DATA PROCESSING AGREEMENT

Note 1: All subsequent personal designations refer to all genders and their linguistic forms and are always understood with the addition “(m/f/d)”.

Note 2: The following contractual document is based on a template from the European Commission, which considers this contractual document legally valid. For this purpose, the European Commission has issued an implementing decision on standard contractual clauses between controllers and processors pursuant to Article 28(7) of the GDPR and Article 29(7) of Regulation (EU) 2018/1725. The implementing decision can be viewed here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915. It must not be confused with the standard contractual clauses pursuant to Article 46 GDPR, which govern transfers to third countries.

SECTION I

Clause 1

Purpose and Scope

a) These standard contractual clauses (hereinafter “Clauses”) are intended 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, on the free movement of such data, and repealing Directive 95/46/EC.
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 pursuant to Annex II.
d) Annexes I to IV are an integral part of the Clauses.
e) These Clauses apply without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
f) These Clauses do not, in themselves, ensure compliance with obligations related to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Unchangeability of the Clauses

a) The parties undertake not to amend the Clauses, except to supplement or update the information specified in the Annexes.
b) This does not prevent the parties from incorporating the standard contractual clauses set out in these Clauses into a more extensive contract and adding further clauses or additional guarantees,

provided that these do not directly or indirectly conflict with the Clauses or restrict the fundamental rights or freedoms of the data subjects.

Clause 3

Interpretation

a) Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these Clauses, such terms have the same meaning as in the respective regulation.
b) These Clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
c) These Clauses shall not be interpreted in a manner that contravenes the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or restricts the fundamental rights or freedoms of data subjects.

Clause 4

Precedence

In the event of a conflict between these Clauses and the provisions of related agreements between the parties, whether existing or entered into later, these Clauses shall prevail.

Clause 5

Bundling Clause

a) An entity that is not a party to these Clauses may accede to these Clauses at any time as a controller or processor, with the consent of all parties, by completing the Annexes and signing Annex I.
b) After completing and signing the Annexes referred to in letter a, the acceding entity shall be treated as a party to these Clauses and shall have the rights and obligations of a controller or processor in accordance with its designation in Annex I.
c) For the period prior to its accession as a party, the acceding entity shall have no rights or obligations arising from these Clauses.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of Processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data is processed on behalf of the controller, are set out 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 it is subject. In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the relevant law prohibits such information on important public interest grounds. The controller may issue further instructions for the entire duration of the personal data processing. These instructions must always be documented.

b) The processor shall inform the controller immediately if it believes that instructions issued by the controller violate Regulation (EU) 2016/679, Regulation (EU) 2018/1725, or applicable Union or Member State data protection law.

7.2 Purpose Limitation

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

7.3 Duration of Processing

The data shall be processed by the processor only for the duration specified in Annex II.

7.4 Security of Processing

a) The processor shall implement at least the technical and organizational measures set out in Annex III to ensure the security of personal data. This includes protection against a personal data breach, whether accidental or unlawful, leading to destruction, loss, alteration, unauthorized disclosure, or unauthorized access to the data (hereinafter “personal data breach”). When assessing the appropriate level of security, the parties shall take into account the state of the art, implementation costs, the nature, scope, context, and purposes of processing, and the risks to the rights and freedoms of data subjects.

b) The processor shall grant its personnel access to personal data only to the extent necessary for performing, managing, and supervising the contract. The processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate legal obligation of secrecy.

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, or genetic or biometric data for uniquely identifying a natural person, data concerning health, sexual life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter “sensitive data”), the processor shall apply special restrictions and/or additional safeguards.

7.6 Documentation and Compliance with Clauses

a) The parties must be able to demonstrate compliance with these Clauses.
b) The processor shall promptly and appropriately respond to the controller’s requests regarding data processing under these Clauses.
c) The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations set out in these Clauses and directly arising from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. Upon request of the controller, the processor shall also allow audits of the processing activities covered by these Clauses at reasonable intervals or in case of indications of non-compliance and shall cooperate in such audits. In deciding on an audit, the controller may consider the processor’s relevant certifications.
d) The controller may conduct the audit itself or engage an independent auditor. Audits may also include inspections of the processor’s premises or physical facilities and shall be conducted with reasonable prior notice where applicable.
e) The parties shall provide the competent supervisory authority(ies) with the information specified in this Clause, including audit results, upon request.

