

DATA PROCESSING AGREEMENT

Note 1: All references to natural persons below shall be understood as referring to persons of all genders.

Note 2: This contractual document is based on a model prepared by the European Commission, which expressly recognises this contractual document as legally compliant. For this purpose, the European Commission adopted an Implementing Decision on standard contractual clauses between controllers and processors pursuant to Article 28(7) of Regulation (EU) 2016/679 (GDPR) and Article 29(7) of Regulation (EU) 2018/1725. The Implementing Decision is available at the following address: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0915>. It must not be confused with the standard contractual clauses within the meaning of Article 46 GDPR, which govern the transfer of personal data to third countries.

STANDARD CONTRACTUAL CLAUSES

SECTION I

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).
- b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- c) These Clauses apply to the processing of personal data as specified in Annex II.
- d) Annexes I to IV are an integral part of the Clauses.
- e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

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

Clause 4

Hierarchy

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

Clause 5

Docking clause

- a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

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 II.

Clause 7

Obligations of the Parties

7.1 Instructions

- a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

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

7.3 Duration of the processing of personal data

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

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

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

7.5 Sensitive data

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

7.6 Documentation and compliance

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

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

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

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

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

7.7 Use of sub-processors

- a) 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 six 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 the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to 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 Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

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

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

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

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

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

- 4) the obligations in Article 32 of Regulation (EU) 2016/679/.

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

Clause 9

Notification of personal data breach

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

9.1 Data breach concerning data processed by the controller

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

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

- b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/1) shall be stated in the controller's notification, and must at least include:

- i. 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;

- ii. the likely consequences of the personal data breach;

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 /, 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

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

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

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

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

- 1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
- 2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
- 3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

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

ANNEX I – LIST OF PARTIES

Controller:

The Controller and the Processor are, independently of this Data Processing Agreement, parties to a separate underlying service agreement governing the provision of the “Onepage” service. The Controller is the company that orders or subscribes to the service, regardless of whether it uses the free trial version or the paid version. The accession date shall be the date on which the service is first ordered or subscribed to.

Processor:

Name: Onepage GmbH

Address: Neue Rothofstr. 13–19, 60313 Frankfurt am Main

Name, position and contact details of the contact person: Marcel Knopf, Managing Director, reachable at the above address, marked for the attention of “personal – confidential – management”.

The accession date shall be the date on which the service is first ordered or subscribed to.

Version: October 2026

ANNEX II – DESCRIPTION OF THE PROCESSING

Preamble

The Processor provides its business customers with the SaaS platform “Onepage”. The platform enables users to create and continuously design websites, including landing pages, and to manage data collected through those websites, so-called leads. For this purpose, the Processor provides its customers with a web portal for browser-based use within an area accessible exclusively to registered users, as well as storage space on servers operated by the Sub-processors listed in Annex IV, all of which are located exclusively within the European Union. The Controller is a customer and therefore a user of the platform.

On this basis, the processing by the Processor may be described as follows:

Categories of data subjects whose personal data are processed

- Current and former visitors to websites generated using Onepage;
- Applicants of the Controller;
- Current and former employees of the Controller;
- Prospective, current and former customers of the Controller;
- Prospective, current and former suppliers of the Controller.

Categories of personal data processed

Data relating to current and former visitors to websites generated using Onepage

- **Technical access data:** visitors' IP addresses, date and time of access, requested URL or page, referrer URL (previously visited page), HTTP status code, volume of data transmitted, browser type and version, operating system, language settings and device type;
- **Only if, for as long as and to the extent activated by the Controller:** cookie and tracking data, including cookie IDs and similar identifiers;
- Visited subpages, duration of visit, clicks, scrolling behaviour and, where applicable, marketing or tracking data, such as UTM parameters, campaign attribution and tagging-pixel-based data;
- **Only if, for as long as and to the extent activated by the Controller:** content and form data submitted through contact or lead forms;
- Data entered by visitors, such as name, email address, telephone number and other form content, including free-text messages, statements of interest, appointment requests and options selected in forms;
- Opt-in or consent status, including the time and content of the consent and evidence of consent to newsletters or similar communications.

