APPENDIX 3: DATA PROCESSING AGREEMENT

1 BACKGROUND

1.1 Kivra will process personal data in order to provide the Services that pertain to the General T&C signed by the Parties. This data processing agreement ("**Data Processing Agreement**") governs the relationship between Kivra and the Sender, wherein Kivra acts in its capacity as data processor and the Sender acts in its capacity as data controller.

1.2 If, and to the extent that, another company in the same group as the Sender is to be regarded as the data controller (solely or together with the Sender) for processing that is subject to this Data Processing Agreement, the Sender hereby confirms that necessary permissions have been obtained on behalf of such company to enter into the Data Processing Agreement.

1.3 Should there be any inconsistencies between the terms provided in this Data Processing Agreement and other agreements, documents or instructions, regardless of their format, concerning the processing of personal data, the terms of this Data Processing Agreement shall take precedence and govern the obligations and actions of the Parties with respect to the processing of personal data.

2 DEFINITIONS

2.1 The definitions and terms used in this Data Processing Agreement shall have the same meaning and implications as the definitions and terms provided in the General T&C.

2.2 The following concepts are to have the meanings stated below, unless the circumstances clearly give rise to other meanings (and terms that are not defined in the Data Processing Agreement such as "data controller", "data processor", "personal data", "processing", and "personal data breach" shall have the meaning stated in the General Data Protection Regulation):

The **"General Data Protection Regulation**" refers to 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 (General Data Protection Regulation).

"Data Subject" refers to a natural person whose personal data is included in the Data.

"Applicable Data Protection Legislation" refers to: (i) The General Data Protection Regulation and replacement legal acts; (ii) applicable Swedish law concerning data protection; and (iii) ordinances and directives pertaining to i) and ii) issued by Supervisory Authority, that are applicable to either Party's operations.

"Supervisory Authority" refers to the Swedish Authority for Privacy Protection (*Integritetsskyddsmyndigheten*) and when applicable, other competent authorities that by virtue of the law supervise either Party's operations.

The **"Data**" refers to the personal data that is transferred to, stored or in any other way processed by Kivra on behalf of the Sender, in accordance with this Data Processing Agreement. The types of personal data covered are stated in Sub-appendix A to this Data Processing Agreement.

3 INSTRUCTIONS

3.1 The Data Processing Agreement is comprised of this document, Sub-appendix A and Sub-appendix B. Sub-appendix A specifies the processing and Sub-appendix B describes Kivra's security measures.

3.2 The Sender gives Kivra permission to transfer the Data to a third party when such is required to fulfill the purpose of this Data Processing Agreement, including the pertaining instructions, and/or to fulfill a legal obligation. This includes, but is not limited to, transferring the Data to suppliers, partners and authorities.

3.3 Kivra must not process the Data in any other way, for other purposes or according to other instructions than those stated in this Data Processing Agreement and Applicable Data Protection Legislation. If Kivra deems that necessary instructions for carrying out the assignment under this Data Processing Agreement are missing, or if Kivra notices that the instructions contravene Applicable Data Protection Legislation, Kivra must immediately inform the Sender of its stand-point and take those measures that Kivra deems necessary to comply with Applicable Data Protection Legislation. Kivra is not therefore obliged to adhere to an instruction if Kivra deems that the instruction contravenes Applicable Data Protection Legislation.

3.4 Kivra can continue to process relevant information from the Data for its own purposes in the role as data controller, for invoicing purposes, and in order to analyse and improve Kivra's services to Senders. Kivra is responsible for informing the Users about this processing in Kivra's at any time applicable privacy notice.

4 SECURITY - TECHNICAL AND ORGANISATIONAL MEASURES

4.1 Kivra is obliged to take appropriate technical and organisational measures to comply with the requirements of Applicable Data Protection Regulation, in particular Article 32 of the General Data Protection Regulation, and thereby ensure that the rights of the Data Subjects are protected. These measures involve Kivra's protection of the Data from unauthorised access, destruction or amendment. A description of these security measures is available in Sub-appendix B. Kivra reserves the right to update Sub-appendix B with security measures taken, without further notice of this in accordance with section 10.3.

4.2 Kivra commits to ensuring that Kivra has the expertise, reliability and resources to implement technical and organisational measures that fulfil the requirements of Applicable Data Protection Legislation, especially requirements related to security, pursuant to the above.

