# Data Processing Agreement (GDPR compliant)

***1. Scope and subject matter of the agreement***

This Data Processing (“DPA”) reflects the parties’ agreement with respect to the terms governing the processing of Personal Data under IBANCOM’s Terms of Service (the “TOS”). This DPA is an amendment to the TOS and is effective upon its incorporation into the TOS, which incorporation may be specified in an Order or an executed amendment to the TOS. Upon its incorporation into the TOS, the DPA will form a part of the TOS.

***2. Definitions***

In this agreement:

(a) « Services » means the services provided to the Customer under the TOS ;
(b) « Personal data » means any information relating to an identified or identifiable natural person (‘data subject’);
(c) « Customer », « controller » or « you » means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
(d) « Processor », « IBANCOM » or « we » means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
(e) « Process/processing » means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction ;
(f) « Sub-processor » or « Sub-contractor » means a third party subcontractor engaged by the processor which, as part of the subcontractor’s role of delivering the Services, Processes Personal Data of the Customer ;
(g) « Technical and organizational security measures » means those measures aimed to ensure a level of security appropriate to the risk including inter alias the pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
(h) “Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their Member states, applicable to the Processing of Personal Data under the Agreement.

### *3. Application of this agreement*

This agreement shall apply to:
a) all Data sent from the date of this agreement by the Customer to IBANCOM for Processing;
b) all Data accessed by the IBANCOM on the authority of the Customer for Processing from the date of this agreement; and
c) all Data otherwise received by IBANCOM for Processing on the Customer's behalf;
in relation to the Services.

### *4. Categories of Personal Data and purpose of the Personal Data Processing*

In order to execute the Agreement, and in particular to perform the Services on behalf of Customer, Customer authorizes and requests that IBANCOM Process the following Personal Data: Customer Information : information that we may collect from your use of the IBANCOM web sites and your interactions with us offline such as :

• Contact information : name, home address, telephone or mobile number, email address, and passwords.
• Financial information : credit card's number and billing information (tax id, number of the payer VAT, billing address, billing email, where invoices are sent) ; Credit card number are handled by 2checkout (our payment gateway), by Paypal, or other types of payement ; IBANCOM only charges your credit card for payments.
• Employment contact details, including : employer name, job title and function, business contact details;

Services Data : data which resides on IBANCOM, customer or third-party systems to which IBANCOM has provided access to perform services.

• Data stored and processed by users, such as: data sent for processing, the history of operations performed by users.
• Log File Information: Three types of logs are saved by IBANCOM's system : Connection logs which are essentially logs from each request to each application. These connection logs may include information such as the web request, Internet Protocol ("IP") address, browser type, referring / exit pages and URLs, number of clicks, domain names, landing pages, pages viewed and other such information. The second type of logs are application logs, which are produced by our software during data processing. Application logs logs are a record of all input data sent for processing to our servers that can help IBANCOM to identify and diagnose the source of current system problems and help predict future problems.
IBANCOM processes Customer information according to the terms of its Privacy policy, and treats services data as confidential in accordance with the terms of your order for services

Categories of Data Subjects: Data subjects include Customer's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, and customers of the Customer. Data subjects also may include individuals attempting to communicate or transfer Personal Data to users of the Services.

### *5. Responsibility of IBANCOM*

IBANCOM shall Process Personal Data solely for the provision of the Services, and agrees to :

• (a) Process and use Personal Data for the purposes set forth in this Agreement or only on documented instructions from the Customer and for no other purpose except with the express prior

written consent of the Customer, or
• (b) Not divulge Data to third parties except to those of its employees, agents and subcontractors who are engaged in the Processing of the Data and are subject to the binding obligations or except as may be required by any law or regulation;
• (c) Implement appropriate technical and organizational measures to safeguard the Data from unauthorized or unlawful Processing or accidental loss, destruction or damage, and that having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and to the nature of the Data to be protected;
• (d) Inform the Customer as soon as possible in the event of the exercise by Data Subjects of any of their rights under the data protection laws in relation to the Data, and, if necessary, assists the Customer in complying with the obligation to respond to those requests in consideration of the undertakings provided in article 7 ;
• (e) Not Process or transfer the Data outside of the European Union except with the express prior written authority of the Customer and ensure that such transfers are made in compliance with appropriate EU laws.
• (f) IBANCOM shall support the Customer with its data protection impact assessment and with regard to prior consultation of the supervisory authority in accordance to Article 35 and 36 of the GDPR..

