VCC Live
Contact Center Software

Data Processing Agreement

Entered into by and between

VCC Live Germany GmbH	
Registered seat	Gontardstraße 11, 10178 Berlin
Company register number	HRB 190017 B
VAT ID	DE277993151
Authorized representative	Szabolcs Tóth managing director or Péter Málhai authorised representative
Data Protection Officer	dr. Rita Seres

as data processor – hereinafter **Data Processor** or **Service Provider** or **VCC Live**

and

XY Company Name	
Registered seat	
Company register number	
VAT ID	
Authorized representative	
Data Protection Officer	
Account name	

as data controller – hereinafter **Data Controller** or **Subscriber** – on the place and date below, with the following content:

Preamble

1. Parties agree that Data Controller – as Subscriber – and VCC Live – as Service Provider – have entered into a Subscription Contract (hereinafter: "**Subscription Contact**") effective as of DATE.
2. Performance of the Subscription Contract requires that the Data Processor processes personal data provided by the Data Controller (hereinafter: "**Personal Data**").
3. Data Controller and Data Processor enter into this Data Processing Agreement (hereinafter: "**Data Processing Agreement**") to cause Data Processor's data controlling activities associated with the services under this Data Processing Agreement to comply with the pertinent legislation, especially the requirements of 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 (hereinafter: **GDPR**).
4. Based on the above, in compliance with Article 28 of the GDPR, Parties lay down the basic rules of Data Processor's data processing activities under the commission of the Data Controller in this Agreement.
5. Data controlling activities carried out by the Data Processor on behalf of the Data Controller shall be detailed in Annex 1 of this Agreement.

1. Processing of Personal Data

1. Data Processor shall process Personal Data exclusively as per the written instructions of the Data Controller – including transmission of Personal Data to any third country or international organization –, except where the Data Processor is mandated by EU or national legislation to process such data. In such cases, Data Processor shall inform the Data Controller of such statutory requirements prior to processing of such data, except where notification of the Data Controller is prohibited by the given legislation to protect important public interests.
2. Data Processor is not entitled to make substantive decisions with regards to data controlling and may not process or control data for its own purposes**.**

2. Employees of the Data Processor

1. Data Processor shall ensure that individuals authorized to process Personal Data commit to a confidentiality obligation or are under an adequate confidentiality obligation required by law.
2. Data Processor shall always ensure that personal data handled by the Data Controller are accessed by employees or other individuals only, whose access is essential to perform the Subscription Contract. Such persons shall commit to a confidentiality obligation or shall be under and adequate confidentiality obligation required by law.

3. Security of Personal Data

1. Considering the results of technical development, best practices currently applied in technological development, the costs of execution and the nature, volume, linkages and purpose of processing of Personal Data, risks affecting the rights and freedoms of data subjects, especially risks resulting from breach of security of Personal Data, the Data Processor shall take the appropriate technical and organizational measures to protect Personal Data against inadvertent or unlawful destruction, inadvertent loss (including deletion), alteration, unauthorized disclosure, use or access, or any form of unlawful processing.
2. Technical security measures taken by the Data Processor shall be described in Annex 2 of this Data Processing Agreement.
3. Data Controller shall be entitled to request evidencing of such technical and organizational measures from the Data Processor. In addition to the presented documentation, Data Processor may use its accession to approved codes of conduct or certification methods to evidence the above.
4. Considering the nature of data controlling, data processor shall support the data controller to the most extent possible in fulfilling of its obligations in terms of responding to requests of data subjects to exercise their rights under Chapter III of the GDPR by implementing technical and organizational measures.
5. Data Processor shall support the Data Controller in fulfilling its obligations under Articles 32-36 of the GDPR (security of data controlling, reporting of breach of personal data to the supervisory authority, information of data subjects about personal data breaches, data protection impact assessment, prior consultation), considering the nature of data controlling and the information available to the Data Processor.