7.7 Use of Sub-processors

a) The processor has the general authorization of the controller to engage sub-processors listed in an agreed list. The processor shall inform the controller in writing at least three weeks in advance of any intended changes to this list by adding or replacing sub-processors, giving the controller sufficient time to object to such changes before the engagement of the relevant sub-processor(s). The processor shall provide the controller with the necessary information to exercise its right of objection.
a) If the processor engages a sub-processor to carry out specific processing activities (on behalf of the controller), such engagement must be governed by a contract imposing on the sub-processor essentially the same data protection obligations as those applicable to the processor under these Clauses. The processor shall ensure that the sub-processor complies with the obligations applicable to the processor under these Clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
b) Upon request, the processor shall provide the controller with a copy of such sub-processor agreement and any subsequent amendments. To protect trade secrets or other confidential information, including personal data, the processor may redact the agreement before providing a copy.

c) The processor is fully liable to the controller for the sub-processor's compliance with its contractual obligations. The processor shall notify the controller if the sub-processor fails to fulfill its contractual obligations.

d) The processor shall agree with the sub-processor a third-party beneficiary clause, whereby the controller – if the processor no longer exists or becomes insolvent – has the right to terminate the sub-processor contract and instruct the sub-processor to delete or return the personal data.

7.8 International Data Transfers

a) Any transfer of data by the processor to a third country or international organization shall take place only on the basis of documented instructions from the controller or to comply with a specific provision of Union or Member State law applicable to the processor and must comply with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that, in cases where the processor engages a sub-processor pursuant to Clause 7.7 to carry out specific processing activities on behalf of the controller and these 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 may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses issued by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided the conditions for using these standard contractual clauses are met.

Clause 8

Assistance to the Controller

a) The processor shall inform the controller promptly of any request received from a data subject. It shall not respond to the request itself unless authorized by the controller.

b) Taking into account the nature of the processing, the processor shall assist the controller in fulfilling its obligation to respond to data subjects' requests to exercise their rights. In fulfilling its obligations under letters a and b, the processor shall follow the controller's instructions.

c) Apart from the obligation to assist the controller under Clause 8(b), the processor shall, taking into account the nature of the data processing and the information available to it, assist the controller in complying with the following obligations:

    1) Obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter "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) Obligation to consult the competent supervisory authority before processing if a data protection impact assessment indicates a high risk unless the controller implements measures to mitigate the risk;

3) Obligation to ensure that personal data is accurate and up to date by notifying the controller promptly if it discovers that the personal data it processes is inaccurate or outdated;
4) Obligations under Article 32 of Regulation (EU) 2016/679.

d) The parties shall specify in Annex III the appropriate technical and organizational measures to assist the controller under this Clause, as well as the scope and extent of the required assistance.

Clause 9

Notification of Personal Data Breaches

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

9.1 Breach of the Controller's Data

In the event of a personal data breach relating to the data processed by the controller, the processor shall assist the controller as follows:

a) prompt notification of the personal data breach to the competent supervisory authority after the controller becomes aware of the breach, if relevant (unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons);
b) provision of the following information required under Article 33(3) of Regulation (EU) 2016/679 in the controller's notification, including at least:

1) the nature of the personal data, where possible, specifying the categories and approximate number of data subjects and the categories and approximate number of data records concerned;
2) the likely consequences of the personal data breach;
3) the measures taken or proposed by the controller to address the breach, including measures to mitigate potential adverse effects. If all information cannot be provided at once, the initial notification shall include the available information, and additional information shall be provided promptly when available.

c) compliance with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject without undue delay if the breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Breach of Protection of Data Processed by the Processor

In the event of a personal data breach relating to data processed by the processor, the processor shall notify the controller promptly after becoming aware of the breach. The notification shall include at least:

a) a description of the nature of the breach (if possible, specifying categories and approximate numbers of data subjects and data records);
b) contact details of a point of contact for further information about the breach;
c) The likely consequences and measures taken or proposed to address the breach, including measures to mitigate potential adverse effects.

