**Data Processing Agreement**

**in accordance with Article 28 of General Data Protection Regulation (GDPR)**

between

- the client and controller – hereinafter referred to as the "**Client**" -

and

**ConfigCat Kft.**

Hungary, 1136 Budapest, Tátra utca 5/A 1. em. 2.

- the processor - hereinafter referred to as the "**Processor**" –

hereinafter each individually referred to as the "**Party**", jointly referred to as the "**Parties**"

## 1. Subject matter and duration of the Agreement

The Subject matter of this Agreement results from the

☒ Service/Performance Agreement
☐ Service Level Agreement (SLA)
☐ Software Maintenance Contract
☐ Partner Contract
☐ Project order/Contract

concluded by and between the Parties on (hereinafter referred to as "**Service Agreement**").

This Agreement is supplemental to, and forms an integral part of the Service Agreement. The duration of this Agreement corresponds to the duration of the Service Agreement.

The Service Agreement covers the service fee to be paid by the Client for the services performed by the Processor under this Agreement and also stipulates the payment conditions.

## 2. Specification of the data processing

(1) Nature and purpose of the intended data processing

Processor shall process personal data only to the necessary and reasonable term and extent for the provision of the services undertaken in the Service Agreement.

Unless otherwise agreed in this Agreement, the data processing shall be carried out exclusively in the member states of the European Union (EU) or the European Economic Area (EEA). Each and every transfer of data to a state which is not a member state of either the EU or the EEA requires the prior explicit consent of the Client and shall only occur if the specific conditions of Chapter V of the GDPR have been fulfilled. The adequate level of protection in the United States of America and other third countries is ensured by standard data protection clauses adopted by the European Commission in accordance with Article 46 Paragraph 2 Point c) of the GDPR.

(2) Type of Data

The subject matter of the personal data processing includes the following data types/categories (List/Description of the Data Categories)

i. Contact Data (email address and/or IP address) of the Client's customer/subscriber/employee, in respect of whom the Client makes use of the Processor's services

(3) Categories of Data Subjects

The Categories of Data Subjects comprise the Client's:

i. Customers
ii. Subscribers
iii. Employees

(4) Duration of the processing of personal Data

Processing by the Processor shall only take place for the duration of the Service Agreement.

**3. Technical and Organisational Measures**

(1) By signing this Agreement, the Client represents that the Processor has presented the appropriate technical and organisational measures to ensure the level of security appropriate to the risk in accordance with Article 32 of GDPR which the Client accepts (Appendix 1). The Client is entitled to make amendment proposals regarding these measures, and if necessary, such amendments shall be implemented by mutual agreement.

(2) The Processor represents that it has established the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 of GDPR together with the principles relating to processing personal data.

(3) The Technical and organizational measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

**4. Rights and obligation of the Processor**

(1) The Processor may only restrict the processing of and correct or erase the data that is being processed on behalf of the Client based on documented instructions of the Client.

(2) The Processor shall immediately forward the direct requests from the data subject concerning a rectification, erasure or restriction of processing to the Client. The Processor undertakes to provide full cooperation and assistance, as it may be reasonably possible, in order to assist the Client in responding to data subjects' requests for the exercising of their rights.

(3) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Processor without undue delay in accordance with the documented instructions of the Client.

(4) The Processor shall make available all information necessary for the Client to demonstrate compliance with the obligations laid down in Article 28 of GDPR and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client.

(5) The Processor shall assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

(6) At the choice of the Client, the Processor deletes or returns all the personal data to the Client after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data in accordance with Section 10 of this Agreement.

## 5. Quality assurance and other duties of the Processor

In addition to complying with the rules set out in this Agreement, the Processor shall comply with the statutory requirements referred to in Article 28 of GDPR; accordingly, the Processor ensures, in particular, compliance with the following requirements:

i. The Processor is not obliged to appoint a Data Protection Officer. The email address data.officer@configcat.com serves as the contact point on behalf of the Processor.
ii. The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Agreement. This also applies if the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements of any civil or criminal law, or administrative rule or regulation regarding the processing of personal data in connection with this Agreement.
iii. In case the Client is subject to an inspection by the supervisory authority, an administrative, civil or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Agreement, the Processor shall make every effort to support the Client.
iv. The Processor shall periodically monitor the internal processes and the technical and organizational measures to ensure that its activity related to this Agreement is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

## 6. Subprocessing

(1) Under this Agreement subprocessing means the services which relate directly to the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Processor shall not engage another processor ("**Subprocessor**") without the prior specific or general written consent of the Client. In the case of general written authorisation, the Processor shall inform the Client of any intended changes concerning the addition or replacement of Subprocessors, thereby giving the Client the opportunity to object to such changes by submitting an objection by email to [...] with subject line "Subprocessor Objection," along with the Client's name, company's name, name of the Subprocessor and grounds for objection (objective justifiable grounds).

