Einwilligung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten

von

Name: Töpper_____

Vorname: Armin_____

Adresse: Bundeallee 46a, 10715 Berlin_____

E-Mail: armin@tekkeikan.de_____

Der Olympischer Sport-Club Berlin e.V. Tekkeikan | Kendosparte („Tekkeikan“) erhebt, verarbeitet und nutzt im Rahmen der sportlichen Zweckbestimmung (z.B. Statistische Erfassung, Meldungen zu Lehrgängen und Turnieren, Kommunikation und Veröffentlichung von Ergebnissen usw.) personenbezogene Daten von Mitgliedern seiner Mitgliedsvereine. Dazu zählen insbesondere Name, Vorname, Adresse, E-Mail, Telefonnummer, Geburtsdatum, und Graduierung. Diese Daten werden unter Berücksichtigung der Datenschutzgrundverordnung mithilfe der Google G Suite gespeichert und verwaltet. Die Kommunikation umfasst neben Rundmails auch die Printmedien sowie Social Media. Darüber hinaus werden unter anderem auf der Website des Tekkeikan die Graduierungen der Kyu- und DAN-Träger, Turnierergebnisse sowie Fotos veröffentlicht.
Ich willige hiermit ein, dass der Tekkeikan personenbezogene Daten von mir in oben genanntem Umfang erhebt, verarbeitet und nutzt. Dazu gehört auch die Weitergabe der Daten an mit dem Tekkeikan verbunden Sportorganisationen oder –verbänden im Rahmen der Erfüllung seiner Aufgaben.
Darüber hinaus willige ich ein, dass vom Tekkeikan mein Name, Foto und die Graduierung in den Medien z.B. Tekkeikan-Website veröffentlicht werden kann.
Diese Einwilligung ist unbefristet erteilt. Sie gilt auch für die Zeit nach Austritt aus dem Verein. Ich kann jederzeit widerrufen.

_____
Datum/Ort

_____
Unterschrift des Mitgliedes des Mitgliedsvereins
(bei Minderjährigen: der Erziehungsberechtigten)

Anlagen:

- Google G Suite Standard Contractual Clauses
- Data Processing Amendment to G Suite and/or Complementary Product Agreement
- UD Media Vertrag über die Verarbeitung von Daten i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

G Suite

Standard Contractual Clauses (processors)

for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

the non-Google legal entity accepting the Clauses (the "Data Exporter")

And

Google LLC (formerly known as Google Inc.),

1600 Amphitheatre Parkway, Mountain View, California 94043 USA

(the "**Data Importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

The Clauses (including Appendices 1 and 2) are effective from the date Data Exporter has both: (i) executed a valid G Suite Agreement and/or Complementary Product Agreement with Data Processing Amendment (collectively the "Services Agreement"); and (ii) clicked to accept these Clauses. In this document, "G Suite Agreement" and "Complementary Product Agreement" have the respective meanings given in the Data Processing Amendment. In this document, "Data Processing Amendment" means the amendment to the G Suite Agreement and/or Complementary Product Agreement that sets out certain terms in relation to the protection and processing of personal data.

If you are accepting on behalf of the Data Exporter, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand the Clauses; and (iii) you agree, on behalf of the party that you represent, to the Clauses. If you do not have the legal authority to bind the Data Exporter, please do not click the "I Accept" button below. The Clauses shall automatically expire on the termination or expiry of the Data Processing Amendment. The parties agree that where Data Exporter has been presented with these Clauses and clicked to accept these terms electronically, such acceptance shall constitute execution of the entirety of the Clauses by both parties, subject to the effective date described above.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '***personal data***', '***special categories of data***', '***process/processing***', '***controller***', '***processor***', '***Data Subject***' and '***Supervisory Authority***' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the ***Data Exporter***' means the controller who transfers the personal data;

(c) 'the ***Data Importer***' means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;

(d) 'the ***Subprocessor***' means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other

subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the ***applicable data protection law***' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) '***technical and organisational security measures***' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer[1]

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.

2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.

3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of

law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject;

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-Processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do

so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.

4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses
This Appendix forms part of the Clauses
Data Exporter

The Data Exporter is the non-Google legal entity that is a party to the Clauses.

Data Importer

The Data Importer is Google LLC, a global provider of a variety of technology services for individuals and businesses.