4. Appointment of further data processors

1. By this Data Processing Agreement, Data Controller gives a general authorization to the Data Processor to the replacement of data processors instructed prior to the effective date of this Data Processing Agreement or to instruct further data processors. Data Processor shall inform the Data Controller about any planned changes affecting the instruction of further data processors or their replacement at least 30 (thirty) days in advance, allowing the Data Controller to object against such changes.
2. If Data Processor uses the services of further data processors to perform the exact data controlling activities on behalf of the data controller, Data Processor shall impose the same data protection obligations on such further data processors as the obligations under this Agreement or other legal actions by entering into an agreement or any other legal action regulated by EU law, especially, such further data processors shall guarantee implementation of adequate technical and organizational measures and ensure that data controlling is compliant with the requirements of GDPR. If such further data processor fails to meet its data protection obligations, the Data Processor instructing it shall be fully liable for the fulfillment of the further data processor's obligation towards the Data Controller.

5. Data Processor's Further Obligations towards the Data Controller

1. If Data Processor receives a request from any data subject to exercise their right(s) under the GDPR, Data Processor shall inform the data subject about having to direct such requests directly to the Data Controller. At the same time, Data Processor shall inform the Data Controller about such requests.
2. Data Processor agrees that based on subsection (2) of Article 30 of the GDPR, it shall maintain records of any and all categories of data processing (data controlling) activities carried out on behalf of the Data Controller. Such records shall contain the following information:
   a) Name and contact details of the Data Processor;
   b) name and contact details of all Data Controllers the Data Processor acts on behalf of, and – if applicable – name and contact details of the representative of the Data Controller or the Data Protection Officer;
   c) Categories of data processing (data controlling) activities carried out on behalf of the individual Data Controllers;
   d) If Personal Data are transmitted to third countries or international organizations, description of appropriate guarantees;
   e) General description of technical and organizational measures provided by the Data Processor.

6. Personal Data Breach

1. Data Processor shall report any personal data breach to the Data Controller immediately after such breach became known to it, but within 48 hours the latest.
2. As a minimum, the above report shall contain:
   a) nature of the personal data breach, including – if possible – categories and estimated number of data subjects, and categories and estimated number of data affected by the personal data breach;
   b) name and contact details of the Data Protection Officer or other point of contact;
   c) likely consequences resulting from the personal data breach; and
   d) all measures taken and planned to remedy the personal data breach, including measures aiming to mitigate the adverse effects resulting from such personal data breach.

7. Deletion or Returning of Personal Data

1. Upon termination of the Subscription Contract due to any reason, Data Processor shall delete any and all data uploaded, recorded or generated by the Data Controller during the use of VCC Live services (e.g. settings, client data, sound files, statistics), as per the requirements of subsection (8) and (9) of Section 3.3. of VCC Live GTA.

8. Audit Rights

1. Upon the request of Data Controller, Data Processor shall release all information that is necessary to evidence compliance with this Data Processing Agreement.
2. Data Processor shall allow and support Data Controller in performing audits conducted by the Data Controller or an auditor instructed by the Data Controller for the inspection of processing of personal data by the Data Processor, at the costs of the Data Controller.
3. During the inspection process, the Data Processor shall grant the Data Controller or the auditor rights to access the data processor's regulations/documentation to familiarize with the processes and measures taken by the data processor and to collect information and evidences. If essential to conduct a successful audit, Data Controller or an auditor instructed by it may copy the relevant part of the documentation only. Data Processor shall reserve the right to deny preparation of such copies, if the information within the document represent severe risks (for example, documents classified as strictly confidential) with regards to the secure provision of the services. Making full copies of policies or documents is not allowed.
4. Data Controller shall notify the Data Processor in advance - at least 10 days in advance - about the expected date and time of the audit.

5. The Data Controller and the auditor instructed by it may not cause any damages or disturbance in the facilities, equipment, employees or business activities of the Data Processor. If Data Controller causes any damages during the inspection process, it shall be fully liable for the damages caused by it.
6. During the audit process, Data Controller shall consider Data Processor's certifications as high-level evidences.
7. Data Controller and any external/internal auditors instructed by it shall assume confidentiality obligations with regards to any and all information disclosed to them during the audit process.