(3) The Client accepts the Subprocessors listed on the website [https://configcat.com/policies/subprocessors] on the day of the conclusion of this Agreement. The Processor will make updates to the Subprocessor lists via this website. In accordance with GDPR, the Processor discloses the Subprocessors to the Client in advance of their first engagement and provides notification of any changes over time.

(4) Changing or adding to the existing Subprocessors is permissible when:

i. the Processor submits a request to the Client on the outsourcing of a service to a Subprocessor in writing or in text form; and
ii. the Client has not objected to the planned outsourcing in writing or in text form in 5 business days from the notice of the request; and
iii. the subprocessing is based on a contractual agreement in accordance with Article 28 Section (2)-(4) of GDPR.

(5) The transfer of personal data from the Client to the Subprocessor and the commencement of the data processing shall only be undertaken after the compliance with all requirements has been achieved.

(6) If the Subprocessor provides the agreed service outside the EU/EEA, the Processor shall ensure the compliance with EU data protection regulations by appropriate measures, e.g. through standard contractual clauses under Article 46 Paragraph 2 Point c) of the GDPR.

(7) During the time of the data processing, the Client may, at any time request in writing that the data processed shall not be transferred to any Subprocessor outside the EU/EEA. In case the Client so requests in writing, the processor undertakes to refrain from using its Subprocessors for data transfers outside the EU/EEA. In the event of such a request by the Client, the data processing may only take place in the EU/EEA. (opt-out)

(8) All provisions of this Agreement, the Service Agreement and every other agreement in the contract chain shall be communicated to and agreed with each and every additional Subprocessor.

**7. Supervisory rights of the Client**

(1) The Client has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to be ascertained of the Processor's compliance with this Agreement in its business operations by means of random checks, which are announced in reasonable time.

(2) The Processor shall ensure that the Client is able to verify compliance with the obligations of the Processor in accordance with Article 28 GDPR**.** The Processor undertakes to give the Client the necessary information upon request and, in particular, to demonstrate the execution of the technical and organizational measures.

(3) Meeting such requirements may be certified by auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor).

(4) The Processor may claim compensation for enabling Client inspections. The compensation includes the costs arising from being unable or restricted to work as well as the loss of profit, however shall not be less than €150/person-hour. Parties agree that offsetting is not possible with respect to claims arising from this Agreement.

**8. Communication in the case of breach**

The Processor shall assist the Client in complying with Articles 32 to 36 of the GDPR. These include:

i. Processor shall ensure an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
ii. Processor shall notify Client without undue delay, and, where feasible, not later than 72 hours upon Processor becoming aware of a breach related to the processing of the personal data, providing Client with sufficient information to allow Client to meet any obligations, to report or to inform data subjects of the violation of the provisions of this Agreement or any data protection laws.
iii. Processor shall assist the Client to fulfill its obligation to provide information to the affected data subject and immediately assist and provide the Client with all relevant information in order to investigate and remedy such breach.
iv. Processor shall support the Client with its data protection impact assessment.
v. Processor shall support the Client based on the prior consultation with the supervisory authority.

**9. Right of the Client to issue instructions**

(1) The Processor processes the personal data based on documented instructions from the Client, including with regard to transfer of personal data to a third country or an international organization, unless required to do so by Union or Member State law which the Processor is subject to; in such a case, the Processor shall

inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Processor shall inform the Client immediately if they consider that an instruction violates any data protection laws and regulations, especially the provisions of the GDPR or other Union or Member State data protection provisions. In such cases, the Processor shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them. Processor's all costs, damages and loss of profit arising from maintaining such instruction shall be covered by the Client.