Data Subjects

The personal data transferred concern the following categories of data subjects: the Data Exporter's end users including employees and contractors; the personnel of the Data Exporter's customers, suppliers and subcontractors; and any other person who transmits data via the "Services" (as defined in the Data Processing Amendment) including individuals collaborating and communicating with the Data Exporter's end users.

Categories of data

The personal data transferred concern the following categories of data: personal data submitted, stored, sent or received by the Data Exporter or its end users via the Services including user IDs, emails, documents, presentations, images, calendar entries, tasks and other data submitted, stored, sent or received by end users via the Services.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: data submitted, stored, sent or received by end users via the Services.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Scope of Processing.

The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Appendix pursuant to the provision of the Services.

Personal data may be processed for the following purposes: to provide the Services and related technical support services.

The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or any of its Subprocessors maintains facilities.

Term of Data Processing.

Data processing will be for the period specified in the Data Processing Amendment. Such period will automatically terminate upon the deletion by the Data Importer of all data as described in the Data Processing Amendment.

Data Deletion.

During the term of the Services Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Services in accordance with the Services Agreement. After termination or expiry of the Services Agreement, the Data Importer will delete the Data Exporter's personal data in accordance with the Data Processing Amendment.

Access to Data.

During the term of the Services Agreement, the Data Importer will provide the Data Exporter with access to and the ability to rectify, restrict processing of and export the Data Exporter's personal data from the Services in accordance with the Services Agreement.

Subprocessors.

The Data Importer may engage Subprocessors to provide parts of the Services and related technical support services. The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Services and related technical support services and not for any other purpose.

Appendix 2

to the Standard Contractual Clauses
This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the Data Importer in

accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer currently takes and implements the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the Services Agreement.

1. Data Center & Network Security.

(a) Data Centers.

Infrastructure. The Data Importer maintains geographically distributed data centers. The Data Importer stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow the Data Importer to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. The Data Importer servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. The Data Importer employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments. Businesses Continuity. The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers.This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. The Data Importer transfers data via Internet standard protocols.

External Attack Surface. The Data Importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The Data Importer considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. The Data Importer's intrusion detection involves

1. Tightly controlling the size and make-up of the Data Importer's attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and the Data Importer's security personnel will react promptly to known incidents.

Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. The Data Importer's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. The Data Importer maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. The Data Importer's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers

connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. The Data Importer has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents. Access Control and Privilege Management. The Data Exporter's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator

Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.The Data Importer employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide the Data Importer with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The Data Importer requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with the Data Importer's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), the Data Importer uses hardware tokens.

3. Data.

(a) Data Storage, Isolation & Authentication.

The Data Importer stores data in a multi-tenant environment on the Data Importer-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. The Data Importer logically isolates data on a per end user basis at the application layer. The Data Importer logically isolates the Data Exporter's data, and logically separates each end user's data from the data of other end users, and data for an authenticated end user will not be displayed to another end user (unless the former end user or an administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data. The Data Exporter will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will

enable the Data Exporter to determine the product sharing settings applicable to end users for specific purposes. The Data Exporter may choose to make use of certain logging capability that the Data Importer may make available via the Services, products and APIs. The Data Exporter agrees that its use of the APIs is subject to the API terms of use. The Data Importer agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) Decommissioned Disks and Disk Erase Policy.

Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving the Data Importer's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security.

The Data Importer's personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g., certifications). The Data Importer's personnel will not process customer data without authorization.

5. Subprocessor Security.

Before onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms as described in Section 11.3 of the Data Processing Amendment.

6. Data Privacy Officer.

The Data Importer's Data Protection Team can be contacted by the Data Exporter's Adminstrators at: https://support.google.com/a/contact/googlecloud_dpr (or via such other means as may be provided by the Data Importer). Administrators must be signed in to their admin account for the Services to use this address.

---

[1]Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

G Suite and/or Complementary Product Model Contract Clauses, Version 1.4

Google Cloud

Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.1)

The Customer agreeing to these terms ("**Customer**") and Google LLC (formerly known as Google Inc.), Google Ireland Limited, Google Commerce Limited, Google Asia Pacific Pte. Ltd or Google Australia Pty Ltd (as applicable, "**Google**") have entered into one or more G Suite Agreement(s) (as defined below) and/or Complementary Product Agreements(s) (as defined below) (each, as amended from time to time, an "**Agreement**").