If all information cannot be provided at once, the initial notification shall include the available information, and further information shall be provided promptly when available. Annex III specifies any additional information the processor must provide to assist the controller in complying with Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Breaches of the Clauses and Termination of the Agreement

a) If the processor fails to fulfill its obligations under these clauses, the controller may – without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 – instruct the processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The processor shall immediately inform the controller if, for any reason, it is unable to comply with these clauses.
b) The controller is entitled to terminate the contract, insofar as it concerns the processing of personal data under these clauses, if:

    1) the controller has suspended the processing of personal data by the processor under letter a and compliance with these clauses is not restored within a reasonable period, in any case within one month of the suspension;

    2) the processor significantly or persistently breaches these clauses or fails to fulfill its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

    3) the processor does not comply with a binding decision of a competent court or the competent supervisory authority(ies) concerning its obligations under these clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor is entitled to terminate the contract, insofar as it concerns the processing of personal data under these clauses, if the controller insists on carrying out its instructions after being informed by the processor that such instructions violate applicable legal requirements under Clause 7.1(b).

d) After termination of the contract, the processor shall, at the controller's choice, delete all personal data processed on behalf of the controller and certify to the controller that this has been done, or return all personal data to the controller and delete existing copies, unless a Union law or Member State law requires storage of the personal data. Until deletion or return of the data, the processor shall continue to comply with these clauses.

ANNEX I – LIST OF PARTIES

Controller:

The controller and the processor are, independently of this data processing agreement, parties to a contractual main agreement regarding the provision of the service “Onepage” (see https://onepage.io/auth/registration). The controller is the company that books this service, whether a free trial or a paid version. The joining date is identical to the date of the first booking of the service.

Processor:

Name: Onepage GmbH
Address: Hanauer Landstraße 172, 60314 Frankfurt am Main
Name, role, and contact details of the contact person: Marcel Knopf, Management, reachable as above under the address note “personal – confidential – management”
The joining date is identical to the date of the first booking of the service.

ANNEX II – DESCRIPTION OF PROCESSING

Preliminary remark

The processor provides its business customers with the SaaS platform “Onepage.” Using this platform, it is possible to create, continuously design, and manage data collected through web pages (so-called leads). For this purpose, the processor provides its customers with a web portal for browser-based use in a section accessible exclusively to registered users, as well as storage space on servers of subprocessors (ANNEX III), which are located exclusively in the EU. The controller is a customer and thus a user of the platform.

Given this, the data processing can be described as follows:

Categories of data subjects whose personal data is processed:

- current and former visitors of websites generated with Onepage
- applicants of the controller
- current and former employees of the controller
- potential, current, and former customers of the controller
- potential, current, and former suppliers of the controller

Categories of personal data processed:

<u>Data of current and former visitors of websites generated with Onepage</u>

- technical access data: IP address of visitors, date and time of access, retrieved URL/page, referrer URL (previously visited page), HTTP status code, transmitted data volume, browser type and version, operating system, language settings, device type
- *only if, as long as, and to the extent activated by the controller:* cookie and tracking data, cookie IDs, and similar identifiers
    - visited subpages, dwell time, clicks, scroll behavior, optionally marketing/tracking data such as UTM parameters, campaign attribution, tagging-pixel-based data
- *only if, as long as, and to the extent activated by the controller:* content and form data in contact/lead forms
    - data entered by visitors, e.g., name, email address, phone number, other form content such as free-text messages, interests, appointment requests, selection options in forms; opt-in/consent status, such as the time, content of consent, proof of agreement to newsletters, etc.

<u>Data of other categories of data subjects</u>

- all data also processed from visitors of Onepage-generated websites
- communication and interaction data

  - content of inquiries via contact forms (e.g., support, consulting, or booking inquiries), optionally comments/reviews if such features are integrated (including name, comment text).
- contract and billing data (only if contracts/orders are initiated or concluded via the landing page)
- basic data on inquiries, bookings, or orders (e.g., chosen offer, inquiry date)
- optionally payment or invoice information (often handled via external payment providers, but initiated through the landing page for the purpose)

Nature of processing

Data are collected on websites generated with Onepage, stored in a cloud environment, and made available to the controller for retrieval. Data are deleted upon instruction and/or the end of the main contract.