**10. Deletion and return of personal data**

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, but at the latest upon termination of this Agreement, the Processor shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to this Agreement that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on the request of the Data Subject.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Agreement and the data protection regulations shall be stored by the Processor beyond the duration of this Agreement or the Service Agreement in accordance with the respective retention periods. Processor may hand such documentation over to the Client upon the termination of this Agreement to relieve the Processor of this contractual obligation. In such cases, minutes shall be taken on the handover process.

**11. Liability and contractual penalty**

(1) Processor shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Client however, the contractual and non-contractual liability of the Processor is maximized and can not result in higher payment obligation than 3 months' amount of the service fee stipulated in the Service Agreement.

(2) In case more than one Processor is involved in the same processing and is responsible for any damage caused by the processing, each Processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(3) Processor shall be exempt from liability if it proves that the violation of the provisions of the Agreement or the data protection laws was caused by a circumstance that was outside of its control and was not foreseeable at the time of concluding this Agreement, and it could not be expected to have avoided that circumstance or averted the damage.

(4) Where the Subprocessor fails to fulfill its data protection obligations, the initial Processor shall remain fully liable to the Client for the performance of that Subprocessor's obligations.

(5) Processor expressly excludes all liability of any kind towards the Client, arising out of any hacker or cyber attack against the Processor's software.

(6) Processor reserves the right to postpone the date of performance of the services if they are prevented from, or delayed in, carrying on their business by acts, events, omissions or accidents beyond their reasonable control, failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, fire, flood, storm or default of Subprocessors by force majeure. In such cases, the Client is not entitled to claim any compensation for the damage arising from the postponement of the performance of the services.

**12. Confidentiality**

(1) Any information, circumstance, data, solution, specification, business plan, financial data, drawing, design and other information that they received about this agreement, the transaction included in this agreement, the other Party or the economic activity of the other Party in connection with this agreement (hereinafter together referred to as "**Confidential Information**") is qualified as confidential information ("üzleti titok") in the meaning of *Act No LIV of 2018 on the protection of business secrets*. The Parties shall neither abuse, nor use for purposes not related to this agreement, nor disclose to third parties, nor publish the Confidential Information without the prior written consent of the other Party. However, the Parties are entitled to disclose the Confidential Information only to the necessary degree to their employees and advisors, who need to have access to and knowledge of the Confidential Information in connection with conclusion and performance of the present Agreement.

(2) The provision of this agreement referred in this Section shall not apply to Confidential Information which:

a) is in or enters the public domain other than as a result of a breach of an obligation under this Agreement; or
b) is or has been acquired from a third party who owes no obligation of confidence in respect of the information; or
c) is or has been independently developed by the other Party or was known to it prior to receipt; or
d) disclosure is required by law.

Processor shall include the same confidentiality obligations as set out in this Section and the applicable laws in the agreement concluded with the Subprocessor.

Parties shall make every effort to prevent the consequences of the breach of confidentiality also in case when such breach is not attributable to the particular Party.

The obligations set out in this Section shall prevail subsequent to the expiry of this Agreement as well.

**13. Notices**

(1) The Processor shall notify the Client on to the planned termination of its services at its earliest convenience.

(2) Any notice should be delivered by hand or sent by prepaid registered mail with return receipt to the address set out in the heading of this Agreement and via e-mail to the following addresses:

- Client:
- Processor: data.officer@configcat.com

Without prejudice to the foregoing, any notice shall conclusively be deemed to have been received (i) on the date confirmed on the return receipt or on the date confirmed by the post in any other proper manner, if sent by post; or (ii) at the time of delivery, if delivered by hand. Regarding the delivery presumption the provisions of the Act CXXX of 2016 on Civil Procedural Rules shall apply.

(3) The Parties shall notify the other party of any change of the above mentioned correspondence addresses. In the absence of such notification any notice shall be deemed as delivered, if there have been any changes of address, even if those were sent to the above addresses or fax numbers.

(4) Besides the above, the Parties shall inform each other about all notices in e-mail as well. The non-performance of the delivery via e-mail shall not affect the delivery's effect regulated above.

**14. Miscellaneous**

(1) This Agreement shall enter into force on the day of its execution by both Parties.

(2) The Parties shall, and shall use their best efforts to procure that any necessary third party shall, from time to time execute such documents and perform such acts and actions as the Parties may require to give full effect and benefit of this Agreement, including but not limited to exercising any right and performing any obligations under this Agreement.

(3) The Parties shall mutually inform each other concerning the merits of this Agreement.