This Data Processing Amendment to G Suite and/or Complementary Product Agreement including its appendices (the "**Data Processing Amendment**") will, as from the Amendment Effective Date (as defined below), be effective and replace any previously applicable data processing amendment and/or other terms previously applicable to privacy, data processing and/or data security.

1. **Introduction**.

   This Data Processing Amendment reflects the parties' agreement with respect to the terms governing the processing and security of Customer Data under the applicable Agreement.

2. **Definitions**.

   2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given elsewhere in the applicable Agreement. In this Data Processing Amendment, unless stated otherwise:

   "**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

   "**Additional Security Controls**" means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines. "Additional Security Controls" may include the Admin Console and other features and functionality of the Services such as two factor authentication, security key enforcement and monitoring capabilities.

   "**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any of its Affiliates display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using any Google Sites functionality within the Services).

   "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

   "**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the applicable Agreement, either per annual period or event giving rise to liability, as applicable.

   "**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

"**Amendment Effective Date**" means the date on which Customer accepted, or the parties otherwise agreed to, this Data Processing Amendment.

"**Audited Services**" means the Services (as defined below), unless the G Suite Services Summary or Complementary Product Services Summary indicates otherwise.

"**Complementary Product Agreement**" means: a Cloud Identity Agreement or other agreement under which Google agrees to provide identity services as such to Customer; Hire Agreement; or other agreement that incorporates this Data Processing Amendment by reference or states that it will apply if accepted by Customer.

"**Complementary Product Services Summary**" means the then-current description of the services provided under a Complementary Product Agreement, as set out in the applicable Agreement.

"**Customer Data**" means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Customer Personal Data**" means personal data contained within the Customer Data.

"**Data Incident**" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Domain**" means the primary domain and any secondary domains managed together by Customer within a single instance of the Admin Console.

"**EEA**" means the European Economic Area.

"**European Data Protection Legislation**" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Full Activation Date**" means: (a) if this Data Processing Amendment is automatically incorporated into the applicable Agreement, the Amendment Effective Date; or (b) if Customer accepted or the parties otherwise agreed to this Data Processing Amendment, the eighth day after the Amendment Effective Date.

"**GDPR**" means 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.

"**Google's Third Party Auditor**" means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

"**G Suite Agreement**" means: one or more Order Form(s) specifying that Google will provide any services described in the G Suite Services Summary under a Master Agreement, combined with a set of General Terms and a G Suite Services Schedule; a G Suite Agreement; a G Suite for Education Agreement; a Google Apps for Work Agreement; a Google Apps Enterprise Agreement; a Google Apps for Business Agreement; a Google Apps for Education Agreement; a Via Reseller version of any of the foregoing agreements; or any other agreement under which Google agrees to provide any services described in the G Suite Services Summary to Customer.

"**G Suite Services Summary**" means the then-current description of the G Suite services (including related editions), as set out at https://gsuite.google.com/terms

/user_features.html (as may be updated by Google from time to time in accordance with the G Suite Agreement).

"**ISO 27001 Certification**" means ISO/IEC 27001:2013 certification or a comparable certification, as related to the Audited Services.

"**ISO 27017 Certification**" means ISO/IEC 27017:2015 certification or a comparable certification, as related to the Audited Services.

"**ISO 27018 Certification**" means ISO/IEC 27018:2014 certification or a comparable certification, as related to the Audited Services.

"**Model Contract Clauses**" or "MCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

"**Non-European Data Protection Legislation**" means data protection or privacy legislation in force outside the European Economic Area and Switzerland.

"**Notification Email Address**" means the email address(es) designated by Customer in the Admin Console or the Order Form to receive certain notifications from Google.

"**Security Documentation**" means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).

"**Security Measures**" has the meaning given in Section 7.1.1 (Google's Security Measures).

"**Services**" means the following services, as applicable: (a) the Core Services for G Suite, as described in the G Suite Services Summary; (b) the Other Services for G Suite, as described in the G Suite Services Summary; and/or (c) the services described in the Complementary Product Services Summary. For clarity, in relation to G Suite, the Services exclude Google+ to the extent it is used to share content or interact with any persons outside an End User's G Suite Domain, and exclude any "other add-on services" described in the G Suite Services Summary.

"**SOC 2 Report**" means a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability, as produced by Google's Third Party Auditor in relation to the Audited Services.