Purpose(s) for which personal data are processed on behalf of the controller

Processing serves the provision of web presences, advertising communication, and analysis of user behavior.

Duration of processing

Data are deleted upon instruction and/or the end of the main contract.

ANNEX III – TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING MEASURES TO ENSURE DATA SECURITY:

I

General measures

Measures for ongoing security assurance (sustainability control)

Data protection as a compliance goal

Respect for core and secondary data protection regulations is a formulated compliance goal of the processor. Organizational authority to ensure data protection compliance rests by virtue of office with management.

Review frequency 18 months

Checks are conducted every 18 months, regardless of occasion, to verify whether the measures documented here are still in place (checkpoint 1) and whether the measures are sufficient to adequately minimize the identified risks (checkpoint 2). It is documented whether the checkpoints are affirmed or denied. If at least one of the checkpoints is denied, new measures are defined and implemented. Occasional checks can be conducted at any time and are also documented.

Training and awareness measures

Employees are regularly trained (usually once a year). The training concept is as follows:

- The aim of the training is to familiarize employees with the basics and key concepts of data protection law. Employees should subsequently be able to determine, based on the prohibition-with-reservation principle, when the processing of personal data is lawful and when it is unlawful. They should also know the required technical and organizational measures and how to contribute to their implementation. Furthermore, an overview of other data protection obligations, particularly under the GDPR and BDSG2018, is provided, including instruction on data confidentiality.

- The following points in particular should be noted regarding the structure:
    - Block 1 begins with a rough introduction, in which an overview of the upcoming training is provided.
    - Block 2 begins with an introduction to data protection law. The basic terms are trained, in particular the terms "personal data," "processing," "consent," "legal provision." The training is oriented towards the legal definitions of the GDPR and the BDSG2018. The prohibition with reservation of permission is explained. The legality requirements for consent are discussed. Subsequently, the most important legal provisions independent of consent are explained, in particular § 26 BDSG2018 (employee data protection), Article 6(1)(b) GDPR (customer data protection), and Article 6(1)(f) GDPR (legitimate interest). For each permission provision, at least one example case is discussed with the training participants (m/f/d) to ensure that everyone can handle the provisions. In addition, the requirements for consent are explained.
    - Block 3 begins with an introduction to the technical and organizational measures according to Article 32 GDPR. In this context, it is explained above all which risks are to be analyzed and how. Then it is explained that these risks are to be minimized with technical and organizational measures. Furthermore, the obligation

to provide evidence is addressed. Subsequently, the most important technical and organizational measures in the company are discussed. Finally, the project plan “Data Protection Organization” is trained here.

- Block 4 deals with specific questions of data protection law in the scope of commissioned data processing.

DPO appointed

The controller has appointed a Data Protection Officer.

Organizational measures, documentation and lawfulness of instructions

The local processor maintains a comprehensive record of processing activities. In particular, it maintains the records pursuant to Article 30(2) GDPR with all statutory mandatory information. If employees come to the conclusion that an instruction violates the GDPR, they consult, in case of doubt, the external data protection officer, who, if necessary, contacts the local controller/client and clarifies the lawfulness of the instruction. It supports the local controller/client in data protection impact assessments; this is in fulfillment of its duties as a processor. However, it does not provide legal advice. Instructions from the local controller/client are documented in writing.

II

Confidentiality

Measures of Anonymization

Technique of Deletion

Data that are pending deletion are anonymized.

Measures of Encryption

The processing in question does not take place on the servers of the processor, but at its subprocessors.

Encryption at AWS

The subprocessor encrypts data at rest using standardized industry algorithms such as AES-256. Encryption is applied, for example, in services like Amazon S3, Amazon RDS, Amazon EBS, and Amazon Glacier. Central systems such as the AWS Key Management Service (KMS) and dedicated hardware security modules (HSM, e.g., “AWS CloudHSM”) are used for key management. Customers have the option to manage keys themselves or have the subprocessor generate and protect them. Without the necessary access keys, stored data are not accessible in plaintext to third parties or the subprocessor. For data in transit, the subprocessor uses standard transport encryption with SSL/TLS. All interfaces and API endpoints support HTTPS (TLS), so that communication between customers

and the AWS cloud is fully protected. Additionally, network encryptions (e.g., IPsec) are implemented for transfers between AWS data centers and within virtual private networks (VPCs).