### *6. Responsibility of the Customer*

The Service Customer, as Data controller, must accept responsibility for abiding by the applicable data protection legislation. Notably, the Customer has an obligation to assess the lawfulness of the processing of personal data stored on the Platform.

The Customer agrees that it shall ensure compliance at all times with the applicable data protection law, and, in particular, the Customer shall ensure that any disclosure of Personal Data made by it to IBANCOM is made with the data subject's consent or is otherwise lawful. The control of Personal Data remains with the Customer, and as between the Customer and IBANCOM, the Customer will at all times remain the Data controller for the purposes of the Services, the TOS, and this Data Processing Agreement. The Customer is responsible for compliance with its obligations as Data controller under the applicable data protection Law, in particular for justification of any transmission of Personal Data to IBANCOM (including providing any required notices and obtaining any required consents), and for its decisions concerning the Processing and use of the data.

### *7. Rights of Data Subject*

IBANCOM will grant Customer electronic access to the Platform environment that holds Personal Data to permit Customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer’s detailed written instructions to delete, release, correct or block access to Personal Data.

IBANCOM shall pass on to the Customer any requests of an individual data subject to delete, release, correct or block Personal Data Processed under the Agreement.

### *8. Cross Border and Onward Data Transfer*

IBANCOM treats all Personal Data in a manner consistent with the requirements of the applicable data protection Law and this Data Processing Agreement in all locations globally.

Data is stored by IBANCOM in data centers located in Germany managed by its subcontractor Google Cloud ( Germany ).

Data centers are located in:
Google Cloud
FRANKFURT, Germany

Google Cloud is GDPR compliant.
https://cloud.google.com/security/gdpr

With respect to Personal Data stored by IBANCOM in data centers in the EEA shall ensure compliance its Subprocessors with the requirements of the applicable data protection law as follows:
• (i) IBANCOM has entered into contracts with Subprocessors which provide that the Subprocessor will undertake data protection and confidentiality obligations consistent with applicable data protection laws;
• (ii) further, where a Subprocessor processes Personal Data in or from a country that has not received an “adequacy” finding, IBANCOM will require the Subprocessor to execute Model Clauses incorporating security requirements consistent with those of this DPA.

***9. Subprocessing***

IBANCOM shall not subcontract any of its processing operations performed on behalf of the Customer under the Agreement and the TOS without the prior written consent of the Customer.

Where IBANCOM subcontracts its obligations under the Agreement, with the consent of the Customer, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on IBANCOM under the Agreement. Where the subprocessor fails to fulfill its data protection obligations under such written agreement IBANCOM shall remain fully liable to the Customer for the performance of the subprocessor’s obligations under such agreement.

The Customer as Data controller may request that IBANCOM audit the Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Data Controller in obtaining a third-party audit report concerning Subprocessor’s operations) to ensure compliance with such obligations. The Controller also will be entitled, upon written request, to receive copies of the relevant terms of IBANCOM’s agreement with Subprocessors that may process Personal Data, unless the agreement contains confidential information, in which case the IBANCOM may provide a redacted version of the agreement.

The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Customer is established.

List of Subprocessors:

| **Company** | **Role** | **Location** |
|---|---|---|
| | | |
| Google Cloud | Data Center | Frankfurt, Germany |

### *10. Technical and Organizational Measures*

When Processing Personal Data on behalf of Customer in connection with the Services, IBANCOM shall ensure that it implements and maintains compliance with appropriate technical and organizational security measures for the Processing of such data. Accordingly, IBANCOM will implement the following measures:

• a) To prevent unauthorized persons from gaining access to data processing systems in which Personal Data are Processed (physical access control), IBANCOM shall take measures to prevent physical access, such as security personnel and secured buildings and factory premises.
• b) To prevent data processing systems from being used without authorization (system access control), the following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and logging of access on several levels.
For API Services hosted at the IBANCOM: (i) logical access to the data centers is restricted and protected by firewall/VLAN; and (ii) the following security processes are applied: centralized logging and alerting, and (iii) firewalls.
• c) To ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing and/or after storage (data access control), Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced.