"**SOC 3 Report**" means a Service Organization Control (SOC) 3 Report (or a comparable report), as produced by Google's Third Party Auditor in relation to the Audited Services.

"**Subprocessors**" means third parties authorized under this Data Processing Amendment to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.

"**Term**" means the period from the Amendment Effective Date until the end of Google's provision of the Services under the applicable Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.

2.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Data Processing Amendment have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the Model Contract Clauses, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

3. **Duration of Data Processing Amendment**. This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Google as described in this Data Processing Amendment.

4. **Scope of Data Protection Legislation**.

4.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if, for example:

(a) the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA; and/or

(b) the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

4.2 Application of Non-European Legislation. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

4.3 Application of Data Processing Amendment. Except to the extent this Data Processing Amendment states otherwise, the terms of this Data Processing Amendment will apply irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies to the processing of Customer Personal Data.

5. **Processing of Data**.

5.1 **Roles and Regulatory Compliance; Authorization**.

5.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Appendix 1;

(b) Google is a processor of that Customer Personal Data under the European Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of that Customer Personal Data under the European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Google that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Google as another processor, have been authorized by the relevant controller.

5.1.3. Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.2 **Scope of Processing**.

5.2.1 Customer's Instructions. By entering into this Data Processing Amendment,

Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and related technical support; (c) as documented in the form of the applicable Agreement, including this Data Processing Amendment; and (d) as further documented in any other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment.

5.2.2 Google's Compliance with Instructions. As from the Full Activation Date (at the latest), Google will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Google is subject requires other processing of Customer Personal Data by Google, in which case Google will inform Customer (unless that law prohibits Google from doing so on important grounds of public interest) via the Notification Email Address. For clarity, Google will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services.

5.3. **Additional Products**. If Google at its option makes any Additional Products available to Customer in accordance with the Additional Product Terms, and if Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services.

6. **Data Deletion**.

6.1. **Deletion During Term**. Google will enable Customer and/or End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the applicable Term and the Customer Data cannot be recovered by Customer or an End User (such as from the "trash"), this use will constitute an instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

6.2. **Deletion on Term Expiry**. Subject to Section 6.3 (Deferred Deletion Instruction), on expiry of the applicable Term Customer instructs Google to delete all Customer Data (including existing copies) from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain afterwards.

6.3. **Deferred Deletion Instruction**. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Data Processing Amendment will continue to apply to such Customer Data until its deletion by Google.

7. **Data Security**.

7.1. **Google's Security Measures, Controls and Assistance**.

7.1.1. Google's Security Measures. Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "**Security Measures**"). As described in Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7.1.2. Security Compliance by Google Staff. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3. Additional Security Controls. In addition to the Security Measures, Google will make the Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4. Google's Security Assistance. Customer agrees that Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

(b) making the Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);

(c) complying with the terms of Section 7.2 (Data Incidents); and

(d) providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Amendment.

7.2. **Data Incidents**.

7.2.1. Incident Notification. If Google becomes aware of a Data Incident, Google will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2. Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Google recommends Customer take to address the Data Incident.

7.2.3. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Google's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4. No Assessment of Customer Data by Google. Google will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements.

Without prejudice to Google's obligations under this Section 7.2 (Data Incidents), Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5. No Acknowledgement of Fault by Google. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3. **Customer's Security Responsibilities and Assessment**.

7.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Google's obligations under Section 7.1 (Google's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and

(iii) retaining copies of its Customer Data as appropriate; and

(b) Google has no obligation to protect copies of Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (for example, offline or on-premise storage), or to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent Customer has opted to use them.

7.3.2. Customer's Security Assessment.

(a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Google's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Google as set out in Section 7.1.1 (Google's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4. **Security Certifications and Reports**. Google will do the following to evaluate and help ensure the continued effectiveness of the Security Measures:

(a) maintain the ISO 27001 Certification, the ISO 27017 Certification and the ISO 27018 Certification; and

(b) update the SOC 2 Report and SOC 3 Report at least once every 18 months.

7.5. **Reviews and Audits of Compliance**.

7.5.1. Reviews of Security Documentation. In addition to the information contained in the applicable Agreement including this Data Processing Amendment, Google will make available for review by Customer the following documents and information to demonstrate

compliance by Google with its obligations under this Data Processing Amendment:

(a) the certificates issued in relation to the ISO 27001 Certification, the ISO 27017 Certification and the ISO 27018 Certification;

(b) the then-current SOC 3 Report; and

(c) the then-current SOC 2 Report, following a request by Customer in accordance with Section 7.5.3(a).

