GDPR Privacy Addendum

This GDPR Privacy ("Addendum") is incorporated into the Agreement made by and between TikaMobile, Inc. ("TikaMobile") and the customer signing this document ("Customer") as of "Effective Date". In the event of a conflict between any terms of the Agreement and terms of this Addendum, the terms of the Addendum will take ownership.

Preliminary Statement:
When using TikaMobile applications, Personal Data may be transmitted between Data Controller and Data Processor. This Addendum outlines the commitments of both Data Controller and Data Processor when data processing occurs. This Addendum is only applicable to Customers who license a software product from TikaMobile.

1. **Definitions:**
    a. *Agreement* **-** includes any contracts, schedules, amendments, addendums, supporting documents, and/or any other statements of work referencing the Policy Master.
    b. *Service* **-** refers to the cloud-based software applications provided by TikaMobile in relation to Data Processor and Data Controller.
    c. *Professional Services* **-** refers to contracted, fee-based services delivered by the Data Processor in references to any statement of work, including but not limited to consulting, implementation, change management, training, optimization and/or recurring services.
    d. *Personal Data* – refers to any information that can be associated to an identified or identifiable person ("Data Subject") that is provided to the Data Processor by the Data Controller. An identifiable or identified person is one whom can be identified directly or indirectly by a data reference such as a name, an ID, location coordinates, or any other specific factors.
    e. Processing - refers to the actions executed involving any Personal Data, through automated means or others including but not limited to using, collecting, recording, structuring, storing, editing, providing, moving, erasing, and eliminating that Personal Data.
    f. *Data Controller* – refers to the Customer providing Personal Data to the Data Processor.
    g. *Data Processor* – Refers to TikaMobile.
    h. *Sub-Processor* – refers to any third party selected by the Data Processor to process Personal Data on behalf of the Data Processor in relation to the Service provided under the Agreement.
    i. *Instructions* – refers to the direction related to Processing data submitted by the Data Controller to the Data Processor.
    j. *Personal Data Breach* – refers to any unlawful or accidental loss, alteration, destruction, or disclosure of, or access to, Personal Data transmitted, stored, or processed by the Data Processor on behalf of the Data Controller.

k. *Data Protection Laws* **-** refers to the rules and regulations publicized by the pursuant governing body related to the production of Personal Data, including the EU General Data Production Regulation ("GDPR") 2016/679

2. Scope of Processing

a. Processing is effects Parties entered into contractual agreements, suggesting Data Controllers to benefit from the procedures and protocols put in place by the Data Processor in securing the processing of Personal Data, which can be further defined in Schedule 1 .

3. General Obligations of the Data Processor

a. The Data Processor will Process the Personal Data of the Data Controller by means outlined in Section 1, and follow guidelines defined by the GDPR policy. Updates to any procedures in relation to this policy or obligations to the Data Processor, Personal Data, or Data Controller will be communicated to associated parties.

b. The Data Processor will only use Personal Data for the purpose of performing agreements outlined between associated parties. Personal Data will not be used in any manner outside of the purpose defined in this Addendum.

c. The Data Processor has contracted 3rd party expertise and agrees to collaborate extensively with both expert professionals and the Data Controller to resolve and advise on any submissions from the Data Controller or Processing parties.

d. The Data Processor commits that Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

e. FOR EU CUSTOMERS ALL DATA WILL BE HOSTED ON AWS FRANKFURT, GERMANY LOCATION. IT WILL NOT BE TRANSFERRED TO ANY OTHER LOCATION WITHOUT CUSTOMERS' PRIOR PERMISSION

f. The Data Processor provides visibility into the actions of the Data Processor that is outlined in this Addendum, but does provide the Data Controller with legal advice regarding compliance with Data Protection Laws in the jurisdictions in which the Data Controller uses the Services outlined in the respective contracts or statements of works.

4. Obligations of the Data Controller

a. The Data Controller permits it has all rights to access and restrict Personal Data that it provides or plans to provide to the Data Processor for Processing and agrees to follow the Data Protection Law.

