Webservices (Amazon Web Services EMEA SARL)  
38 Avenue John F. Kennedy, L-1855 Luxembourg

#### *Description of the processing:*

This sub-processor is used to store the data in the cloud (cloud hosting). The server location is in Frankfurt (AWS Region Europe (Frankfurt), eu-central-1). The storage of all data takes place within the European Union.