7.5.2. Customer's Audit Rights.

(a) If the European Data Protection Legislation applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Data Processing Amendment in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance).

(b) If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, without prejudice to any audit rights of a supervisory authority under such Model Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

(c) Customer may also conduct an audit to verify Google's compliance with its obligations under this Data Processing Amendment by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

7.5.3. Additional Business Terms for Reviews and Audits.

(a) Customer must send any requests for reviews of the SOC 2 Report under Section 7.5.1(c) or audits under Section 7.5.2(a) or 7.5.2(b) to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).

(b) Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 Report under Section 7.5.1(c); and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).

(c) Google may charge a fee (based on Google's reasonable costs) for any review of the SOC 2 Report under Section 7.5.1(c) and/or audit under Section 7.5.2(a) or 7.5.2(b). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(d) Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to

appoint another auditor or conduct the audit itself.

7.5.4. No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA).

8. **Impact Assessments and Consultations**. Customer agrees that Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

(a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation); and

(b) providing the information contained in the applicable Agreement including this Data Processing Amendment.

9. **Data Subject Rights; Data Export**.

9.1. **Access; Rectification; Restricted Processing; Portability**. During the applicable Term, Google will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion During Term), and to export Customer Data.

9.2. **Data Subject Requests**.

9.2.1. Customer's Responsibility for Requests. During the applicable Term, if Google receives any request from a data subject in relation to Customer Personal Data, Google will advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2. Google's Data Subject Request Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) Google will assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

(a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and

(b) complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. **Data Transfers**.

10.1. **Data Storage and Processing Facilities**. Customer agrees that Google may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process Customer Data in the United States and any other country in which Google or any of its Subprocessors maintains facilities.

10.2. **Transfers of Data Out of the EEA**.

10.2.1. Google's Transfer Obligations. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA and the

European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data") under any Agreement, Google will, in relation to Transferred Personal Data under all Agreements:

(a) if requested to do so by Customer, ensure that Google LLC as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or

(b) offer an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data under any Agreement, Customer agrees that:

(a) if under the European Data Protection Legislation Google reasonably requires Customer to enter into Model Contract Clauses in respect of such transfers, Customer will do so; and

(b) if under the European Data Protection Legislation Google reasonably requires Customer to use an Alternative Transfer Solution offered by Google, and reasonably requests that Customer take any action (which may include execution of documents) strictly required to give full effect to such solution, Customer will do so.

10.3. **Data Center Information**. Information about the locations of Google data centers is available at: https://www.google.com/about/datacenters/inside/locations/index.html (as may be updated by Google from time to time).

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. **Subprocessors**.

11.1. **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Amendment Effective Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Google Affiliates from time to time. In addition, Customer generally authorizes the engagement as Subprocessors of any other third parties ("**New Third Party Subprocessors**"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Google LLC of the processing of Customer Data if such consent is required under the Model Contract Clauses.

11.2. **Information about Subprocessors**. Information about Subprocessors, including their functions and locations, is available at https://gsuite.google.com/intl/en/terms/subprocessors.html (as may be updated by Google from time to time in accordance with this Data Processing Amendment).

11.3. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Google will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Data Processing Amendment) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Google as described in Section 10.2 (Transfers of Data Out of the EEA); and

(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Amendment, are imposed on the Subprocessor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4. **Opportunity to Object to Subprocessor Changes**.

(a) When any New Third Party Subprocessor is engaged during the applicable Term, Google will, at least 30 days before the New Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

(b) Customer may object to any New Third Party Subprocessor by terminating the applicable Agreement immediately upon written notice to Google, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

12. **Cloud Data Protection Team; Processing Records**.

12.1. **Google's Cloud Data Protection Team**. Google's Cloud Data Protection Team can be contacted by Customer's Administrators at https://support.google.com/a/contact/googlecloud_dpr (while Administrators are signed in to their Admin Account) and/or by Customer by providing a notice to Google as described in the applicable Agreement.

12.2. **Google's Processing Records**. Customer acknowledges that Google is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Google is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Google via the Admin Console or other means provided by Google, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. **Liability**.

