Privacy Notice related to the processing of personal data in connection with the use of the UNBLU Cloud Platform

1. Introduction

UNBLU Inc. and its Affiliates ("UNBLU") are committed to ensure compliance with applicable data protection laws and regulations of Switzerland and the European Union, as well as other data protection requirements in any of the jurisdictions where UNBLU operates including certain US jurisdictions and Canada. This Privacy Notice ("Notice") is based, among others, on the principles and requirements of the European Union General Data Protection Regulation ("GDPR), and other applicable national data protection laws, including Swiss Law. By means of this Notice UNBLU informs Customer, about how and why UNBLU processes personal data of end-users, (data subjects as defined in the GDPR), and about end-users´ rights as a data subject in regard to the processing of end-users´ personal data when an UNBLU Customer uses cloud platform services from UNBLU.

2. Scope and Supplement

This Notice covers all forms of processing of personal data by UNBLU in relation to the provision of the UNBLU cloud services. It describes how UNBLU processes personal data obtained directly from the user, or from the UNBLU Customer or business partner. It applies to the processing of end-user personal data obtained through the use of the UNBLU Cloud service.

This Notice may be supplemented by specific data protection and privacy notices and statements that relate to specific forms or purposes of data processing.

3. Personal Data UNBLU processes, Purposes and Legal Basis

This section of Notice describes what personal data UNBLU collects and processes, for what purposes and on what legal basis. The amount of personal data UNBLU processes depends on the context and circumstances of Customer interaction with UNBLU and/or the Customer's use of UNBLU services. UNBLU strives to minimize all data processing.

3.1. Processing of user data

Summary owns and offers to customers its communication platform ("The UNBLU Platform"). The control of what data is entered and processed in UNBLU's Platform is the responsibility of the customer. transmits and stores the data according to the agreed customer requirements. It is the responsibility of the Controller to design the underlying business processes in line with their requirements and relevant regulations. All UNBLU data processing is done for the purpose of operating the UNBLU software. Depending on the agreed customer choices, the UNBLU Platform may include chat, messaging, video/voice calls, co-browsing, document co-browsing, screen-sharing and file upload. It is the responsibility of the controller to define business procedures and rules around the usage of the Platform and personal data.

3.2. Duration:

The data processing under this Data Protection Notice is provided for the duration of the underlying UNBLU Cloud Agreement. After termination of the UNBLU Cloud Agreement, all data will be erased 30 days after the contract duration. It is the responsibility of the controller to export any data the controller wishes to retain within the 30 day window.

3.3. Nature and purpose:

A live engagement system is typically conducted to assist the controller in an online transaction or to assist with general enquiries through the digital channels of the controller. UNBLU provides a system with the following functionalities:

- live chat
- messaging
- co-browsing
- document sharing
- document co-browsing
- web based video/audio chat.

3.4. Type of Personal Data:

It is the responsibility of the controller to define business procedures and rules around the usage of the UNBLU Platform and to define what categories of data the service may be used for. Examples of types of personal data stored in the UNBLU Platform are:

- Date of the online session
- Duration of the online session
- Participants of a conversation session
- Websites visited during the session
- Contents of chat or message conversations
- Browser, OS, Location and other technical details from the participants
- if enabled, recordings of sessions
- Documents uploaded during the conversation
- Types of services engaged during the session
- Users' IP addresses

3.5. Categories of data subjects:

Data subjects are:

- Agents which are typically employees of the controller
- Visitors, which are typically the end customers of the controller

Typically, UNBLU as the data processor, only transmits and stores the end-user data according to the agreed customer requirements. It is the responsibility of the controller to design the underlying business processes in accordance with the applicable legal requirements. The legal basis for processing is the UNBLU Cloud Agreement or another contract between controller and UNBLU related to the provision of the services through the UNBLU Cloud Platform.

In the Unblu cloud, Unblu only uses necessary cookies for the Unblu platform to function properly.