5 INFORMATION DUTY AND ASSISTANCE

5.1 After detecting that there has been a case of, or an attempted, unauthorised access, destruction or amendment to the Data, as well as any other personal data breach, Kivra must inform the Sender of this without undue delay. In the event that the Service, or parts of the Service are unavailable for other reasons than those named above, for example due to internal system disruptions, information about this will be published via kivrastatus.se.

5.2 When Kivra notifies the Sender in accordance with section 5.1 above, the notice must include information about:

a) the nature of the personal data breach including, where possible, the categories of and the approximate number of Data Subjects concerned and the categories and approximate number of Data records concerned,
b) the name of and the contact details for the data protection officer or other point of contact from which more information can be obtained,
c) the likely consequences of the personal data breach, and
d) the measures that Kivra has taken or proposed to address the personal data breach including, when appropriate, measures to mitigate the potential adverse effects of the breach.

5.3 If, and to the extent that it is not possible to provide information in accordance with section 5.2 simultaneously, information can be provided in batches, however without further undue delays.

5.4 Kivra must reasonably assist and collaborate with the Sender in ensuring compliance with obligations in accordance with Articles 32–36 of the General Data Protection Regulation, with respect to the type of processing and the information that Kivra has at its disposal, and in ensuring that the Data Subject's rights can be fulfilled in accordance with Applicable Data Protection Legislation.

5.5 Kivra must inform the Sender without undue delay of any contacts with the Supervisory Authority concerning, or that can be significant to, Kivra's processing of Data. This obligation is, however, limited to such processing of Data that concerns or may come to concern the Sender. Kivra does not have the right to represent the Sender nor to act on its behalf vis-à-vis the Supervisory Authority.

6 AUDITS

6.1 The Sender has the right to audit, or to hire a third party to audit, Kivra's processing of the Data to assure itself that such processing complies with the Applicable Data Protection Legislation, this Data Processing Agreement and any instructions issued. Unless otherwise stipulated in any separate special written agreement, each Party will bear its own costs for auditing and for providing information, in accordance with section 6.1 herein.

6.2 Kivra must reasonably contribute to such checks and audits and, upon request, provide the Sender the assistance and documentation reasonably required for this purpose.

6.3 If the Sender engages a third party to carry out an inspection of Kivra's processing of the Data on behalf of the Sender, the Sender must ensure that such third party signs an appropriate non-disclosure agreement, before any inspection, agreeing to not disclose information to any third party.

6.4 Oversight for auditing, submitting information and similar must be scheduled at times of the day, and otherwise take place in a manner that has the least possible impact on Kivra's operations. Auditing of Kivra must be carried out with regard to the security measures established by Kivra, provided that these measures do not prevent or make it substantially difficult to perform the audit.

7 ENGAGEMENT OF SUB-PROCESSORS

7.1 The Sender hereby accepts the use of the sub-processors already engaged by Kivra, as stated in Sub-appendix A to this Data Processing Agreement.

7.2 Kivra undertakes to inform the Sender of any plans to engage new sub-processors and/or to replace current sub-processors at least thirty (30) days before such plans are implemented. If the Sender does not revert to Kivra within the thirty (30) days, the Sender is considered to have accepted Kivra's plan to engage/replace the sub-processor(s) of which Kivra has informed the Sender. If the Sender does not approve a sub-processor that Kivra intends to use, the Parties commit to collaborating with each other to find a suitable solution. If no suitable solution can be found, the Sender has the right to terminate this Data Processing Agreement immediately.

7.3 Kivra undertakes to sign a written agreement with current and new sub-processors which governs the processing performed by the sub-processor. The agreement shall impose the same data protection obligations on the sub-processor as those imposed on Kivra in this Data Processing Agreement. In the event that the sub-processor does not fulfil its obligations regarding the processing, Kivra will remain liable vis-à-vis the Sender for the sub-processor's fulfilment of its obligations under this Data Processing Agreement.

7.4 Furthermore, Kivra may only transfer or otherwise process the Data under this Personal Data Processing Agreement outside the EU/EEA if the Sender has given written consent in advance. A transfer to a country outside the EU/EEA also requires that Kivra, before the transfer begins, fulfils the requirements and measures that follow from Applicable Data Protection Legislation, which includes that Kivra must ensure that the transfer takes place to countries that have been decided by the European Commission to have an adequate level of protection or if necessary, include the EU Commission's standard contractual clauses applicable at any time.