Data relating to the other categories of data subjects

- All data that may also be processed in relation to visitors to websites generated using Onepage;
- Communication and interaction data, including:
 - The content of enquiries submitted through contact forms, such as support, consultation or booking enquiries;

- Where such functions are integrated, comments or reviews, including the name and the text of the comment;
- Contractual and billing data, but only where contracts or orders are initiated or concluded through the landing page;
- Basic data relating to enquiries, bookings or orders, such as the offer selected and the date of the enquiry;
- Where applicable, payment or invoice information, which is often processed through external payment providers but may be initiated via the landing page for the relevant purpose.

Data processed in relation to all categories of data subjects

When content is delivered through the Content Delivery Network, the following data may in particular be processed: the IP address of the requesting client, the time of the request, the requested URL or path, technical request headers, query parameters transmitted and the requested content. Standard access logging and cookie logging are disabled. In addition, no edge functions are integrated that would result in the storage of additional logs relating to visitor requests.

Special categories of personal data pursuant to Article 9(1) GDPR

Where the Controller carries out a professional or business activity in the course of which the processing of special categories of personal data pursuant to Article 9(1) GDPR may arise—for example, as a medical practice, law firm or tax consultancy—and activates or otherwise configures corresponding content, input fields, functions or communication facilities on a website created using the platform, special categories of personal data within the meaning of Article 9(1) GDPR may also be processed.

This may include, in particular, health data and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. It may further include genetic data or biometric data processed for the purpose of uniquely identifying a natural person, as well as data concerning sex life or sexual orientation.

Nature of the processing

The data are collected on websites generated using Onepage, stored in a cloud environment and made available to the Controller for retrieval.

A Content Delivery Network is used to deliver static content through onecdn.io. In this context, the following operations may in particular be carried out: TLS termination, routing and content delivery and—depending on the relevant request and cache configuration—the temporary caching of content at geographically distributed edge and regional edge locations worldwide.

The data shall be deleted upon the Controller's instruction and/or upon termination of the underlying service agreement.

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

The processing serves to provide websites and online presences, conduct marketing and promotional communications and analyse user behaviour. It further serves the technical provision, protection and efficient delivery of content through a Content Delivery Network.

Duration of the processing

The data shall be deleted upon the Controller's instruction and/or upon termination of the underlying service agreement.

ANNEX III – Technical and organisational measures including technical and organisational measures to ensure the security of the data

I General Measures

Measures implemented by the Sub-processors

The core of the processing covered by the Agreement is carried out by the Sub-processors listed in **Annex IV**. In this respect, the companies named therein implement the following security measures:

Sub-processor	Technical and organisational measures / certifications
Amazon Web Services EMEA S.à r.l.	AWS GDPR Data Processing Addendum; ISO-certified services; SOC compliance information; AWS Artifact; Amazon CloudFront compliance information.
Google Cloud EMEA Limited	Google Cloud Data Processing Terms; Google Cloud compliance resources.
Cloudflare, Inc.	Cloudflare Customer Data Processing Addendum; Cloudflare Security Exhibit; Cloudflare Trust Hub; SOC 2 compliance resources.

Measures ensuring the ongoing security of processing

Data protection as a compliance objective

Compliance with the fundamental and ancillary requirements of data protection law is an expressly defined compliance objective of the Processor. The organisational responsibility for ensuring compliance with data protection law lies, by virtue of their office, with the management.

Review cycle of 18 months

At intervals of 18 months and without the need for a specific reason, the Processor shall review whether the measures documented herein are still being implemented (**review point 1**) and whether those measures remain sufficient to adequately mitigate the identified risks (**review point 2**).

The Processor shall document whether each review point has been answered in the affirmative or in the negative. If at least one of the two review points is answered in the negative, new measures shall be defined and implemented. Reviews triggered by a specific event may be carried out at any time and shall likewise be documented.

Training and awareness measures

Employees shall receive regular training, generally once a year. The training concept includes the following:

- The purpose of the training is to familiarise employees of all genders with the fundamentals and basic concepts of data protection law. In particular, employees should subsequently be able to answer the fundamental question of when the processing of personal data is lawful and when it is unlawful, based on the principle that processing is prohibited unless permitted. They should also be familiar with the required technical and organisational measures and

understand how they can and must contribute to their implementation within the company. In addition, the training shall provide an overview of other data protection obligations, in particular those arising under the GDPR and the **Federal Data Protection Act 2018 (BDSG 2018)**. Particular attention shall be paid to the obligation to maintain data confidentiality.