9. Liability and Damages

1. If either of the Parties breaches this Agreement willfully or of gross negligence**,** the Party in breach shall fully compensate the other Party for the damages incurred to it.
2. Data Processor shall only be liable for damages caused by the data controlling if it failed to fulfill the obligations under the GDPR expressly pertaining to data processors, or if willfully or negligently failed to obey the instructions of the Data Controller.
3. If this Agreement is breached, Data Processor shall hold the Data Controller harmless of any final liability for damages, final fines or penalties. In case of negligent (not gross negligent or willful) breach, damages claimable by the Data Controller towards the Data Processor may not exceed the following:
   a) for an indefinite term Subscription Contract, the extent of 3 months' license fee
   b) for a definite term Subscription Contract, the extent of 1 year's license fee
4. Data Processor shall be free from liability for damages if evidences that it acted with due diligence to prevent such damages.

10. Closing Provisions

1. If there is a discrepancy between this Agreement and the Subscription Contract between Parties, the provisions of the Individual Subscription Contract shall prevail.
2. This Agreement shall be effective upon execution and shall be valid until termination of the Subscription Contract.
3. This Agreement shall be governed by German law and the law of the European Union. Hungarian courts shall have exclusive competency with regards to any disputes arising in connection with this Agreement.

Annexes

Annex 1: Data handled by the Data Processor on behalf of the Data Controller

Annex 2: Technical Security Measures

Date: Berlin, 01. January 2020

VCC Live Germany GmbH – Data Processor

XYZ Company GmbH – Data Controller

Annex 1: Data handled by the Data Processor on behalf of the Data Controller

a) name of the Data Controller (company name):

b) DPO of the Data Controller (name and contact information):

c) subject of data controlling:
Here you need to describe the specific data processing operations. For example: storing of uploaded, recorded or generated data, data during the use of the Service (eg. settings, client data, CDRs, statistics) as well as files (eg. audio files, email messages)

d) term of data controlling:
It depends on the data involved. Eg. 30 days after the termination of the subscription contract or compulsory storage stated in statutory regulation.

e) nature of data controlling:
This can be a technical feature (machine or manual), but it may also be occasional or regular.

f) purpose of data controlling:
You should enter here the purpose of the data processing operations that VCC performs on behalf of the data controller. For example, fulfillment of a statutory obligation (with reference to the relevant regulation).

g) type of Personal Data:
(e.g. name, email address, telephone number, VAT ID, etc.)

h) categories of data subjects:
(e.g. employees, Data Controller's clients, etc.)

Date: Berlin, 01. January 2020

VCC Live Germany GmbH – Data Processor

XYZ Company GmbH – Data Controller

Annex 2. Technical Security Measures

1. Integrated Management System

1. For the protection of data, information and the business continuity the Processor maintains a regulatory and compliance framework – called Integrated Management System (IMS) – that applies international industry standards such as ISO 27001, ISO 22301, PCI-DSS.
2. The Processor's Corporate Governance Policy describes all the efforts that are made to ensure compliance with protection of information, data and business continuity.
3. The Processor's Integrated Management System covers amongst others: Information Security, Physical security, Network Security, Protection Against Malicious Code, Operational Security, Asset Management, Access Management
4. The Processor undertakes to comply with related legal regulations, in particular GDPR.

2. Server hosting and office environment

1. The Processor keeps its servers, which are used for data processing, in professional server hosting environment provided by certified data centers. Data centers, qualified as sub-contractors, based on the contractual relationship with the Processor, guarantee the following:
   a) the data center shall provide and maintain appropriate premises, facilities and equipment necessary to ensure secured physical premises for the adequate protection against losses or damages to the premises or the equipment, including against loss or unlawful access to the Personal Data;
   b) the data center shall protect the electrical energy and telecommunication infrastructure from interception or damage;
   c) the data center shall use uninterruptible power devices for critical infrastructure, and shall regularly test them.
2. The Controller has the right to to have the Personal Data processed at one or more of data center(s) listed on the data center list in the VCC Live GTA.
3. The Processor will not use services from alternative locations other than those are stated in VCC Live GTA.
4. The Processor guarantees that the used services and facilities ensure that the Personal Data will be processed separately from the Processor's other clients' data.