8 LIABILITY

8.1 If any Party (including those working under the supervision of a Party or a sub-processor engaged by a Party) acts in breach of this Data Processing Agreement or Applicable Data Protection Legislation, such Party must indemnify the other Party against any damages caused by such unlawful conduct.

8.2 Kivra shall be liable for damage that arises as a consequence of processing of the Data only if Kivra has not fulfilled its specific obligations in accordance with this Data Processing Agreement. Kivra will be exempted from liability if it appears that Kivra is in no way responsible for the event that caused the damage.

8.3 A Party's right to compensation under section 8.1 is limited to direct damages up to a total amount corresponding to five (5) price base amounts per calendar year, in accordance with the Social Insurance Code (2010:110). Under no circumstances is a Party to be liable for indirect damages, such as lost profits, loss of income, obstruction from fulfilling commitments to third parties, liability for damages to third parties or other resulting damages. This limitation of liability does, however, not apply in case of gross negligence or intent.

8.4 Any fines pursuant to article 83 of the General Data Protection Regulation, or Chapter 6, Section 2 of the Act containing supplementary provisions to the EU General Data Protection Regulation (2018:218), will be borne by the party charged with the fee by the Supervisory Authority.

8.5 If either party becomes aware of any circumstances that may cause damage to any other Party, they must immediately inform the other Party about the situation and actively work together to prevent and minimise such damage.

9 CONFIDENTIALITY

Each Party must ensure that persons who have access to the Data or confidential information have undertaken to adhere to confidentiality or be subject to a statutory duty of confidentiality in accordance with the requirements of Applicable Data Protection Legislation, and are informed about how they must process the Data.

10 AMENDMENTS AND NOTICES

10.1 The Sender can only amend content in this Data Processing Agreement to the extent that such amendments are needed to satisfy requirements stipulated by Applicable Data Protection Legislation. Such amendments take effect no later than thirty (30) days after Kivra has received the notice of amendment.

10.2 The Sender must notify Kivra of any adjustments to the Sender's instructions, which are described in detail in Sub-appendix A, in accordance with section 10.4 so that necessary amendments to processes can be implemented. Kivra has the right to resign from the assignment if the Sender's instructions cannot be reasonably fulfilled. Such amendments take effect no later than thirty (30) days after Kivra has received the notice of amendment.

10.3 Kivra reserves the right to amend and/or make additions to this Data Processing Agreement at any time. Any amendments and additions must be notified no later than thirty (30) days before the amendment takes effect. Kivra nevertheless always has the right to implement such amendments and additions that are required by Applicable Data Protection Legislation or official decisions. If the Sender does not accept Kivra's amendments and/or additions, the Sender has the right to immediately terminate this Data Processing Agreement.

10.4 All notices and other communications from a Sender to Kivra under this Data Processing Agreement, must take place in writing via e-mail to privacy@kivra.com. All notices and other communications from Kivra to the Sender must take place in writing via e-mail to the e-mail address provided by the Sender. Notices are deemed to have been received by the receiving Party on the same day that the e-mail is received. Each Party is responsible for keeping its contact details up-to-date.

11 TERM AND MEASURES AT EXPIRATION

11.1 The Data Processing Agreement is valid from the date of signing and for as long as Kivra processes the Data under the General T&C.

11.2 The Parties agree that after the termination of the processing, and depending on the Sender's instructions to Kivra, Kivra and any sub-processors will erase transferred Data and copies without any undue delay, but no later than thirty (30) days after the General T&C or the Data Processing Agreement ceases to be valid.

12 APPLICABLE LAW AND DISPUTE RESOLUTION

Applicable law and dispute resolution is governed by section 17 in the General T&C. .