- The training shall be structured in particular as follows:
 - **Block 1** begins with a general introduction providing an overview of the training to follow.
 - **Block 2** begins with an introduction to data protection law. The basic concepts shall be covered, in particular the terms “personal data”, “processing”, “consent” and “legal provision”. The training shall be based on the legal definitions contained in the GDPR and the BDSG 2018. The principle that processing is prohibited unless permitted shall be explained. The legal requirements for valid consent shall be discussed. The most important legal bases that do not depend on consent shall then be explained, in particular Section 26 BDSG 2018 concerning employment data protection, Article 6(1)(b) GDPR concerning customer data protection and Article 6(1)(f) GDPR concerning legitimate interests. At least one practical example shall be discussed with the participants for each legal basis in order to ensure that all participants are able to apply the relevant provisions. The requirements for valid consent shall also be explained.
 - **Block 3** begins with an introduction to the technical and organisational measures pursuant to Article 32 GDPR. In particular, it shall explain which risks must be analysed and how they are to be assessed. It shall then be explained that these risks must be mitigated through technical and organisational measures. The obligation to provide evidence of compliance shall also be addressed. The most important technical and organisational measures implemented within the company shall subsequently be discussed. Finally, the “Data Protection Organisation” project plan shall be covered.
 - **Block 4** addresses specific data protection issues arising in the context of processing carried out on behalf of a controller.

Data Protection Officer appointed

The Processor has appointed a Data Protection Officer.

Organisational measures, documentation and lawfulness of instructions

The Processor maintains a comprehensive record of processing activities. In particular, it maintains the records required under **Article 30(2) GDPR**, including all information required by law. If employees conclude that an instruction infringes the GDPR, they shall, in cases of doubt, consult the external Data Protection Officer. Where necessary, the Data Protection Officer shall contact the Controller or client of the Processor and clarify the lawfulness of the instruction. The Processor shall support the Controller or client in carrying out data protection impact assessments in fulfilment of its obligations as Processor. However, the Processor does not provide legal advice. Instructions issued by the Controller or client shall be documented in text form.

II Confidentiality

Measures for anonymisation

Data deletion procedure

Data scheduled for deletion shall be anonymised.

Measures for encryption

The processing covered by the Agreement does not take place on the Processor's own servers, but at its Sub-processors. Reference is therefore made to the security measures of the Sub-processors described above.

Physical access control measures

The Processor's office premises do not contain any permanent hardware components, in particular no server. Furthermore, activities relating to the processing covered by the Agreement are generally not carried out there. The premises are used primarily for management and administrative activities and for receiving mail.

Accordingly, physical security measures are of limited significance. Nevertheless, the Processor implements the following supplementary measures.

Building, locked door with mechanical key

The building in which the premises relevant to the processing are located is locked. Access is possible either by a person inside the building opening the entrance door from the inside or by a person opening the entrance door using a separate access device, namely a mechanical key.

Office, locked door with mechanical key

The office premises are locked. Access is possible either by a person inside the office premises opening the relevant door from the inside or by a person opening the relevant door using a separate access device, namely a mechanical key.

Internal instruction concerning secure rooms

Employees are required by internal instruction to perform remote work only in secure rooms. Secure rooms are rooms which, as a rule, cannot be entered by unknown third parties, are not readily visible from outside the relevant building and are generally not entered by visitors.

Internal instruction concerning the reporting of physical access breaches

Employees are required by internal instruction to report suspected incidents requiring notification under **Articles 33 and 34 GDPR** where such incidents are connected with breaches of physical access controls. The same obligation applies where the occurrence of such a breach is established rather than merely suspected.

System access control measures

The Processor's office premises do not contain any permanent hardware components, in particular no server. Furthermore, activities relating to the processing covered by the Agreement are generally not carried out there. The premises are used primarily for management and administrative activities and for receiving mail.

Accordingly, physical security measures are of limited significance. Nevertheless, the Processor implements the following supplementary measures.

