Anhang zur Datenverarbeitung

Bitte lesen Sie diese Vereinbarung sorgfältig durch, da sie wichtige Informationen zu Ihren Rechten und Rechtsmitteln enthält.

Die englische Version der gesetzlichen Vereinbarungen und Richtlinien gilt als die einzige aktuelle und gültige Version dieses Dokuments. Jede übersetzte Version wird nur als Service bereitgestellt, um das Lesen und Verstehen der englischen Version zu erleichtern. Übersetzte Versionen sind nicht rechtsverbindlich und können die englischen Versionen nicht ersetzen. Im Falle von Meinungsverschiedenheiten oder Konflikten haben die englischsprachigen rechtlichen Vereinbarungen und Richtlinien Vorrang.

Anhang zur Datenverarbeitung

Letzte Überarbeitung: 2025-07-01 12:52:40

This Data Processing Addendum (the "Addendum") is executed by and between Hostinger International Ltd. (a Cyprus private limited company, registered address 61 Lordou Vironos str., 6023 Larnaca, Cyprus) or Hostinger UK Limited (UK private limited company, registered address Nwms Center, 31 Southampton Row, Office 3.11, 3rd Floor, London, England, WC1B 5HJ) and, if applicable, its Affiliates ("Hostinger") and you ("Customer") and is annexed to and supplements our Terms of Service and any and all agreements governing Covered Services (collectively, the "Terms of Service").

1. DEFINITIONS

1.1 Unless otherwise defined in this Addendum, all capitalized terms not defined in this Addendum will have the meanings given to them in the Terms of Service.

"Affiliates" means any entity which is controlled by, controls or is in common control with Hostinger.

“Covered Services” means hosted services that could involve our Processing of Personal Data, such as: (1) Hosting Services, (2) VPS Services, (3) Email Services, (4) Domain Services, (5) Website Builder, (6) Hostinger Horizons, (7) Hostinger Reach.

“Customer Data” means the Personal Data of any Data Subject Processed by Hostinger within the Hostinger Network on behalf of Customer pursuant to or in connection with the Terms of Service.

“Data Protection Laws” means all data protection or privacy laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to the (i) the Australian Privacy Principles and the Australian Privacy Act (1988), (ii) Brazil’s Lei Geral de Proteção de Dados (LGPD), (iii) the California Consumer Privacy Act (CCPA), (iv) Canada’s Federal Personal Information Protection and Electronic Documents Act (PIPEDA), (v) the EU GDPR, (vi) any national data protection laws made under or pursuant to the GDPR (vii) the EU e-Privacy Directive (Directive 2002/58/EC), (viii) Singapore’s Personal Data Protection Act 2012 (PDPA), (ix) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance, and (x) UK GDPR or Data Protection Act 2018; in each case as may be amended, superseded or replaced.

“EEA” means the European Economic Area.

“EU GDPR” means the 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.

“EU Standard Contractual Clauses” means the standard data protection clauses approved by the European Commission decision 2021/914 of 4 June 2021, incorporated herein by reference. Module Two (Controller to Processor) EU Standard Contractual Clauses and Module Three (Processor to Processor) EU Standard Contractual Clauses are available for download at the EUR-Lex website.

“Hostinger Network” means Hostinger’s data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within Hostinger’s control and are used to provide the Covered Services.

“Security Incident”means a breach of security of the Hostinger Security Standards resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data on systems managed or controlled by Hostinger.

“Security Standards” means the security standards attached to this Addendum as Appendix 2.

"Sensitive Data" means (a) social security number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother’s maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of “special categories of data” under GDPR or any other applicable law or regulation relating to privacy and data protection.

“Sub-Processor” means any Processor engaged by Hostinger to Process data on behalf of Customer.

“UK GDPR” means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

“UK International Data Transfer Addendum” means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, incorporated herein by reference. The UK International Data Transfer Addendum is available for download at the UK Information Commissioner's Website

1.2 The terms “Personal Data”, “Data Subject”, “Processing”, “Controller” and “Processor” as used in this Addendum have the meanings given in the EU GDPR irrespective of which Data Protection Laws apply.

2. SCOPE OF THE DATA PROCESSING AND RELATIONSHIP OF PARTIES

2.1 Hostinger as Processor. The parties acknowledge and agree as follows: (i) that Hostinger is a Processor of Customer Data under Data Protection Laws; (ii) that Customer is a Controller or Processor, as applicable, of the Customer Data under Data Protection Laws; and (iii) that each party will comply with its obligations under applicable Data Protection Laws with respect to the Processing of Customer Data.

2.2 Details of Data Processing. The subject matter of Processing Customer Data by Hostinger is the performance of the Covered Services pursuant to the Terms of Service. Hostinger shall only process Customer Data for the following purposes: (i) Processing in accordance with the Terms of Service; (ii) Processing initiated by end users in their use of the Covered Services; (iii) Processing to comply with other documented, reasonable instructions provided by Customers (ex. via email) where such instructions are consistent with the Terms of Service. Hostinger shall not: (a) process, retain, use, sell, or disclose Customer Data except as necessary to provide Covered Services pursuant to the Terms of Service, or as required by law; (b) sell such Customer Data to any third party; (c) retain, use, or disclose such Customer Data outside of the direct business relationship between Hostinger and Customer, unless otherwise required by law.

For the avoidance of doubt, Processing of Customer Data shall comply with all Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. If Customer is a Controller of the Customer Data, Customer acknowledges and agrees as follows: (i) Customer must use commercially reasonable efforts to disclose clearly, and obtain consent to, any data collection, sharing and usage that takes place on any Covered Services; and (ii) Customer must make clear that as a consequence of your use of Covered Services, end user’s data may be processed outside of their country of origin. If Customer is a Processor of the Customer Data, Customer warrants that Customer’s instructions and actions with respect to Customer Data, including the appointment of Hostinger as another Processor, have been authorized by the relevant Controller. Hostinger shall not be required to comply with or observe Customer's instructions if such instructions would violate Data Protection Laws. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this Addendum are further specified in Appendix 1 ('Details of the Processing') to this Addendum.

3. CONFIDENTIALITY OF CUSTOMER DATA

Hostinger will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). In the event Hostinger receives a valid civil subpoena, and to the extent permitted, Hostinger will endeavor to provide Customer with reasonable notice of the demand via email or postal mail to allow Customer to seek a protective order or other appropriate remedy (unless otherwise required by subpoena, court order or any other valid legal document).

4. SHARED RESPONSIBILITY MODEL OF SECURITY

4.1 Hostinger has implemented and will maintain the technical and organizational measures for the Hostinger Network as described herein this Section and as further described in Appendix 2 to this Addendum, Security Standards. In particular, Hostinger has implemented and will maintain the following technical and organizational measures that address the (i) security of the Hostinger Network; (ii) physical security of the facilities; (iii) controls around employee and contractor access to (i) and/or (ii); and (iv) processes for testing, assessing and evaluating the effectiveness of technical and organizational measures implemented by Hostinger. In the event that we are not able to meet any of our obligations set forth herein, we will provide written notice (via our website or email) as soon as practically feasible.

4.2 Hostinger makes available a number of security features and functionalities that Customer may elect to use in relation to the Covered Services. Customer is responsible for (a) properly configuring the Covered Services, (b) using the controls available in connection with the Covered Services (including the security controls) to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (c) taking such steps as Hostinger considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

5. DATA SUBJECT RIGHTS

Taking into account the nature of the Covered Services, Hostinger offers Customer certain controls that Customer may elect to use to retrieve, correct, delete or restrict use and sharing of Customer Data as described in the Covered Services. Customer may use these controls as technical and organizational measures to assist it in connection with its obligations under Data Protection Laws, including its obligations relating to responding to requests from Data Subjects. As commercially reasonable, and to the extent lawfully required or permitted, Hostinger shall promptly notify Customer if Hostinger directly receives a request from a Data Subject to exercise such rights under any applicable Data Protection

Laws (“Data Subject Request”). In addition, where Customer’s use of the Covered Services limits its ability to address a Data Subject Request, Hostinger may, where legally permitted and appropriate and upon Customer’s specific request, provide commercially reasonable assistance in addressing the request, at Customer’s cost (if any).

6. SUB-PROCESSING

6.1 Authorized Sub-Processors. Customer agrees that Hostinger may use Sub-Processors to fulfil its contractual obligations under its Terms of Service and this Addendum or to provide certain services on its behalf, such as providing support services. Customer hereby consents to Hostinger’s use of Sub-Processors as described in this Section.

6.2 Sub-Processor Obligations. Where Hostinger uses any authorized sub-Processor as described in Section 6.1:

(i) Hostinger will restrict the sub-Processor’s access to Customer Data only to what is necessary to maintain the Covered Services or to provide the Covered Services to Customer and any end users in accordance with the Terms of Service. Hostinger will prohibit the sub-Processor from accessing Customer Data for any other purpose;

(ii) Hostinger will enter into a written agreement with the sub-Processor and, to the extent that the sub-Processor is performing the same data Processing services that are being provided by Hostinger under this Addendum, Hostinger will impose on the sub-Processor substantially similar contractual obligations that Hostinger has under this Addendum; and

(iii) Hostinger will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the sub-Processor that cause Hostinger to breach any of Hostinger’s obligations under this Addendum.

6.3 New Sub-Processors. From time to time, Hostinger may engage new Sub-Processors under and subject to the terms of this Addendum. New Sub-Processors will be added to the Appendix 3. If Customer does not approve of a new Sub-Processor, then Customer may terminate any Covered Services without penalty by providing, within 10 days or receipt of notice from Hostinger, written notice of termination that includes an explanation of the reasons for your non-approval. If the Covered Services are part of a bundle or bundled purchase, then any termination will apply to its entirety.

7. SECURITY INCIDENT

7.1 Security Incident. If Hostinger becomes aware of a Security Incident, Hostinger will without undue delay: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

7.2 Hostinger assistance. To assist Customer in relation to any Personal Data breach notifications Customer is required to make under Data Protection Laws, Hostinger will include in the notification such information about the Security Incident as Hostinger is reasonably able to disclose to Customer, taking into account the nature of the Covered Services, the information available to Hostinger, and any restrictions on disclosing the information, such as confidentiality.

7.3 Failed Security Incidents. Customer agrees that a failed Security Incident will not be subject to the terms of this Addendum. A failed Security Incident is one that results in no unauthorized access to Customer Data or to any of Hostinger's Network, equipment, or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful login attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

7.4 Notification. Notification of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Hostinger selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the Hostinger management console and secure transmission at all times.

7.5 No acknowledgement of fault by Hostinger: Hostinger's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Hostinger of any fault or liability of Hostinger with respect to the Security Incident.

8. CUSTOMER RIGHTS

8.1 Independent determination. Customer is responsible for reviewing the information made available by Hostinger relating to data security and its Security Standards and making an independent determination as to whether the Covered Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum. The information made available is intended to assist Customer in complying with Customer's obligations under applicable Data Protection Laws. Customer agrees that the Covered Services and the Security Standards implemented and maintained by Hostinger provide a level of security appropriate to the risk to Personal Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Personal Data as well as the risks to individuals).

8.2 Customer audit rights. Customer has the right to confirm Hostinger's compliance with this Addendum as applicable to the Covered Services by making a specific request in writing, at reasonable intervals, to the address set forth in the Terms of Service. If Hostinger declines to follow any instruction requested by Customer regarding a properly requested and scoped audit or inspection, Customer is entitled to terminate this Addendum and the Terms of Service.

9. TRANSFERS OF CUSTOMER DATA

9.1 Application of EU Standard Contractual Clauses. Module Two (Controller to Processor) EU Standard Contractual Clauses or Module Three (Processor to Processor) EU Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Customer Data. These EU Standard

Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, these EU Standard Contractual Clauses will not apply where the data is transferred in accordance with a recognized compliance standard for the lawful transfer of Personal Data outside the EEA, such as when necessary for the performance of Covered Services pursuant to the Terms of Service or with your consent.

1. For each Module, where applicable:
    1. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;
    2. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-Processor changes will be as set forth in Section 6.3 (New Sub-Processors) of this Addendum;
    3. in Clause 11 of the EU Standard Contractual Clauses, the optional language is English;
    4. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Cyprus law;
    5. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of the Cyprus;
    6. in Appendix I, Part A of the EU Standard Contractual Clauses:
        - List of Parties

          Data Exporter(s): The data exporter is the entity identified as "Customer" in the Addendum
          Signature and date: As of the date of Data Exporter's electronic acceptance of Data Importer's Terms of Service, Data Exporter is deemed to have signed these EU Standard Contractual Clauses.
          Role: Controller (under Module Two) or Processor (under Module Three)

          Data importer(s): Hostinger International Ltd.
          Contact details: gdpr@hostinger.com
          Signature and date: As of the date of Data Exporter's electronic acceptance of Data Importer's Terms of Service, Data Importer is deemed to have signed these EU Standard Contractual Clauses.
          Role: Processor
    7. in Appendix 1, Part B of the EU Standard Contractual Clauses:
        - Description of Transfer

          Categories of Data Subjects whose Personal Data is transferred are described in Appendix 1 of the Addendum.
          Categories of Personal Data transferred are described in Appendix 1 of the Addendum. Sensitive data transferred are described in Appendix 1 of this Addendum.
          The frequency of the transfer is a continuous basis for the duration of the Terms of Service.
          Nature of the Processing is described in Section 2.2 and Appendix 1

        of the Addendum.
        Purpose(s) of the data transfer and further Processing are described in Section 2.2 and Appendix 1 of this Addendum.
        The period for which the Personal Data will be retained described in Appendix 1 of this Addendum.
        For transfers to (sub-) Processors, the subject matter, nature and duration of the Processing is set forth in Appendix 3 to the Standard Contractual Clauses.

8. in Appendix 1, Part C of the EU Standard Contractual Clauses:
    - Competent Supervisory Authority
      Office of the Commissioner for Personal Data Protection (Cyprus) is the competent supervisory authority.
9. in Appendix 2 of the EU Standard Contractual Clauses:

   The technical and organizational security measures implemented by the Data Importer are as in Appendix 2 of the Addendum.
10. in Appendix 3 of the EU Standard Contractual Clauses:

    List of sub-Processors are in Appendix 3 of this Addendum.

9.3 Application of UK International Data Transfer Addendum. The UK International Data Transfer Addendum will apply to Customer Data transferred via Covered Services from the United Kingdom, either directly or via onward transfer, to any country not recognized by the competent United Kingdom regulatory authority or governmental body as providing an adequate level of protection for Customer Data. The UK International Data Transfer Addendum will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the United Kingdom. Notwithstanding the foregoing, the UK International Data Transfer Addendum will not apply where the data is transferred in accordance with a recognized compliance standard for the lawful transfer of Customer Data outside the United Kingdom, such as when necessary for the performance of Covered Services pursuant to the Terms of Service or with your consent.

1. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Addendum, the UK International Data Transfer Addendum will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:
    1. In Table 1 of the UK International Data Transfer Addendum, the parties' details and key contact information is located in Section 9.2 (i)(f) of this Addendum.
    2. In Table 2 of the UK International Data Transfer Addendum, information about the version of the EU Standard Contractual Clauses, modules and selected clauses which this UK International Data Transfer Addendum is appended to is located in Section 9.2 (EU Standard Contractual Clauses) of this Addendum.
    3. In Table 3 of the UK International Data Transfer Addendum:
        1. The list of Parties is located in Section 9.2 (i)(f) of this Addendum.

    2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Appendix 1 (Details of the Processing) of this Addendum.
    3. Appendix 2 is located in Appendix 2 (Security Standards) of this Addendum
    4. The list of sub-Processors is in Appendix 3 of this Addendum.
4. In Table 4 of the UK International Data Transfer Addendum, both the Importer and the Exporter may end the UK International Data Transfer Addendum in accordance with the terms of the UK International Data Transfer Addendum.

10. TERMINTION OF THE ADDENDUM

This Addendum will continue in force until the termination of our Processing in accordance with the Terms of Service (the “Termination Date”).

11. RETURN OR DELETION OF CUSTOMER DATA

As described in the Covered Services, the Customer may be provided controls that may use to retrieve or delete Customer Data. Deletion of Customer Data will take place thirty (30) days following Termination Date, subject to the terms of the particular Covered Services. Customer acknowledges that it is Customer’s responsibility to export, before the Termination Date, any Customer Data you want to retain after the Termination Date.

12. LIMITATIONS OF LIABILITY

The liability of each party under this Addendum will be subject to the exclusions and limitations of liability set out in the Terms of Service. Customer agrees that any regulatory penalties incurred by Hostinger in relation to the Customer Data that arise as a result of, or in connection with, Customer’s failure to comply with its obligations under this Addendum and any applicable Data Protection Laws will count towards and reduce Hostinger’s liability under the Terms of Service as if it were liability to the Customer under the Terms of Service.

13. ENTIRE TERMS OF SERVICE; CONFLICT

This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and Hostinger, whether written or verbal, regarding the subject matter of this Addendum, including any data Processing addenda entered into between Hostinger and Customer with regard to the Processing of Personal Data and on the free movement of such data. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Addendum and any other terms in this Addendum or the Terms of Service, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Addendum, as applicable, will prevail. Except as amended by this Addendum, the Terms of Service will remain in full force and effect. If there is a conflict between the Terms of Service and this Addendum, the terms of this Addendum will control.

APPENDIX 1

DETAILS OF THE PROCESSING

1. Nature and purpose of Processing. Hostinger will Process Customer Data as necessary to perform the Covered Services pursuant to the Terms of Service and as further instructed by Customer throughout its use of the Covered Services.

2. Duration of Processing. Subject to Section 10 and 11 of this Addendum, Hostinger will Process Customer Data during the effective date of the Terms of Service. Notwithstanding the foregoing, Hostinger may retain Customer Data, or any portion of it, if required by applicable laws or regulation, including applicable Data Protection Laws, provided that such Customer Data remains protected in accordance with the terms of this Addendum and applicable Data Protection Laws.

3. Categories of Data Subjects. Customer may upload Personal Data in the course of its use of the Covered Services, the extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Covered Services

4. Categories of Personal Data. Customer may upload Personal Data in the course of its use of the Covered Services, the type of and extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data of Data Subjects:

- Name
- Address
- Telephone number
- Date of birth
- Email address
- Other data collected that could directly or indirectly identify Data Subjects.

5. Sensitive Data or Special Categories of data. Customer may upload Sensitive Data in the course of its use of the Covered Services, the type of and extent to which is determined and controlled by Customer in its sole discretion. Customer is responsible for applying restrictions or safeguards that fully take into consideration the nature of the data and the risks involved prior to transmitting or Processing any Sensitive Data via the Covered Services.

APPENDIX 2

SECURITY STANDARDS

I. Technical and organizational measures

We are committed to protect our customers' information. Taking into account the best practices, the costs of implementation and the nature, scope, circumstances and purposes of Processing as well as the different likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons we take the following technical and organizational measures. When selecting the measures the confidentiality, integrity, availability and resilience of the systems are considered.

II. Data Privacy Program

Our Data Privacy Program is established to maintain a global data governance structure and secure information throughout its lifecycle. We regularly test, assess and evaluate the effectiveness of its Data Privacy Program and Security Standards.

1. Confidentiality. “Confidentiality means that Personal Data is protected against unauthorized disclosure.”

We use a variety of physical and logical measures to protect the confidentiality of its customers' Personal Data. Those measures include:

Physical security

- Physical access control systems in place (Badge access control, Security event monitoring etc.)
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Destruction of data on physical documents (shredding)

Access control & prevention of unauthorized access

- User access restrictions applied and role-based access permissions provided/reviewed based on segregation of duties principle
- Strong authentication and authorization methods
- Centralized password management and strong/complex password policies (minimum length, complexity of characters, expiration of passwords etc.)
- Controlled access to e-mails and the Internet
- Anti-virus management

Encryption

- Encryption of external and internal communication via strong cryptographic protocols
- Encrypting Personal Data and sensitive data at rest (databases, shared directories etc.)
- Full disk encryption for company PCs and laptops
- Remote connections to the company networks are encrypted via VPN

Data minimization

- PII/SPI minimization in application, debugging and security logs
- Pseudonymization of Personal Data to prevent directly identification of an individual
- Segregation of data stored by function (test, staging, live)

- Logical segregation of data by role based access rights
- Defined data retention periods for Personal Data

Security testing

- Penetration Testing for critical company networks and platforms hosting Personal Data
- Regular network and vulnerability scans

2. Integrity. “Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term "data", it expresses that the data is complete and unchanged.”

Appropriate change and log management controls are in place, in addition to access controls to be able to maintain the integrity of Personal Data such as:

Change & release management

- Change and release process including (impact analysis, approvals, testing, security reviews, staging, monitoring etc.)
- Role & Function based (Segregation of Duties) access provisioning on production environments

Logging & monitoring

- Logging of access and changes on data
- Centralized audit & security logs
- Monitoring of the completeness and correctness of the transfer of data (end-to-end check)

3. Availability. “The availability of services and IT systems, IT applications, and IT network functions or of information is guaranteed, if the users are able to use them at all times as intended.”

We implement appropriate continuity and security measures to maintain the availability of its services and the data residing within those services:

- Regular fail-over alerts applied for critical services
- Extensive performance/availability monitoring and reporting for critical systems
- Incident response programme
- Critical data either replicated or backed up (Cloud Backups/Hard Disks/Database replication etc.)
- Planned software, infrastructure and security maintenance in place (Software updates, security patches etc.)
- Use of uninterruptible power supplies, fail redundant hardware and network systems
- Alarm, security systems in place
- Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems, fire and/or smoke detectors, fire suppression systems etc.)
- DDOS protection to maintain availability

- Load & Stress Testing

4. Data Processing Instructions. "Data Processing Instructions refers to ensuring that Personal Data will only be processed in accordance with the instructions of the data Controller and the related company measures"

We have established internal privacy policies, agreements and conduct regular privacy trainings for employees to ensure Personal Data is processed in accordance with customers' preferences and instructions.

- Privacy and confidentiality terms in place within employee contracts
- Regular data privacy and security trainings for employees
- Appropriate contractual provisions to the agreements with sub-contractors to maintain instructional control rights
- Regular privacy checks for external service providers
- Providing customers full control over their data Processing preferences

APPENDIX 3

SUB-PROCESSORS

- AMAZON WEB SERVICES EMEA SARL
- Google Cloud EMEA Limited
- Cloudflare, Inc.
- MailChannels Corporation
- Proofpoint, Inc.
- Anthropic Ireland, Limited
- spectra tech, UAB

HOSTINGER

NPRD-Anfrage-Richtlinie   Datenschutzerklärung   Rückerstattungsrichtlinie

Allgemeine Geschäftsbedingungen   Impressum

VISA AMEX DISCOVER JCB Diners Club INTERNATIONAL und mehr

Preisangaben ohne Mehrwertsteuer