13.1. **Liability Cap**. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data Out of the EEA), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party, subject to Section 13.2 (Liability Cap Exclusions).

13.2. **Liability Cap Exclusions**. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. **Third Party Beneficiary**. Notwithstanding anything to the contrary in the applicable Agreement,

where Google LLC is not a party to such Agreement, Google LLC will be a third party beneficiary of Section 7.5 (Reviews and Audits of Compliance), Section 11.1 (Consent to Subprocessor Engagement) and Section 13 (Liability) of this Data Processing Amendment.

15. **Effect of Amendment**. To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, such Agreement remains in full force and effect. For clarity, if Customer has entered more than one Agreement, this Data Processing Amendment will amend each of the Agreements separately.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services and related technical support to Customer.

Duration of the Processing

The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by Google in accordance with the Data Processing Amendment.

Nature and Purpose of the Processing

Google will process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with the Data Processing Amendment.

Categories of Data

Personal data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other data.

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As from the Amendment Effective Date, Google will implement and maintain the Security Measures set out in this Appendix 2 to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. Data Center & Network Security.

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are

designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. Employing intelligent detection controls at data entry points; and
3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

3. Data.

(a) Data Storage, Isolation & Authentication.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End Users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) Decommissioned Disks and Disk Erase Policy.

Disks containing data may experience performance issues, errors or hardware failure that lead

them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security.

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security.

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

G Suite and Complementary Product Data Processing Amendment, Version 2.1

Vertrag über die Verarbeitung von Daten i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

zwischen

Olympischer Sport-Club Berlin e.V. - Kendo Sparte, Armin Töpper, Priesterweg 8, DE-10829 Berlin

- Auftraggeber -

und

UD Media GmbH, Kölner Str. 28, 41812 Erkelenz

vertreten durch die Geschäftsführer Herr Thomas Borgans und Herr Ronny Schick

- Auftragnehmer -

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom 29.01.2018 in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1. Gegenstand des Auftrags ist die Bereitstellung von Hosting-Lösungen bzw. eines (oder mehrerer) dedizierten/dedizierter Server sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. . Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.A. z.B. eines Webservers, FTP-Servers oder SSH (insoweit verfügbar) die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

2. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben. Der Auftrag endet, wenn der Auftraggeber keine Hosting-Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

3. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format

(Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Wendet sich eine betroffene Person mit Forderungen zur Auskunft, Berichtigung, Sperrung oder Löschung an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.
4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

6. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

§ 4 Allgemeine Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen im Sinne des Artikel 28 Abs. 3 a) DSGVO, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf

Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt (vgl. Anlage 2). Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 f. DSGVO erfüllt sind. Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen ebenfalls für diese.

6. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

   In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

11. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der

Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.

   Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, als Post-/Transportdienstleistungen, unter Einbeziehung von Berufsgeheimnisträgern (Rechtsanwälte, Wirtschaftsprüfer), durch Inkassobüros mit Forderungsübertragungen, durch Bankdienstleistungen für den Geldtransfer in Anspruch nimmt. Auch die Wartung oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen gehören nicht dazu, insofern der Auftragnehmer sicherstellt, dass kein unmittelbarer Zugriff auf personenbezogene Daten erfolgt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.
3. Der Auftragnehmer trägt dafür Sorge, dass der Auftraggeber eine aktuelle Liste der eingesetzten Unterauftragnehmer im Kundenportal stets zum Abruf zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragnehmern ergeht hierüber eine Information an den Auftraggeber.
4. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragnehmer zu übertragen.

§ 8 Geheimhaltungspflichten

1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 9 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im übrigen nicht.
4. Es gilt deutsches Recht.

§ 10 Haftung und Schadensersatz

1. Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.
2. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verbreiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Berlin, den 20.08.2018

Auftraggeber

Erkelenz, den 04.06.2018

UDMEDIA
Mit Sicherheit zur eigenen Homepage

Auftragnehmer

Anlagen:

- Gegenstand des Auftrags
- Technische und organisatorische Maßnahmen

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst die Bereitstellung von Hosting-Lösungen bzw. eines (oder mehrerer) dedizierten/dedizierter Server sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. im Rahmen der vom Auftragnehmer auf dessen Webseiten angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkte.