Encryption at Google

The subprocessor encrypts all customer data at rest on storage media and backup media using strong algorithms such as AES-128 or AES-256. Encryption is applied automatically without customer intervention for all data in Workspace core applications (e.g., Gmail, Drive, Docs, Sheets, Meet). Google's own key management mechanisms in the data center protect the keys, with physical and technical protection systems for storage media and key material. For data in transit, the subprocessor protects customer data with industry-standard transport encryption, especially HTTPS (TLS), which is standard for all users and interfaces. Additionally, communication between Google data centers and transmissions over the public internet is encrypted.

Measures of Physical Entry Control

There are no permanent hardware components, especially no server, within the offices of the processor. Furthermore, no processing-related activities are generally performed there, only executive-administrative tasks and mail handling. Therefore, physical security measures are of minor significance. Nevertheless, the processor takes the following additional measures:

Building, locked door (mechanical key)

The building housing the operations relevant to data processing is locked. Access is possible either by a person inside opening the door or by using a separate access means (here: mechanical key).

Office, locked door (mechanical key)

Office rooms are locked. Access is possible either by a person inside opening the door or by using a separate access means (here: mechanical key).

Internal instruction, secure rooms

Employees are instructed to perform remote work only in secure rooms. Secure rooms are those generally not accessible to unknown third parties, not easily visible from outside, and generally not entered by visitors.

Internal instruction, reporting entry violations

Employees are instructed to report suspected reportable cases under Articles 33, 34 GDPR in connection with entry violations. The same obligation applies if not only suspicion, but certainty exists.

Measures of System Access Control

Inside the offices of the data processor, there are no permanent hardware components, in particular no server. Furthermore, the work related to the processing is generally not performed there, but only

administrative-executive tasks and the receipt of mail. Therefore, physical security measures are of minor importance. Nevertheless, the processor implements the following additional measures:

Internal instruction, restricted access
Employees are required by internal instruction to grant third parties, including family members, no or only absolutely necessary access to the data processing resources owned by the company.

Internal instruction, reporting access violations
Employees are required by internal instruction to report any suspicion of notifiable cases under Articles 33 and 34 GDPR in connection with access violations. The same obligation applies if not only suspicion, but certainty exists.

Internal instruction, general measures
Employees are required by internal instruction to implement the following “general measures” even during remote work.

General measures
The following measures are implemented, regardless of whether the data processing is carried out remotely or on-site (general measures):

Change of default and blank passwords
After installation of new software or commissioning of new hardware, default and blank passwords are changed.

Password-protected clients
All clients are password-protected.

individual passwords
All authorized persons have individual passwords.

restricted use of admin access
The so-called admin access is used only for admin activities. Persons who have admin rights use separate access credentials for non-admin activities.

restricted overall access to passwords
Only a narrowly limited group of persons has overall access to all access data.

operating systems, security patches
With regard to the operating systems used, all available security patches are installed.

operating systems, updates
With regard to the operating systems used, all available updates are installed.

web browsers, security patches
With regard to the web browsers used, all available security patches are installed.

web browsers, updates

With regard to the web browsers used, all available updates are installed.

virus protection on all clients

All clients and servers have virus protection.

virus scans

The antivirus programs used perform automated, regular virus scans.

antivirus programs, updates

With regard to the antivirus programs used, all available updates are installed.

release requirement for new software

New software may only be installed if it has previously been approved centrally.

software approval only after review of the manuals

New software may only be installed if the manual is either already known or has been read.

release requirement for new hardware

New hardware may only be put into operation if it has previously been approved centrally.

hardware approval only after review of the manuals

New hardware may only be put into operation if the manual is either already known or has been read.