Internal instruction concerning restricted access

Employees are required by internal instruction not to grant third parties, including family members, access to company-owned data-processing equipment, or to grant such access only to the extent absolutely necessary.

Internal instruction concerning the reporting of system access breaches

Employees are required by internal instruction to report suspected incidents requiring notification under Articles 33 and 34 GDPR where such incidents are connected with breaches of system access controls. The same obligation applies where the occurrence of such a breach is established rather than merely suspected.

Internal instruction concerning cross-functional measures

Employees are required by internal instruction to implement the “cross-functional measures” described below also when working remotely.

Cross-functional measures

The following measures apply irrespective of whether processing takes place remotely or on the premises:

Changing default and blank passwords

Default and blank passwords shall be changed following the installation of new software or the commissioning of new hardware.

Password-protected clients

All client devices shall be password-protected.

Individual passwords

All authorised persons shall have individual passwords.

Restricted use of administrator accounts

Administrator accounts shall be used only for administrative activities. Persons with administrator rights shall use separate accounts for non-administrative activities.

Restricted comprehensive access to passwords

Only a strictly limited group of persons shall have comprehensive access to all access credentials.

Operating systems, security patches

All available security patches shall be installed for the operating systems used.

Operating systems, updates

All available updates shall be installed for the operating systems used.

Web browsers, security patches

All available security patches shall be installed for the web browsers used.

Web browsers, updates

All available updates shall be installed for the web browsers used.

Anti-virus protection on all clients

All client devices and servers shall have anti-virus protection.

Virus scans

The anti-virus programs used shall carry out automated, regular virus scans.

Updates to anti-virus programs

All available updates shall be installed for the anti-virus programs used.

Approval requirement for new software

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

Approval of software after review of manuals

New software may be installed only if its manual is known or has been read beforehand.

Approval requirement for new hardware

New hardware may be commissioned only after it has been centrally approved.

Approval of hardware after review of manuals

New hardware may be commissioned only if its manual is known or has been read beforehand.

Data access control measures

Central allocation of rights

Access rights to personal data shall be allocated centrally.

Need-to-know principle

Access rights to personal data shall be allocated in accordance with the **need-to-know principle**.

Adjustments to access rights

If the duties of an authorised person change, their access rights shall be adjusted as necessary in accordance with the need-to-know principle.

Withdrawal of rights

When an authorised person's activities end, their access rights shall be withdrawn fully and without undue delay.

Data transfer control measures**Reference to encryption measures**

Reference is made to the encryption measures described above.

Data entry control measures**Logging of entries**

Entries shall be logged insofar as manual entries are made at all within the area relevant to the processing covered by the Agreement.

Processor control measures**Article 28 GDPR**

Before any sub-processing arrangement is entered into, the Processor shall verify whether the statutory requirements have been met. In particular, it shall verify whether a contractual instrument meeting the requirements of **Article 28(3) GDPR** is in place and whether the company to be appointed provides sufficient guarantees that appropriate technical and organisational measures will be implemented in such a manner that the processing complies with the requirements of the GDPR and ensures the protection of the rights of data subjects.

The company shall be appointed only if the result of the review is positive. The result shall be documented in all cases.

Article 44 GDPR

If the appointment of a Sub-processor entails a transfer to a third country within the meaning of **Article 44 GDPR**, the Processor shall verify whether the company to be appointed complies with the requirements set out in Chapter V of the GDPR, in particular Articles 44 to 50 GDPR, and whether the other provisions of the GDPR are also complied with.

This shall also apply to any onward transfer of personal data from the relevant third country or international organisation to another third country or international organisation.

The company shall be appointed only if the result of the review is positive. The result shall be documented in all cases.

Article 46 GDPR — Transfer Impact Assessment

If the appointment entails a transfer to a third country within the meaning of Article 44 GDPR and the company to be appointed undertakes to comply with the standard contractual clauses within the meaning of **Article 46 GDPR**, a **Transfer Impact Assessment** shall be carried out.

The company shall be appointed only if the result of the assessment is positive. The result shall be documented in all cases.

Article 35 GDPR

If the appointment itself or the processing commissioned falls within the scope of **Article 35 GDPR**, a data protection impact assessment shall be carried out.