2. Art(en) der personenbezogenen Daten*

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- [X] Abrechnungsdaten
- [ ] Angebotsdaten
- [ ] Finanzdaten
- [ ] Bankverbindungsdaten
- [X] Bestelldaten
- [X] E-Mail-Nachrichten
- [ ] Mitarbeiterdaten
- [ ] Vertragsdaten
- [ ] Stammdaten
- [ ] Nutzungsdaten
- [X] Videos / Bilder
- [ ] _____
- [ ] _____

* Zutreffendes vom Auftraggeber anzukreuzen

3. Kategorien betroffener Person*

Kreis der von der Datenverarbeitung betroffenen Personen:

- ☐ Kunden
- ☐ Mitarbeiter
- ☐ Angehörige
- ☒ Nutzer
- ☐ Auszubildene
- ☐ Unterhaltsberechtigte
- ☒ Interessenten
- ☐ Bewerber
- ☐ Ruheständler
- ☒ Kontaktpersonen
- ☐ Praktikanten
- ☐ Pressevertreter
- ☐ Lieferanten / Dienstleister
- ☐ Frühere Mitarbeiter
- ☐ Geschädigte
- ☐ Geschäftspartner
- ☐ Berater
- ☐ Zeugen
- ☐ Gesellschafter
- ☒ Mitglieder
- ☐ Makler / Vermittler
- ☐ Mieter

☐ _____

☐ _____

* Zutreffendes vom Auftraggeber anzukreuzen

Anlage 2
Technische und organisatorische Maßnahmen

UD Media trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

- Zutrittssystem zur Rechenzentrums-Fläche nach Anmeldung und vorheriger Avisierung mit kontaktlosem Ausweissystem, PIN-Code und Dokumentation
- Zutritt zu Server-Racks mittels RFID-kodierten KEMAS-Schlüsseln
- Videoüberwachung der Außenbereiche und Räume mit Aufzeichnung
- Detektierte Zaunanlage zur Abgrenzung des Gebäudes
- 24 Stunden / 7 Tage besetzter Leitstand auf dem Gelände
- 24 Stunden / 7 Tage Sicherheitspersonal vor Ort
- Zertifizierung des Betreibers (Telehouse Deutschland GmbH, Frankfurt am Main): ISO/IEC 27001:2013, IDW PS951, ISAE 3402, ISO 9001, PCI:DSS

Zugangskontrolle

- UD Media vermietet die Datenverarbeitungsanlage an den Kunden.
- Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung.
- Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden („Herr der Daten“) .
- Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt.

- UD Media sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Aufzeichnungen darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden
- Die Datenverarbeitung selbst erfolgt durch den Kunden. UD Media hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.
- Besonderheiten für Webhosting-Kunden und Managed-Server-Kunden: UD Media nutzt autorisierte Benutzerkennungen (Keys) und individuelle, sichere Passwörter für den Zugang zu Datenverarbeitungssystemen. Die konkreten Verarbeitungsvorgänge beim Kunden sind UD Media nicht bekannt. Insofern obliegt es dem Kunden durch softwaretechnische Gestaltungen dafür Sorge zu tragen, dass die Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können.
- Besonderheiten für Root-Server-Kunden: Bei Root-Servern haben Mitarbeiter von UD Media keinerlei Zugang. Dementsprechend obliegt es dem Kunden, das System zu sichern.

Zugriffskontrolle

- UD Media hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass der Zugriff auf Daten ausschließlich durch den Kunden erfolgt.
- Mitarbeiter von UD Media sind gemäß DSGVO zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.
- Adäquate Protokollierung der Tätigkeiten von UD Media
- Webhosting & Managed-Server-Kunden: Monitoring und Wartung der Systeme durch UD Media mit adäquater Protokollierung der Administrationszugriffe.
- Bei Root-Servern haben unsere Mitarbeiter keinerlei Zugang. Ein Zugriff auf Daten erfolgt nur, insoweit der Kunde UD Media explizit mit einer Administrationsaufgabe beauftragt und einen Zugang einrichtet.

Trennungskontrolle

- Bitte beachten Sie hierzu unsere Ausführungen unter „Zugangskontrolle“ und „Zugriffskontrolle“.
- Webhosting & Managed-Server-Kunden: Es liegt eine logische Trennung einzelner Kundensysteme vor.
- Root-Server: Es liegt eine logische und physikalische Trennung einzelner Kundensysteme vor.
- Jedes System verfügt über ein Berechtigungskonzept.