Measures of data access control

central assignment of rights

Access rights to personal data are assigned centrally.

need-to-know principle

Access rights to personal data are assigned according to the need-to-know principle.

adjustments in the assignment of rights

If the tasks of an authorized person change, the access rights are adjusted as necessary according to the need-to-know principle.

revocation of rights

If the activity of an authorized person ends, the access rights are immediately and completely revoked.

Measures of disclosure control

reference to encryption

Reference is made to the measures for encryption.

Measures of input control

inputs are logged

Inputs, insofar as they are made manually at all in the area relevant to the assignment, are logged.

Measures of order control

Article 28 GDPR

Before any subcontracting, it is checked whether the legal requirements are met, in particular whether a contract document pursuant to Article 28(3) GDPR exists and whether the company to be commissioned offers sufficient guarantees that appropriate technical and organizational measures are implemented so that the processing is carried out in accordance with the GDPR requirements and ensures the protection of the rights of the data subject. Commissioning only takes place if the result is positive. The result is documented in any case.

Article 44 GDPR

In the event that subcontracting involves a transfer to a third country within the meaning of Article 44 GDPR, it is checked whether the company to be commissioned complies with the conditions laid down in Chapter 5 of the GDPR (Articles 44 to 50 GDPR) and whether the other provisions of this Regulation are complied with; this also applies to any further transfer of personal data from the respective third country or international organization to another third country or another international organization. Commissioning only takes place if the result is positive. The result is documented in any case.

Article 46 GDPR – TIA

In the event that commissioning involves a transfer to a third country within the meaning of Article 44 GDPR and the company to be commissioned commits to the Standard Contractual Clauses within the meaning of Article 46 GDPR, a so-called Transfer Impact Assessment is carried out. Commissioning only takes place if the result is positive. The result is documented in any case.

Article 35 GDPR

In the event that the commissioning itself or the commissioned data processing falls within the scope of Article 35 GDPR, a data protection impact assessment is carried out. Commissioning only takes place if the result is positive. The result is documented in any case.

Subsequent checks

The aforementioned checks are repeated regularly without specific occasion as long as the commissioning continues.

Responsibilities

The following responsibilities apply to the aforementioned measures:

Management

Data protection officer

As required under the DPA (data processing agreement), also the controller (client)

Measures of separation control

differentiated folder and access model

Electronically stored data are separated by means of a differentiated folder and access model.

III

Availability, Recoverability, Resilience

Measures of Availability Control

The processing in question does not take place on servers of the processor, but at its subprocessors.

Availability at AWS

The subprocessor is certified according to ISO/IEC 27018:2014 and ISO 27001. The provider takes the following measures in concreto: Data centers are built in clusters in various global regions. All data centers are online and serve customers. No data center is “cold.” In the event of an error, automated processes shift customer data traffic out of the affected area. It is ensured that in the event of a data center failure, sufficient capacity is available to compensate for the load balancing of the remaining locations. Furthermore, the provider differentiates between different availability zones. Each availability zone is designed as an independent failure zone. This means that the availability zones within a typical metropolitan region are geographically separated and located in low-water floodplains (the specific categorization of floodplains varies by region). In addition to the uninterruptible power supply and on-site backup generators, the power supply is fed through various grids from independent utility companies to further reduce single points of failure. Availability zones are all connected redundantly.

Availability at Google

The subprocessor is certified according to ISO 27001. In addition, the following must be stated: Google stores the data in a protected environment of its own servers. Data, the services database, and the file system architecture are replicated across multiple geographically distributed data centers, ensuring that confidentiality and separation of data are guaranteed. The infrastructure systems used for this purpose are capable of eliminating single points of failure and minimizing the impact of anticipated environmental risks. Dual circuits, switches, networks, or other necessary devices help to provide this redundancy. It is ensured that Google can detect and minimize certain risks at an early stage. The necessary maintenance can usually be carried out without disruption. There are documented preventive maintenance procedures. Preventive maintenance of data center equipment is carried out based on a standardized change process. The power supply systems of the data center

are designed to be redundant and maintainable without impairing continuous operations, 24 hours a day and 7 days a week. In most cases, both a primary and an alternative power source of equal capacity are provided for critical infrastructure components in the data center. Backup power is provided through various mechanisms such as uninterruptible power supplies, which deliver consistently reliable power protection during voltage dips, power outages, overvoltage, undervoltage, and out-of-tolerance frequency conditions. When mains power is interrupted, the emergency power supply is designed to power the data center at full load for up to 10 minutes until the diesel generator systems take over. The diesel generators are able to start up automatically within seconds to deliver sufficient emergency power to typically operate the data center at full capacity for several days.