5. Confidentiality

a. The Data Processor commits to compliance with the terms defined in the Addendum regarding confidential information, which may or may not include Personal Data provided by the Data Controller.

b. The Data Processor commits to ensuring employees are educated with the details of this addendum and how TikaMobile commits to GDPR Compliance.

6. Cooperation Obligations

a. The Data Processor obligates to cooperate with all involved in provided Services and ensures fluid data accuracy and compliance. Data Controllers are assured consistent and transparent communications regarding updates and incidents and have the right to request information regarding Personal Data and Processing.

7. Deletion of Personal Data

a. The Data Controller has the right to delete, access, or receive copies of all Personal Data maintained by the Data Processor, outlined, and collected through respective Service agreements and contracts. The Data Processor commits to compliance and immediate action upon the Data Controllers request.

b. Provides access to requested data to the Controller in no less than 30 days.

8. Third-Party Certifications and Audits

a. If requested, the Data Processor will audit and provide proof of compliance to the Data Controller. The Data Controller will provide the Data Processor at least 30 days prior notice of an audit, unless an emergency request is received from a government official or authority figure, in which 5 days' notice will be provided.

b. Data Processor has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Data Controller's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Data Processor shall make available to Data Controller a copy of the most recent third-party audits or certifications, as applicable

9. Sub-Processors

a. The Data Processor will not engage with any other Data Processor without consent or authorization by the Data Controller
b. The Data Controller can verify their specific list of Sub-Processors from the Data Processor at any time.

10. Appropriate Security Measures

a. The Data Processor has implemented and will maintain the technical and organizational measures as described below:
    i. Pseudonymization and encryption to ensure an appropriate level of security
    ii. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are being operated
    iii. Measures to backup and archive appropriately in order to restore availability and access Data in a timely manner in the event of a physical or technical incident
    iv. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures that is implemented.

Additional details are available in IT.SOP-PHYSEC-02 Physical Security Policy & Procedures, IT.SOP-DRP-04 Disaster Recovery, IT.SOP-MAINT-07 Server Maintenance & IT.POLY-SEC-03 Malicious Software Policy, IT.POLY-ENCRYPT-07 Encryption Policy, IT.SOP-INCIDENT-08 Incident Response Policy & Procedures which can be provided upon request.

11. Personal Data Breach Indemnity

a. In case of a breach or electronic or physical incident, the Data Processor has protocols in place in order to address any malfunction immediately and with good intent. When an incident is suspected, the company's goal is to recover as quickly as possible, limit the damage done, and secure the network. Procedures include alarming the organization, removal of the compromised, disabling infected accounts, securing backups to another system, identifying causation, rebuilding systems, restoring validated data, and reflecting on cause and response measures.
b. As incidents occur, users of affected Personal Data will be notified immediately with action plans in place to address the occurrence. Consistent communications methods will be established with appropriate resources between the Data Controller and the Data Processor.

Execution

The authorized representatives of the parties have executed this Addendum by their signatures below:

TikaMobile, Inc.	**Customer Legal Name:**
	Company: _____
By:_____	By:_____
Name:_____	Name:_____
Title: _____	Title: _____
Date: _____	Date: _____

Schedule 1: Data Processing Instructions

The Data Processor will use and Process Personal Data of the Data Controller according to the following scope, manner, and purpose:

1. Personal Data uploaded to the Service provided by the Data Controller will be hosted and stored by the Data Processor and be accessible and usable by the Data Controller via the offerings provided via the Service.
2. Personal Data will only be used for purposes defined in the Service agreement between the Data Controller and Data Processor. The Data Processor will not use Personal Data in any other manner.
3. Personal Data to be Processed by the Service includes the following categories:
    a. Data Subjects defined by the Data Controller which are necessary for the use of the Service include healthcare professional persons who provide the marketing and sales of its products, services or support, and persons whom patients and participants who receive the marketing and sales of its products, services or support.
        i. Healthcare Professional Personal Data consist of:
            1. Name, address, email, telephone numbers, employer information, medical or specialty licenses and IDs, etc.
        ii. Patient and Clinical trial participants Personal Data consist of:
            1. Name, address, email, telephone numbers, birth date, insurance coverage, facility ID's, health/medical data related to the treatment or trial, etc.
    b. Data Subjects who are Data Controller's employees,
        i. Personal Data consist of name, title, address, email, telephone number, username, password, etc.
4. The Service includes but is not limited to the cloud-based software applications provided by the Data Processor to the Data Controller pursuant to the Agreement.

Schedule 2: Technical and Organizational Security Measures

This schedule provides the current technical and organizational security measures in place at TikaMobile. Changes may be made to these standards in order to remain compliant to security, government, regulatory or other changes that dictate the landscape of the Services provided. Changes made will never degrade the standards of protection outlined in the schedule.

Security Policy and Standards

1. TikaMobile has up to date information security policies which are applied across the entire enterprise. These policies include
    a. Procedures and discourse to be followed in response to an event
    b. Penalties and actions for defilement
    c. Guidelines for observation
2. TikaMobile has clearly defined security standards and holds signed agreements from all employees, contractors and 3rd parties involved in Services provided.

Security Organization and Management

1. Policies and responsibility for security management is in place for:
    a. Outlining and monitoring the information security arrangements of TikaMobile
    b. Main points of contact for information on security issues

2. Policies and arrangements are in place to ensure users, staff, and other employees are accountable and responsible for all actions related to information security.

Security Architecture

1. A structured and enforced security architecture covering all information resources, assets, and standards of TikaMobile has been developed and applied to all lengths of the company.
2. The architecture:
    a. Defines access privileges implemented or removed immediately following the onboard or offboard of that individual with TikaMobile;
    b. Enforces security protocols required for different levels of production and information;
    c. Provides customer and technical support for all authorized users of the Services provided by TikaMobile;
    d. Drives the secure flow of data between technical environments;
3. An accurate record of the critical information assets is updated and maintained by TikaMobile at all times.

Personnel Security

1. Personnel procedures are in place to:
    a. Oversee information processing activity
    b. Educate personnel to reduce risk of improper activity
2. User roles and access rights have been defined and split between operational staff and network and systems development staff.
3. Legacy activity is stored and monitored by appropriate personal, designated in the handling and processing of information and assets. Activity captured provides adequate information to ensure accountability.

Physical and Environmental Security

1. Equipment and facilities are protected against loss or damage. Measures include but are not limited to
    a. Restricted areas are accessible only to authorized staff
    b. Employment of security personnel to provide protection
    c. Employees are empowered to protect secure information and assets
2. Production environments employ specialized equipment to:
    a. Ensure optimal uptime
    b. Recover information in case of damage or breach.
    c. Reduce physical environmental threats

Network Management and Systems Maintenance

1. Remote access may only be obtained after proper authentication.
2. Firewalls are in place for both internal and external system protection, in addition to establishing control over information flow between the network an outside world.
3. Environments are established to separate development and production releases and capabilities. User authentication is defined by their role in the system and application release.
4. Software and connecting system integrations are updated and maintained in accordance with security protocols and scheduled enhancements, ensuring optimal performance.
5. Internet use policies are established across the enterprise. Intrusion detection services ensure protection of critical systems, including those connected to the internet. Encryption methods are used when data is in transit across untrusted networks.
6. Process for changes, enhancements and developments to systems are defined and documented into a formal process.

Access Control and Compliance

1. Proficient methods for authentication have been deployed to meet company standards. Passwords, usernames, and points of access operate securely in good practice. Efficient mechanisms for access verification are put in place to ensure user identity is protected and executed properly.
2. All servers and supporting technologies are enabled with protection and methods or restoration to maintain essential functionality and services.
3. Access by all users and associates is logged and maintained for tracking and legacy purposes. User identification supports individual accountability.
4. Authorization procedures are reviewed, updated, and applied to maintain high security measures and ensure efficient process.
5. All changes from all users documented within the system are recorded for auditing purposes, reviewed periodically or when requested.
6. TikaMobile has processes and procedures in place for handling security incidents in a timely manner
7. Monitoring responsibilities are defined, ensuring proper updates are applied.
8. All systems are scanned regularly for vulnerabilities.