3. Physical Security

1. The Processor shall use a policy that specifies the requirements for physical access and control of the access in the premises in which the Personal Data is processed.
2. When operating with an automated access control system, the Processor guarantees that the system will record all events and that they are periodically reviewed.
3. The Processor guarantees that all its employees can be identified and have unique passes that are used in an appropriate manner.
4. The Processor guarantees that physical security can be ensured outside working hours at the premises that store or process the Personal Data.
5. The Processor guarantees that the personnel responsible for the security are instructed to undertake relevant action or escalate security incidents to a higher level.
6. The Processor guarantees that at the premises, in which the Personal Data is processed, a clear security policy is followed.

4. Network Security

1. The processor preserves the confidential character and integrity of the Personal Data through the following:
    - use of secured network architecture;
    - networks that store the Personal Data are designed, developed, controlled and managed in compliance with industrial standards regulated in the Processor's Integrated Management System;
    - boundary devices that prevent unauthorized access to systems or data, allowing only explicitly authorized and authenticated access.
2. The Processor shall use a firewall system that keeps track of internal and external traffic, and guarantees that:
    - the firewalls are adequately configured and regularly reviewed;
    - the firewalls use a record of events and warnings in real time;
    - access lists are used in network routers in order to limit access to sensitive interior networks and servers.
3. The Processor shall guarantee that regular vulnerability detection tests are part of its Integrated Management System.

5. Protection against Malicious Code

1. The Processor installs and maintains antivirus software on systems where it is relevant. The Processor and its subcontractor(s) shall act in good faith regarding the detection of hidden code or data intended to or that can cause:
    - destruction, alteration, retention, compromise of the security or facilitating the Personal Data theft;
    - deactivation or blocking of software or systems;
    - access to the Personal Data by resorting to undocumented or unauthorized access methods.
2. The Processor shall ensure timely updates of antivirus software and antivirus definitions.
3. The Processor will immediately notify the Controller as soon as it becomes aware of a virus infection of systems that directly affect the Personal Data and provides a report to the Controller detailing each incident and the undertaken measures for preventing its re-occurrence.

6. System Management

1. The Processor shall maintain system security measures in order to prevent itself from unauthorized access, alteration, interception and destruction of information through processing errors, system errors, loss or abuses of the Personal Data.
2. The Processor regularly updates its installed applications in terms of security perspectives.
3. The remote maintenance is controlled by utilizing the following control mechanisms:
    - access through firewall and VPN;
    - use of secured workstations;
    - access right for restricted number of authorized users;
    - registered user activities.

7. Data Management

1. The Controller can access the Personal Data using VCC Live client software, such as VCC Live Desk and VCC Live Archiver. The communication channels between VCC Live client software and VCC Live server-side services are encrypted, using appropriate algorithms based on risk assessment.
2. Before the Processor destroys any media or storage device that stores Personal Data the Processor will take the necessary steps in order to prevent data loss and data leakage.
3. The Processor guarantees that a risk protection policy related to the use of workstations, mobile computers and communication devices, used for provision of the services to the Controller, is in place.

8. User and Access Management

1. The Processor has an established, documented and periodically reviewed procedure for granting and limiting access to systems that contain the Personal Data to personnel who need to access these systems in order to fulfil their obligations.
2. The Processor uses a policy (Access Management Policy) for generation of passwords and user accounts that is complied with by the Processor's personnel. This includes procedures that are to be followed when personnel leave their workstation (Clear Screen and Clear Desk Policy), and control and management processes for user accounts when terminating employment relations or in role changes. As a minimum, these measures shall:
    - require all system users to enter a unique user identification code or number or password before gaining access to the systems;
    - a minimum password length of at least ten characters to be set; the password shall contain letters and numbers; the maximum term of the password shall be 90 days, and to have a minimum and maximum use term;
    - control the data, to which a user has access or the right to alter, and guarantee that adequate permission is provided before the processing of each change;
    - control the supplement and deletion of system users;
    - control users' access to zones and system characteristics;
    - ensure that access to the Personal Data is granted at a minimum level required for the achievement of business purposes, and access rights are altered or removed when business requirements or purposes change.
3. The Processor uses an automated locking system when a workstation used for access or processing of the Personal Data is left without supervision for a period exceeding 10 minutes.

Date: Berlin, 01. January 2020

VCC Live Germany GmbH – Data Processor

XYZ Company GmbH – Data Controller