The company shall be appointed only if the result of the assessment is positive. The result shall be documented in all cases.

Follow-up reviews

The reviews described above shall be repeated at regular intervals and without the need for a specific reason for as long as the sub-processing arrangement remains in force.

Responsibilities

The following parties shall be responsible for the measures described above:

- The management;
- The Data Protection Officer;
- Where required under the Data Processing Agreement, the Controller or client.

Data separation control measures

Differentiated folder and access model

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

III Availability, Recoverability and Resilience

Availability control measures

The processing covered by the Agreement does not take place on the Processor's own servers, but at its Sub-processors. Reference is therefore made to the security measures of the Sub-processors described above.

Measures ensuring prompt recoverability

The availability control measures described above ensure prompt recoverability. A contingency plan has been implemented for incidents involving data loss or restricted availability.

Measures ensuring resilience

Continuous system monitoring is carried out.

ANNEX IV – List of sub-processors

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

Amazon Web Services EMEA S.à r.l. (AWS)

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

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

Name, position and contact details of the contact person:

- Data Protection Officer: dpo@amazon.com, as specified in the AWS GDPR Data Processing Addendum;
- General contact details and current contact persons: available via the AWS contact page.

Third-country status:

1. Amazon Web Services EMEA S.à r.l. has its registered office in Luxembourg and is therefore established in a Member State of the European Union. AWS is used in the context of the processing covered by this Agreement, in particular for cloud storage, infrastructure and content delivery services. The content is stored in the origin storage in the AWS Region eu-central-1 (Frankfurt). The dynamic origin servers are operated under api-eu.onepage.io. To the extent that storage and processing in the origin storage and on the dynamic origin servers take place within the European Union, no transfer of personal data to a third country takes place in this respect.
2. For the delivery of static content via onecdn.io, the Amazon CloudFront service provided by Amazon Web Services EMEA S.à r.l. is used. Amazon CloudFront uses globally distributed edge locations. The edge location processing a request depends in particular on the network location of the requesting user, CloudFront's automated routing, the configuration of the distribution and the relevant cache status. Accordingly, the selected edge location need not be located in the same country as the requesting user and may be located outside the European Union. In the event of a cache miss, CloudFront may retrieve the requested content from the origin in Frankfurt via a regional edge cache and, depending on the cache configuration, temporarily store it at the selected edge location or at a regional edge location.

The following situations must be distinguished:

- a) Technical transit only. To the extent that a third country is used exclusively as a technical transit point for the transmission and personal data are neither made available to a recipient nor processed, stored or subjected to access by a recipient in that third country, this does not constitute a transfer within the meaning of Article 44 GDPR.
- b) Processing at an edge or regional edge location outside the European Union. This must be distinguished from processing operations at a CloudFront edge or regional edge location situated outside the European Union, including TLS termination, routing, content delivery or caching. Where personal data are processed or made available to a recipient at such a location, this may constitute a transfer within the meaning of Article 44 GDPR. The following distinctions apply:

- i. Adequacy decision pursuant to Article 45 GDPR. To the extent that the relevant edge or regional edge location is situated in a third country for which an applicable adequacy decision pursuant to Article 45 GDPR exists, the transfer is lawful on that basis, provided that the specific recipient and the specific processing fall within the material and personal scope of the adequacy decision. This applies in particular to Argentina, Brazil, Israel, Japan, Canada, the United States, New Zealand, Switzerland, South Korea and the United Kingdom.
- ii. Safeguards pursuant to Article 46 GDPR. To the extent that a processing operation in a third country constitutes neither mere technical transit nor a transfer covered by an applicable adequacy decision pursuant to Article 45 GDPR, the transfer shall be safeguarded in accordance with Article 46 GDPR. Based on the technical location assessment currently used, this applies in particular to Egypt, Australia, Bahrain, Chile, Hong Kong, India, Indonesia, Qatar, Kenya, Colombia, Malaysia, Mexico, Nigeria, Oman, Peru, the Philippines, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand, Türkiye, the United Arab Emirates and Vietnam.