Pseudonymisierung & Verschlüsselung

- Für die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten ist der Kunde verantwortlich, soweit dies nach dem Verwendungszweck möglich ist und keine im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

2. Integrität

Eingabekontrolle

- Mitarbeiter von UD Media dürfen grundsätzlich nicht auf Daten des Kunden zugreifen bzw. Daten eingeben, verändern oder löschen.
- UD Media hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden erfolgen kann.
- Beauftragt der Kunde UD Media explizit zur Eingabe, Änderung oder des Löschens von Daten des Kunden erfolgt eine Aufzeichnung von Mitarbeiterzugriffen von UD Media auf Daten des Kunden in Logfiles gemäß gesetzlicher Bestimmungen.

- Sperrungen erfolgen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges. Die Vornahme von Sperrungen wird protokolliert.
- Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

Weitergabekontrolle

- Verschlüsselte Datenkommunikation für administrative Aufgaben seitens UD Media, z.B. per SSL-Verschlüsselung
- Verschlüsselter Transport von E-Mails (TLS/SSL)
- Dem Kunden obliegt es durch eine Verschlüsselung, z.B. dem Einsatz eines SSL-Zertifikats, dafür zu sorgen, dass übertragene Daten (z.B. das Auslesen von Daten in Kontaktformularen) nicht lesbar sind.
- Zugriffsrechte der einzelnen Mitarbeiter von UD Media orientieren sich an der Erforderlichkeit für die Aufgabenerfüllung (z.B. Administratoren im Rahmen der Verwaltung der Netzwerkhardware oder zur Wartung der Systeme)

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeit

- Maßnahmen zum Brandschutz und bei Stromausfällen
    - N+1 redundant ausgelegte Klimatisierungssysteme
    - Konstante Raumtemperatur von 24° (+2/-4°)
    - Temperaturüberwachung mittels Sensoren
    - Optische/thermische Brandmelder auf zwei Ebenen (Rohdecke und Doppelboden)
    - Aktive Brandlöschung durch Inergen-Löschanlage, Doppelboden- und/oder Raumlöschung

- Zwei unabhängige Stromversorgungen (A+B-Feed)
- N+1 redundante, USV-gesicherte Stromversorgung mit Batterie-Backup
- Notstromversorgung mit einer Gesamtleistung von 21MVA
- RZ-Betrieb kann bei Stromausfall 3 Tage unter Volllast aufrecht erhalten werden
- Redundante Netzwerkanbindung

Für darüber hinausgehende Schutzmaßnahmen, insbesondere auf der Ebene des Betriebssystems, ist der Kunde verantwortlich. UD Media bietet Optionen zur Sicherstellung durch den Abschluss von individuellen Service-Level-Agreements und Backup-Tarifen.

Belastbarkeit

Alle Systeme, welche für die Infrastruktur der Dienstleistung von UD Media relevant sind, werden redundant vorgehalten und überwacht. Für die Belastbarkeit der Systeme des Kunden ist der Kunden selbst verantwortlich. Es können Schutzmaßnahmen aktiviert werden, um DDOS-Angriffe auf die Systeme des Kunden abzuwehren.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(1) Datenschutz-Management-System

- Eine Datenschutzleitlinie der Unternehmensleitung
- Richtlinien zum Umgang mit personenbezogenen Daten und der zugehörigen IT für alle Mitarbeiter
- Verfahren, die den konkreten Umgang mit personenbezogenen Daten regeln
- Bestellung eines Datenschutzbeauftragten (insoweit erforderlich)

(2) Incident Response Management

- Richtlinien für Mitarbeiter, wie mit möglichen Sicherheitsvorfällen umzugehen ist
- Verfahren, wie die verantwortliche Stelle mit festgestellten oder gemeldeten Sicherheitsvorfällen umzugehen hat, insbesondere, wann ein Datenschutzbeauftragter und die Datenschutzbehörde zu involvieren ist.

(3) Auftragskontrolle

- Sorgfältige Auswahl von Auftragsverarbeitern gemäß DSGVO
- Insofern UD Media Subunternehmer bestellt, gelten für diese die gleichen Regelungen und Bestimmungen wie für UD Media selbst.
- Anweisung an Mitarbeiter von UD Media über Umfang und Inhalt der vom Kunden erteilten Weisungen
- Verpflichtung der Mitarbeiter von UD Media auf das Unterzeichnen einer Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO