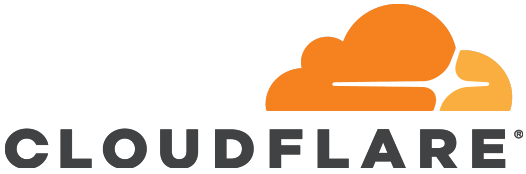

CLOUDFLARE DATA PROCESSING ADDENDUM

Cloudflare, Inc. ("**Cloudflare**") and the counterparty agreeing to these terms ("**Customer**") have entered into an Enterprise Subscription Agreement, Self-Serve Subscription Agreement or other written or electronic agreement for the Services provided by Cloudflare (the "**Main Agreement**"). This Data Processing Addendum**,** including the appendices (the **"DPA")**, forms part of the Main Agreement.

This DPA will be effective, and will replace and supersede any previously applicable terms relating to their subject matter (including any data processing amendment, agreement or addendum relating to the Services), from the date on which Customer clicked to accept or the parties otherwise agreed to this DPA ("**DPA Effective Date**").

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

DATA PROCESSING TERMS

This DPA applies where and only to the extent that Cloudflare processes Personal Data submitted by or for Customer to Cloudflare or collected and processed by or for Customer using the Service where such Personal Data is subject to Applicable Data Protection Laws (as defined below).

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by Applicable Data Protection Laws. Accordingly, Cloudflare agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to Cloudflare or collected and processed by or for Customer using the Service.

1. Definitions

1.1 The following definitions are used in this DPA:

a) "**Adequate Country**" means a country or territory that is recognized under EU and UK Data Protection Laws as providing adequate protection for Personal Data.

b) "**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists).

c) "**Applicable Data Protection Laws**" means all laws and regulations of the jurisdictions in which a Cloudflare Group company has a physical presence that are applicable to the processing of personal data under the Main Agreement, including EU and UK Data Protection Laws and CCPA.

d) "**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199, 2018).

e) "**Cloudflare Group**" means Cloudflare and any of its Affiliates.

f) "**Customer Group**" means Customer and any of its Affiliates established and/or doing business in the European Economic Area, Switzerland or the United Kingdom.

g) "**Data Processor**" means an entity which processes personal data on behalf of the controller and to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose personal data information for the purpose of providing the Services.

h) "**EU and UK Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom, applicable to the processing of Personal Data under the Main Agreement, including (where applicable) the GDPR, the Swiss Federal Act on Data Protection, and the UK Data Protection Act.

i) "**GDPR**" means the General Data Protection Regulation (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).

j) "**Personal Data**" means all data which is defined as '*personal data*' under EU and UK Data Protection Laws and all data defined as '*personal information*' under the CCPA and which Cloudflare, in its role as data processor, receives from Customer or otherwise accesses, stores or processes on behalf of Customer as part of Cloudflare's provision of the Service to Customer.

k) "**processing**", "**data controller**", "**data subject**", and "**supervisory authority**" shall have the meanings ascribed to them in EU and UK Data Protection Laws.

l) "**Services**" shall refer to all of the cloud-based solutions offered, marketed or sold by Cloudflare or its authorized partners that are designed to increase the performance, security and availability of Internet properties, applications and networks, along with any software, software development kits and application programming interfaces ("**APIs**") made available in connection with the foregoing.

m) "**SCCs**" mean the Standard Contractual Clauses, available here, which are the standard data protection clauses for the transfer of personal data to processors established in third countries as described in Art. 46 of the GDPR as from time to time varied, amended or substituted by the European Commission.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller or processor, and Cloudflare is a data processor or sub-processor, as applicable, and accordingly:

(a) Cloudflare agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;

(b) The parties acknowledge that the Customer discloses Personal Data to Cloudflare only for the performance of the Service as defined by the Main Agreement and that this constitutes a valid business purpose for the processing of such data.

2.4 If Customer is a data processor, Customer warrants to Cloudflare that Customer's instructions and actions with respect to the Personal Data, including its appointment of Cloudflare as another processor and, where applicable, concluding the SCCs, have been authorised by the relevant controller.

2.5 Where and to the extent that Cloudflare processes data which is defined as '*personal data'* under EU and UK Data Protection Laws as a data controller as set out in the Cloudflare Privacy Policy, Cloudflare will comply with applicable EU and UK Data Protection Laws in respect of that processing.

2.6 Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

3. Cloudflare obligations

3.1 With respect to all Personal Data it processes in its role as a data processor or sub-processor, Cloudflare warrants that it shall:

(a) only process Personal Data in order to provide the Service and act only in accordance with: (i) this DPA, (ii) the Customer's written instructions as represented by the Main Agreement and this DPA, and (iii) the requirements of Applicable Data Protection Laws;

(b) not sell, retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Service, including for a commercial purpose other than providing the Service. Cloudflare's performance of the Service may include disclosing Personal Data to sub-processors where this is relevant in accordance with Section 4 of this DPA.

(c) to the extent that the Personal Data is subject to EU and UK Data Protection laws, upon becoming aware, inform the Customer if, in Cloudflare's opinion, any instructions provided by the Customer under clause 3.1(a) infringe the GDPR;

(d) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Cloudflare may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service;

(e) take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(f) without undue delay after becoming aware, notify the Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Cloudflare, its sub-processors, or any other identified or unidentified third party (a "**Personal Data Breach**");

(g) promptly provide the Customer with reasonable cooperation and assistance in respect of a Personal Data Breach and all reasonable information in Cloudflare's possession concerning

such Personal Data Breach insofar as it affects the Customer, including the following to the extent then known:

(i) the possible cause and consequences for the Data Subjects of the Personal Data Breach;

(ii) the categories of Personal Data involved;

(iii) a summary of the possible consequences for the relevant data subjects;

(iv) a summary of the unauthorised recipients of the Personal Data; and

(v) the measures taken by Cloudflare to mitigate any damage;

(h) shall not make any public announcement about a Personal Data Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law;

(i) to the extent Cloudflare is able to verify that a data subject is associated with the Customer, Cloudflare shall promptly notify the Customer if it receives a request from a data subject to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "**Data Subject Request**"). Cloudflare shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees.

(j) to the extent Cloudflare is able, and in line with applicable law, shall provide reasonable assistance to Customer in responding to a data subject request to access, rectify, correct, or erase that individual's Personal Data in such case where the Customer does not have the ability to address a Data Subject Request without Cloudflare's assistance. The Customer is responsible for verifying that requestor is the data subject whose information is being sought. Cloudflare bears no responsibility for information provided in good faith to Customer in reliance on this subsection. Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance;

(k) other than to the extent required to comply with applicable law, following termination or expiry of the Main Agreement or completion of the Service, Cloudflare will delete all Personal Data (including copies thereof) processed pursuant to this DPA;

(l) taking into account the nature of processing and the information available to Cloudflare, Cloudflare shall provide such assistance to the Customer as the Customer reasonably requests in relation to Cloudflare's obligations under Applicable Data Protection Laws with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority under Applicable Data Protection Laws and/or communications to data subjects by the Customer in response to any Personal Data Breach; and

(iii) the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to the security of processing;

provided that the Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance.

4. Sub-processing

4.1 Cloudflare will only disclose Personal Data to sub-processors for the specific purposes of carrying out the Service on Cloudflare's behalf. Cloudflare does not sell or disclose Personal Data to third parties for commercial purposes.

4.2 The Customer grants a general authorization: (a) to Cloudflare to appoint other members of the Cloudflare Group as sub-processors, and (b) to Cloudflare and other members of the Cloudflare Group to appoint third party data center operators, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service.

4.3 Cloudflare will maintain a list of sub-processors on the Cloudflare.com website and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Cloudflare of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Cloudflare is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.3 in respect of the proposed use of the sub-processor. If Cloudflare requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between Cloudflare and the sub-processor within ninety (90) days from the Customer's notification of objections, the Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the applicable Order Form and/or Insertion Orders with at least thirty (30) days written notice, solely with respect to the service(s) to which the proposed new sub-processor's processing of Personal Data relates. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 4.3, the Customer will be deemed to have consented to the sub-processor and waived its right to object. Cloudflare may use a new or replacement sub-processor whilst the objection procedure in this clause 4.3 is in process.

4.4 Cloudflare will ensure that any sub-processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on Cloudflare in this DPA (the "**Relevant Terms**"). Cloudflare shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

5. Audit and records

5.1 Cloudflare shall, in accordance with Applicable Data Protection Laws, make available to the Customer such information in Cloudflare's possession or control as the Customer may reasonably request with a view to demonstrating Cloudflare's compliance with the obligations of data processors under Applicable Data Protection Law in relation to its processing of Personal Data.

5.2 The Customer may exercise its right of audit under Applicable Protection Laws in relation to Personal Data, through Cloudflare providing:

(a) an audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that Cloudflare's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; and

b) additional information in Cloudflare's possession or control to a data protection supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Cloudflare under this DPA.

6. Data transfers from the EEA, Switzerland, and the UK

6.1 In connection with the Service, the parties anticipate that Cloudflare may process outside of the European Economic Area ("**EEA**"), Switzerland, and the United Kingdom, certain Personal Data protected by EU and UK Data Protection Laws in respect of which the Customer or any member of the Customer Group may be a data controller or data processor, as applicable, under such EU and UK Data Protection Laws.

6.2 To the extent Cloudflare is a recipient of and processes Personal Data protected by EU and UK Data Protection Laws in a country that does not provide an adequate level of protection for Personal Data (within the meaning of the GDPR):

(a) Cloudflare agrees to abide by and process such Personal Data in accordance with the SCCs. Cloudflare will comply with the obligations of the 'data importer' in the SCCs and the Customer will comply with the obligations of the 'data exporter'. Customer (as 'data exporter') will be deemed to have entered into the SCCs with Cloudflare (as 'data importer').

(b) In addition, although Cloudflare does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as Cloudflare is self-certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, it shall continue to process such Personal Data in compliance with the Privacy Shield Principles, and Cloudflare agrees to notify the Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles.

(c) In the event Customer seeks to conduct any assessment of the adequacy of the SCCs, Cloudflare shall, to the extent it is able, provide reasonable assistance to the Customer for the purpose of any such assessment, provided Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance.

6.3 To the extent Cloudflare adopts an alternative data export mechanism (including any new version of or successor to the Privacy Shield adopted pursuant to applicable EU and UK Data Protection Laws) for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism.

6.4 The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA, Switzerland, or UK.

6.5 If, in the performance of this DPA, Cloudflare transfers any Personal Data to a sub-processor located outside of the EEA, Switzerland, or UK (without prejudice to obligations of the data exporter under the SCCs), Cloudflare shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) the requirement for Cloudflare to execute or procure that the sub-processor execute to the benefit of the Customer SCCs or

(b) the existence of any other specifically approved safeguard for data transfers (as recognised under EU and UK Data Protection Laws) and/or a European Commission finding of adequacy.

6.6 The following terms shall apply to the SCCs:

(a) The Customer may exercise its right of audit under the SCCs as set out in, and subject to the requirements of, clause 5.2 of this DPA; and

(b) Cloudflare may appoint sub-processors as set out in, and subject to the requirements of, clauses 4 and 6.5 of this DPA.

7. Third Party Data Access Requests

7.1 In Cloudflare's role as a data processor or sub-processor, as applicable, it may be subject to third party legal process requesting access to or disclosure of Personal Data that are inconsistent with Applicable Data Protection Laws. If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer in its role as data processor or sub-processor (as applicable) then, to the extent that Cloudflare is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will:

(a) immediately notify Customer of the request unless such notification is legally prohibited;

(b) inform the third party that it is a processor or sub-processor (as applicable) of the Personal Data and is not authorized to disclose the Personal Data without Customer's consent;

(c) instruct the third party to direct its data request to Customer; and

(d) pursue legal remedies prior to producing data to the extent necessary.

7.2 If Cloudflare provides access to or discloses Personal Data in response to third party legal process either with Customer authorization or due to a mandatory legal compulsion, then Cloudflare will only disclose such Personal Data to the extent it is legally required to do so and in accordance with applicable lawful process.

7.3 Clauses 7.1 and 7.2 shall not apply in the event that Cloudflare has a good-faith belief the government request is necessary due to an emergency involving the danger of death or serious physical injury to an individual. In such event, Cloudflare shall notify Customer of the data disclosure as soon as possible following the disclosure and provide Customer with full details of the same, unless such disclosure is legally prohibited.

8. General

8.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

8.2 Cloudflare's liability under or in connection with this DPA, including under the SCCs, is subject to the exclusions and limitations on liability contained in the Main Agreement.

8.3 This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

8.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts of San Francisco, California.

8.5 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable and the invalid or unenforceable provision will be deemed modified so that it is valid and enforceable to the maximum extent permitted by law. Without limiting the generality of the foregoing, Customer agrees that Section 8.2 (Limitation of Liability) will remain in effect notwithstanding the unenforceability of any provision of this DPA.

8.6 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

Annex 1

Details of the Personal Data and processing activities

(a) Personal data processed: in relation to visitors to and/or authorized users of the Customer's domains, networks, websites, application programming interfaces ("**APIs**"), or application, including the Cloudflare product Cloudflare for Teams as may be applicable, identification data, professional life data, personal life data, connection data, localization data (including IP addresses), and any other data Customer receives from such visitors or authorized users. Customer, its online visitors, authorized users, and/or other partners may also upload content to Customer's online properties which may include personal data and special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

(b) Duration of the processing: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable);

(c) Processing activity: Processing necessary to provide the Service to Customer, pursuant to the Main Agreement;

(d) Purpose(s) of the processing is/ are: necessary for the provision of the Service;

(e) Personal data may concern the following data subjects: Natural persons that (i) access or use the Customer's domains, networks, websites, application programming interfaces ("**APIs**"), and applications, or (ii) are authorized users of the Cloudflare product Cloudflare for Teams, such as our Customers' employees, agents, or contractors.

Annex 2

Security Measures

A. Data importer/Cloudflare has implemented and shall maintain a security program in accordance with industry standards.

B. More specifically, data importer/Cloudflare's security program shall include:

Access Control of Processing Areas

Data importer/Cloudflare implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/Cloudflare implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/Cloudflare and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/Cloudflare commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and

- control of files, controlled and documented destruction of data.

Availability Control

Data importer/Cloudflare implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/Cloudflare implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/Cloudflare implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within data importer/Cloudflare's organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for different Purposes

Data importer/Cloudflare implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/Cloudflare's data base separate which data is used for which purpose, i.e. by functionality and function;

- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/Cloudflare will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/Cloudflare shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer/Cloudflare shall implement suitable measures to monitor access restrictions to data importer/Cloudflare's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/Cloudflare and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.