(4) This Agreement may only be amended or modified in writing with the mutual agreement of the Parties. This shall be applicable for the modification of this particular clause as well.

(5) In case any provisions of this Agreement or its parts hereof are void or unfeasible, this invalidity or infeasibility shall not have an effect on the whole Agreement. The provisions not affected by the invalidity shall have full effect, and be enforceable. The Parties shall substitute the invalid or unfeasible provisions with such provisions that are mostly comparable to them and is the closest to the aim of the invalid or unfeasible provision and the contractual will of the Parties and meets the requirements of GDPR.

(6) In the event of contradictions between this Agreement and other agreements between the Parties, in particular the Service Agreement, the provisions of this Agreement shall prevail.

(7) For the settlement of any dispute arising in connection with this Agreement, including any disputes on the interpretation, validity of the Agreement, the Parties attempt to settle the negotiation out of court. In the event that out of court negotiations do not succeed, the Parties stipulate exclusive jurisdiction of the courts of Hungary.

(8) This Agreement is governed by Hungarian law. The provisions of the GDPR and the Act V of 2013 on the Civil Code shall appropriately apply to issues not covered by this agreement.

(9) The terms used in this Agreement shall be interpreted in accordance with the GDPR.

Appendixes:

Appendix 1: Technical and Organisational Measures

The duly authorized representatives of the Parties have signed this Agreement, after reading and interpretation, as it is in full harmony with their contractual will.

| | |
|---|---|
| _____ | _____ |
| **Client** | **Processor** |

**Appendix 1- Technical and Organisational Measures**

**The Processor enters all technical and organizational measures here.**

**Physical Access Control**

Development site:

- Access to data processing equipment and systems is only possible via user authentication using a password or through a Single-Sign-On (SSO) solution.
- Security locks

Linode's servers and data centers:

- Access to the data center floor is restricted to data center employees and authorized visitors.
- Data Centers are staffed 24/7/365 with security guards and technicians.
- All employees and visitors are identified using biometrics and state issued Ids before entering the facility.

**Data Medium Control**

- The hard drives of computers are encrypted.

**Storage Control**

- Access to data processing equipment and systems is only possible via user authentication using a password or through a SSO solution.

**Internal Access Control**

- Not applicable

**Electronic Access Control**

- Access to data processing equipment and systems is only possible via user authentication using a password or through a SSO solution.
- Tool-assisted password management is utilized in all areas.
- All in-house applications that are accessible through a browser over the Internet have TLS protected connections.
- Protection against unauthorized access via the use of virus protection and firewall
- SSO is offered for ConfigCat customers.
- 2 factor authentication is offered for ConfigCat customers.

**Data Transfer Control**

- Data is only transferred over an encrypted connection.

**Data Entry Control**

- Access to the system and data changes at the user level are logged.

**Transport Control**

- There is no transport of physical data storage media containing unencrypted third-party data within ConfigCat.
- Data storage media in computers are encrypted and secured with a password.

**Rapid Recovery Control**

- Backup and recovery concept.
- Backup operation control.

**Reliability**

- Automatic notification in case of system failure.

Linode’s servers and data centers:

- HVAC and power have redundant systems, so if one goes out, the others keep our systems powered and within operating temperature.
- All of Linode's systems are segregated from other tenants by locking cabinets. Only datacenter staff assigned to supporting Linode systems have access to the keys.
- Multiple Internet carriers using independent fiber connections to the data center floor.
- Our networks within the data centers have redundant routers, switches, and service providers. Multiple systems can fail without affecting downtime or performance.

**Data Integrity**

- Backup and recovery concept.
- Backup operation control.
- Monitoring of production systems.

**Order Control**

- Carefully selected service providers.

**Availability Control**

Linode’s servers and data centers:

- HVAC and power have redundant systems, so if one goes out, the others keep our systems powered and within operating temperature.
- All of Linode's systems are segregated from other tenants by locking cabinets. Only datacenter staff assigned to supporting Linode systems have access to the keys.
- Multiple Internet carriers using independent fiber connections to the data center floor.
- Our networks within the data centers have redundant routers, switches, and service providers. Multiple systems can fail without affecting downtime or performance.

**Isolation Control**

- Test, development, and production systems are technically separated from each other.
- Feature flag evaluation is executed on the client side not sent to ConfigCat’s servers.