3.6. Legal obligations and compliance

UNBLU´s business is subject to various laws and regulations that impose legal obligations on UNBLU. Some of these laws and regulations may require the collection and processing of personal data (e.g., tax laws, commercial laws, trade and export compliance regulations etc.). Where such legal obligations are based on EU or EU Member State laws and regulations, the legal basis for processing personal data is UNBLU legal obligation. Where such legal obligations are based on laws and regulations of third countries (non-EU),

compliance with these legal obligations may represent a legitimate interest. If so, the legal basis for processing personal data is legitimate interest. The latter applies also to the processing of personal data for the purpose of ensuring compliance with UNBLU policies, codes of conduct and regulations.

4. Sharing Personal Data with Service Providers and Third Parties

The UNBLU Cloud Platform runs on external platforms and systems managed by UNBLU's subprocessors, listed in the Customer's UNBLU Service Contract. The privacy policies of these external subprocessors apply. Any such subprocessing of data will be made under the subprocessor's due diligence and monitoring protocol and will be governed by a a data processing agreement between the subprocessor and UNBLU.

5. Storing periods for Personal Data

5.1. Generally, UNBLU keeps personal data for no longer than is necessary for providing the service as agreed with the controller. Typically, data is stored for all ongoing conversations. For terminated conversations data is stored for one year in the UNBLU Platform, unless another retention period has been agreed with the controller). If a longer retention period is required, the controller can export the data from the UNBLU Platform and take over the processing responsibility of the data.

5.2. If UNBLU processes personal data for the purpose of compliance with laws and regulations that impose legal obligations on UNBLU, UNBLU keeps personal data for as long as such laws and regulations require.

6. Transfers of Personal Data to Third Countries

6.1. UNBLU does not perform any data transfers to third countries, unless directly instructed to do so by the controller in accordance with section 6.2 below.

6.2. The UNBLU Cloud Platform is hosted either on the GCP or on the Aspectra services depending on the configuration of the UNBLU services chosen by the Customer. The GCP data centre is owned by Google. Any processing of personal data made by Google is subject to the Google data protection policy applicable to the GCP data centre. The Aspectra data centre is owned by Aspectra AG (located in Zurich), and all data stored in their data centre are hosted in Switzerland. In case of use of GCP, the Customer can choose the data location within or outside the EEA or Switzerland. In the event of the Customer choses to a data location outside the EEA or Switzerland, UNBLU will use legal instruments of data transfer in accordance with the Applicable Data Protection Laws.

7. Security of Personal Data

7.1. UNBLU has implemented technical and organizational security measures to protect personal data UNBLU processes against accidental or unlawful manipulation, destruction or loss, alteration, and against any unauthorized disclosure or access. Such security measures include advanced authentication tools, firewalls, data loss protection, monitoring of IT infrastructure, and encryption of personal data.

7.2. The technical and organizational security measures are reviewed and adjusted on a regular basis, taking into account the state of the art of technology, the nature, scope, context and purposes of processing and the risks and probability of occurrence. However, given the dynamic context of security measures, state of the art of technology, vulnerabilities, threats and risks, absolute security cannot be guaranteed.

7.3. If Customer has a particular concern about the security of Customer´s personal data, Customer may make an inquiry at legal@unblu.com.

8. End-user's Rights over its Personal Data

The end user has many rights over its personal data and how it is used. All requests regarding the data subject's rights should be addressed to the data controller, UNBLU will assist the controller to fulfill any end-user requests, as applicable according to GDPR or other applicable laws. The controller has, among other obligations, the duty to inform the end user of its rights under the Applicable Data Protection Laws.

9. How to contact UNBLU on Data Protection

If Customer has any questions or concerns about this Privacy Notice or about the protection of Customer´s personal data, please feel free to contact our Data Protection Team at legal@unblu.com

10. Data Processor

Since the purpose and means of the personal data processing are determined by another the controller, UNBLU will process the data in accordance with the instructions of such controller and UNBLU will only be a data processor under the applicable regulations.

11. Amendments to this Notice

UNBLU reserve the right to amend this Notice at any time.