SUB-APPENDIX A: SPECIFICATION

SERVICE	PURPOSE OF PROCESSING	PERSONAL DATA CATEGORIES	DATA SUBJECT CATEGORIES	DURATION OF THE PROCESSING OF THE PERSONAL DATA FOR THE PURPOSE	SUB-PROCESSORS (LOCATION)
Payable E-Correspondences (optional)	Kivra shall receive and share payment information with the Sender in cases where the Sender chooses to receive the information directly from Kivra and not via a Partner	Payment information.	Users.	A maximum of 13 months.	Not applicable. (Tink AB, Getswish AB and Trustly Group AB are data controllers for their respective processing of the Data.)
Swish (optional)	Kivra is to share Data with Getswish AB to enable payments, and is to receive confirmations and status of the payment from Getswish AB.	Data about payment.	Users.	Sharing is done immediately.	Not applicable. (Getswish AB is the data controller for its processing of the Data.)
Automatic payments (optional)	Kivra is to share Data with Trustly Group AB in order to set up the direct debit mandate and enable payment, and similarly receive confirmation and status of the direct debit mandate and payment from Trustly Group AB, and share these with the Sender. Kivra may also share the User's name to facilitate the Sender's troubleshooting.	Data about direct debit mandate and payment. Data about User's name.	Users.	Sharing is done immediately. 45 days as Retrieval Period for Automatic Payment.	Not applicable. (Trustly Group AB is the data controller for its processing of the Data.)
Campaigns (optional)	Kivra is to distribute campaigns to Users. When segmentation is to be used, also limit the list of Users that are to be exposed to the campaign.	Data needed to distribute campaigns. When segmentation is to be used: personal identity number.	Users.	For the period during which the Sender chooses to distribute the campaigns, or a maximum of 365 days. Personal identity numbers are immediately deleted once segmentation has taken place.	Not applicable.
Forms (optional)	Kivra is to make responses available to the Sender during the Retrieval Period for Forms in cases where the Sender chooses to retrieve the responses directly from Kivra and not via a Partner.	Personal data that is in the questionnaire. Metadata that pertains to the questionnaire. If the Sender retrieves Users' bank account details, bank account details are processed.	Users.	30 days.	If bank account details are retrieved: Tink AB, which provides a service for verifying bank account details (EU/EEA).

Registered E-Correspondences (optional)	Kivra is to make proof of receipt available to the Sender during the Retrieval Period for Registered E-Correspondences in cases where the Sender chooses to retrieve such proof of receipt directly from Kivra and not via a Partner.	Personal data that is in the proof of receipt, namely personal identity number, information regarding the signature with BankID, and metadata from the registered E-Correspondence.	Users.	30 days.	Not applicable.

SUB-APPENDIX B: SECURITY

1 INTRODUCTION

1.1 The goal of this document is to provide transparent, high-level information to Kivra's stakeholders about Kivra's commitment to information security. The document describes Kivra's information security responsibilities and undertakings regarding both the services that Kivra provides to Senders (Sw. *Avsändare*), i.e. the Delivery Service (Sw. *Förmedlingstjänsten*) and any Additional Services (Sw. *Tilläggstjänster*) as well as the services that Kivra provides to Users (Sw. *Användare*). i.e. the digital mailbox (Sw. *digitala brevlådan*). These services are in this document together referred to as the "**Kivra Platform**".

1.2 As Kivra may change its security measures over time, this document may be revised accordingly. Partners and Senders of Kivra can always receive the latest version of this document by contacting Kivra's Security Team as security@kivra.com.

2 KIVRA'S CORPORATE TRUST COMMITMENT

Kivra is committed to achieving and maintaining the trust of our stakeholders. Our goal is to be as transparent as possible with our stakeholders in offering security to meet and exceed expectations in today's ever changing tech landscape.

3 GOVERNANCE

3.1 Policy Ownership

Kivra has a documented Information Security Policy that all employees must read and acknowledge. This policy is approved by the Board of Directors, reviewed and updated annually. Information Security Policy development, maintenance, and issuance is the responsibility of the Kivra CISO.

3.2 Kivra Infrastructure

Kivra hosts the Kivra Platform in a hybrid-cloud environment. Content is hosted in multiple on-premise data centers located within Sweden. The data center facilities are provided by Swedish suppliers, all hardware and software is owned by Kivra and maintained by either our employees or consultants contracted directly by Kivra.

3.3 Third-Party Architecture

Kivra may use one or more third-party suppliers. When doing so, Kivra contractually ensures that these third parties follow adequate security requirements.

Kivra has Risk Management procedures in place that take integrations with, and solutions from, third parties into account on a service/system level. This is governed by the Information Security Policy and the Third Party Risk Management Instruction.

3.4 Audits, Certifications, and Regulatory Compliance

Kivra is connected to the infrastructure Mina meddelanden, governed by the Agency for Digital Governance ("**DIGG**"). As such, Kivra is regularly audited by DIGG towards their ISO27001-based information security requirements.