Description of the processing: Amazon Web Services EMEA S.à r.l. processes personal data on behalf of the Processor in order to provide cloud storage, infrastructure and content delivery services. The processing includes, in particular, the storage and processing of content and other data on AWS infrastructure, including the storage of content in the origin storage in the AWS Region eu-central-1 (Frankfurt) and processing on the dynamic origin servers operated under api-eu.onepage.io. AWS is also used for infrastructure services required to provide, operate, secure and ensure the availability and recoverability of the platform and the websites created through the platform. For the delivery of static content via onecdn.io, Amazon CloudFront, a Content Delivery Network provided by Amazon Web Services EMEA S.à r.l., is used. Amazon CloudFront performs, in particular, TLS termination, request routing and content delivery and, depending on the relevant request and cache configuration, temporarily stores content at globally distributed edge and regional edge locations. In this context, the following data may in particular be processed: the IP address of the requesting client, the time of the request, the requested URL or path, technical request headers, query parameters transmitted and the requested content. Standard access logging and cookie logging are disabled. In addition, no edge functions are integrated that would result in the storage of additional logs relating to visitor requests.

Google Workspace

Name: Google Cloud EMEA Limited

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

Name, position and contact details of the contact person:

- Data Protection Officer: Kristie Chon Flynn, contactable through the privacy team via the Google Cloud data protection contact form, preferably using the administrator account;
- General information: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

Third-country status:

Not applicable, as Google Cloud EMEA Limited is established in Ireland, which is a Member State of the European Union. It is acknowledged that this Sub-processor has a parent company in the United

States. However, this Sub-processor has contractually assured the Processor that it will process the data exclusively within the European Union. The Processor is entitled to rely on this assurance. This is consistent with the case law of the courts within the European Union. For example, in its decision of 7 September 2022, case no. 15 Verg 8/22, the Higher Regional Court of Karlsruhe held as follows: “In this context, it assured that personal health data would be transferred exclusively to A. S.à r.l., L., and that, for the purpose of processing such data, the data would not leave the European Union but would be processed only in Germany. In addition, the joined party stated that A. S.à r.l., L. had assured it that all data of the joined party would be processed in Germany and confirmed during the oral hearing before the Senate that, by the time the offer was implemented, it would conclude all contracts internally required with A. which would give effect to the assurances made in its offer. The defendants were entitled to understand the statements made by the joined party in the tender documents as such a binding undertaking. The defendants were entitled to rely on this undertaking.”

Description of the processing:

Google Cloud EMEA Limited stores and processes personal data on behalf of the Processor for the provision of cloud storage and infrastructure services.

Cloudflare

Name: Cloudflare, Inc.

Address: 101 Townsend Street, San Francisco, CA 94107, United States of America

Name, position and contact details of the contact person:

- Data protection contact: Data protection enquiries may be submitted through the Cloudflare Privacy Portal;
- General contact details: Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, United States of America; enquiries may be submitted using the Cloudflare contact form;
- EU representative appointed for the European Economic Area: Cloudflare Portugal, Unipessoal Lda., Rua Alexandre Herculano 50, 8.º andar, 1250-011 Lisbon, Portugal.

Third-country status: Article 45 GDPR

Description of the processing: Cloudflare, Inc. processes personal data on behalf of the Processor for image optimisation and the technical processing of Open Graph preview images. When images are uploaded, the image files are transferred to Cloudflare once for optimisation. No visitor data are transferred in this process. The optimised images are subsequently stored in AWS cloud storage in the eu-central-1 (Frankfurt) Region and delivered via onecdn.io using Amazon CloudFront. For Open Graph preview images, URLs under /cdn-cgi/image/* are used. In the event of a cache miss, Amazon CloudFront forwards the relevant requests to Cloudflare for processing. Cloudflare adjusts the dimensions of the requested preview images. The relevant requests are made in particular by social-network crawlers when page links are shared. In this respect, visitors' browsers do not establish a direct connection to Cloudflare. In connection with these requests, Cloudflare may in particular be provided with the request path, selected query parameters and technical request information, including the IP address of the requesting client. The processing is carried out exclusively for the purpose of image optimisation and the delivery or provision of the requested Open Graph preview images. This does not apply where the Controller activates Cloudflare for its own domain.