In addition to the access control rules set forth above, IBANCOM implements an access policy under which Data Controller controls access to its API Services environment and to Personal Data and other data by its authorized personnel.

• d) To ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control), IBANCOM will comply with the following requirements: Except as otherwise specified for the API Services, transfers of data outside the Service environment are encrypted (HTTPS). The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted once received through such services. Data Controller is solely responsible for the results of its decision to use non-encrypted communications or transmissions.
• e) To ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed (input control), IBANCOM will comply with the following requirements: Personal Data source is under the control of the Customer, and Personal Data integration into the system is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer.
• f) To ensure that Personal Data is protected against accidental destruction or loss: back- ups are taken on a regular basis; back-ups are encrypted and are secured.
• g) To ensure that Personal Data which is collected for different purposes may be Processed separately, data from different Data Controllers' environments is logically segregated on IBANCOM's systems.
h) To provide the option to disable logging of input data sent to the service. This feature is available in our Client Area -> Account -> Settings -> Security and Privacy section and is labeled "Query Logging". When disabled, IBANCOM servers will not store the input information sent to our API and web applications by the Customer.

### *11. Audit Rights*

The Customer may audit IBANCOM's compliance with the terms of the Agreement and this Data Processing Agreement up to once per year.

The Customer may perform more frequent audits of the Service computer systems that Process Personal Data to the extent required by laws applicable to the Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by both parties and must execute a written confidentiality agreement acceptable to IBANCOM before conducting the audit.

To request an audit, the Customer must submit a detailed audit plan at least 4 weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. IBANCOM will review the audit plan and provide Data Controller with any concerns or questions (for example, any request for information that could compromise IBANCOM's security, privacy, or employment policies).

The audit reports are Confidential Information of the parties under the terms of the Agreement. Any audits are at the Data Controller's expense.

Any request for IBANCOM to provide assistance with an audit is considered a separate service if such audit assistance requires the use of different or additional resources. IBANCOM will seek the Data Controller's written approval and agreement to pay any related fees before performing such audit assistance.

### *12. Incident Management and Breach Notification*

IBANCOM evaluates and responds to incidents that create suspicion of unauthorized access to or handling of Personal Data.

The Customer is informed of such incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those incidents. IBANCOM will work with the Customer, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of the Services environment, and to establish root causes and remediation steps.

IBANCOM operations staff is instructed on responding to incidents where handling of personal data may have been unauthorized.

IBANCOM shall notify the Customer without undue delay after becoming aware of a personal data breach. IBANCOM shall promptly investigate any security breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by law, IBANCOM will provide Data Controller with a description of the security breach, the type of data that was the subject of the breach, and other information Data Controller may reasonably request concerning the affected persons. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected persons.

### *13. Legally Required Disclosures*

Except as otherwise required by law, IBANCOM will promptly notify the Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("demand") that it receives and which relates to the Personal Data IBANCOM

is Processing on Customer's behalf. At Customer's request, IBANCOM will provide reasonable information in its possession that may be responsive to the demand and any assistance reasonably required for the Customer to respond to the demand in a timely manner. The Customer acknowledges that IBANCOM has no responsibility to interact directly with the entity making the demand.

***14. Obligation after the termination of personal data processing services***

The parties agree that on the termination of the provision of data processing services, IBANCOM will make available for retrieval or otherwise will return Customer's Personal Data stored in the Platform environment, unless legislation imposed upon the parties prevents it from returning or destroying all or part of the personal data transferred. In that case, the parties warrant that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

**15. Data Protection Officer**

All questions and queries regarding data processing and data protection should be addressed to the data protection officer.

Name: Kostadin Markov
Email: k.markov@iban.com

***16. Governing law***

This agreement will be governed by the laws Republic of Bulgaria.

| | |
|---|---|
| GW Solutions LTD.<br><br>Signature:<br><br>Name:<br><br>Title:<br><br>Date: | <br><br>Signature:<br><br>Name:<br><br>Title:<br><br>Date: |