Measures of Rapid Recoverability

Through the aforementioned measures of availability control, it is ensured that rapid recoverability is guaranteed. An emergency concept for incidents of data loss or limited availability is implemented.

Measures of Ensuring Resilience

Continuous system monitoring takes place.

ANNEX IV – LIST OF SUBPROCESSORS:

The controller has approved the use of the following subprocessors:

AWS

Name: Amazon Web Services EMEA S.à.r.l.

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg, Grand Duchy of Luxembourg

Name, function, and contact details of the contact person:

- Data Protection Officer: dpo@amazon.com (see AWS GDPR Data Processing Addendum)
- General contact options and current contacts via the AWS contact page: https://aws.amazon.com/compliance/contact/

Third-country status: n/a, since Luxembourg (EU) – It is acknowledged that this subprocessor has a parent company in the USA. However, this subprocessor has contractually assured the processor that the data will be processed exclusively within the EU. The processor may rely on this. This corresponds to the case law of courts within the EU. For example, the Higher Regional Court of Karlsruhe decided in its order of 7 September 2022, case no. 15 Verg 8/22, as follows: *"In this context, it assured that personal health data would be transmitted exclusively to A. S.à.r.l., L., and that the data would also not leave the EU for processing, but would be processed only in Germany. In addition, the interested party stated that A. S.à.r.l., L. had assured her that all data of the interested party would be processed in Germany and further confirmed in the oral hearing before the Senate that she would conclude all internally necessary contracts with A. by contract award that implement her commitments as stated in the offer. The applicants understood the statements of the interested party in the tender documents in the sense of such a binding assurance. The applicants may rely on this performance promise."*

Description of processing: Storage and processing of personal data on behalf of the processor (cloud storage, infrastructure services).

Google Workspace

Name: Google Cloud EMEA Limited

Address: 70 Sir John Rogerson's Quay, Dublin 2, Ireland

Name, function, and contact details of the contact person:

- Data Protection Officer: Kristie Chon Flynn, reachable via the data protection team at https://support.google.com/a/contact/googlecloud_dpr (best via the administrator account); General information: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

Third-country status: n/a, since Ireland (EU) – It is acknowledged that this subprocessor has a parent company in the USA. However, this subprocessor has contractually assured the processor that the data will be processed exclusively within the EU. The processor may rely on this. This corresponds to the case law of courts within the EU. For example, the Higher Regional Court of Karlsruhe decided in its order of 7 September 2022, case no. 15 Verg 8/22, as follows: *"In this context, it assured that personal health data would be transmitted exclusively to A. S.à.r.l., L., and that the data would also not leave the EU for processing, but would be processed only in Germany. In addition, the interested party stated that A. S.à.r.l., L. had assured her that all data of the interested party would be processed in*

Germany and further confirmed in the oral hearing before the Senate that she would conclude all internally necessary contracts with A. by contract award that implement her commitments as stated in the offer. The applicants understood the statements of the interested party in the tender documents in the sense of such a binding assurance. The applicants may rely on this performance promise."
Description of processing: Storage and processing of personal data on behalf of the processor (cloud storage, infrastructure services).

Cloudflare
Name: Cloudflare, Inc.
Address: 101 Townsend Street, San Francisco, CA 94107, USA
Name, function, and contact details of the contact person:

- Data Protection Officer: privacyquestions@cloudflare.com; additional contact details per DPA: +44 (0) 20 3514 6970

Third-country status: USA, Article 45 GDPR (EU–U.S. DPF)
Description of processing: Provision of web hosting, reverse proxy, DNS, and content delivery network (CDN) services; delivery and caching of website content, security and protection functions (e.g., against DDoS attacks), as well as logging of access for analysis and optimization of availability and performance; during delivery and caching, personal data (e.g., IP addresses, access times, or log data) may be processed and transmitted across globally distributed servers.