Kivra's information security is governed by an Information Security Management System (ISMS) that adheres to the ISO 27001 standard.

4 SECURITY CONTROLS

4.1 Organization of Security

Kivra's COO is responsible for the overall Information Security Management of the Kivra Platform, including oversight and accountability. This responsibility is enforced by the Kivra CISO who answers directly to the Kivra COO and leads a Security Team that consists of a Security Subject Matter Expert, Security Engineers and Infrastructure Security. All Business Function/System Owners (Product Owners and Engineering Managers) have Information and IT Security responsibilities within their roles.

The Physical and Personal security of Kivra's offices and employees is the responsibility of the Kivra COO, also coordinated by the Security Team.

4.2 Asset Classification and Logical Access Control

- Kivra maintains an inventory of essential information assets such as servers, databases, and software governed by the IT Policy and the IT Asset Management Instruction.
- Kivra adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff.
- Kivra maintains separate development, sandbox (UAT), staging and production environments. Access to each environment and within each environment is separated and strictly controlled.
- All access to Kivra's servers or data is logged and can only be accessed using multifactor authentication or by users using Mobile Bank-ID.
- Kivra's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.
- Audits on accounts and access are performed regularly.

4.3 Personnel Security and Training

- All employees at Kivra sign a confidentiality agreement when their employment begins. In addition, Kivra conducts background checks for system administrators, developers and other users with privileged access as part of its onboarding process. This also includes key roles within the Kivra Management Team.
- All employees are informed of, and agree to comply with, Kivra's IT- and Information Security policies and practices as a part of their initial on-boarding.
- All Kivra employees undergo security and privacy training as part of their on-boarding and receive frequent training sessions focusing on specific subjects such as phishing.
- Kivra conducts frequent awareness related tests and communicates security related information to all employees and consultants through several internal communication channels.

4.4 Physical and Environmental Security

- Access to Kivra facilities is controlled by 24-hour security. Additionally, all Kivra offices are protected by locked access and are under 24-hour video surveillance (recording triggered by motion). All Kivra employee workstations are encrypted and password protected, and all Kivra user accounts require two-factor authentication.
- Data centers facilities and physical security are provided by Swedish suppliers complying with Kivra contractual requirements.

4.5 Policies and Logging

The Kivra Platform is operated in accordance with the following procedures to enhance security:

- All processing of content is logged monitoring user activity and potential anomalies.
- API key information for third-party services provided by the Sender are encrypted for storage.
- Kivra keeps audit logs for all access to production servers.
- Server access is controlled via public key access, instead of passwords.
- Logs are stored in a secure centralized host to prevent tampering.
- Kivra application and ssh audit logs are stored for five years.
- Passwords are not logged under any circumstances.
- Access to Kivra mail and document services is only allowed on approved workstations and mobile devices that have automated security policies enforced.

4.6 Intrusion Detection

Kivra monitors system, user, and file behavior across its infrastructure using a host-based Intrusion Detection System. Intrusion Detection alerts are monitored by the Security Team and an external SOC.

Kivra's APIs use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and alerts are handled by Kivra's engineering team.

4.7 Security Logs

All Kivra systems used in the provisioning of the Kivra Platform, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized log server (for network systems) in order to enable security reviews and analysis. Kivra has automated alerts and searches on these logs.

4.8 System Patching and Configuration Management

Kivra patches its servers on a regular basis, which ensures that the latest patches for the software we use are applied. Kivra's configuration management system regularly applies configuration based on repositories.

Kivra maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

4.9 Vulnerability Management

Kivra's infrastructure and applications are continuously scanned for vulnerabilities. Alerts are monitored by our Security Team. Kivra also maintains a list membership to various CVE vulnerability mailing lists. Patches and vulnerabilities are remediated based on severity. This is governed by the Information Security Policy and the Vulnerability Management Instruction.

In addition, Kivra integrates security into its development process by utilizing static code analysis tools to identify potential vulnerabilities in our codebase before deployment.

4.10 Third-Party Penetration Testing

Kivra undergoes a third-party penetration test of the Kivra Platform on an annual basis. Kivra also conducts our own internal penetration tests in relation to significant changes in our services and environment.

4.11 Monitoring

For technical monitoring, maintenance and support processes, Kivra uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- Application Tracing
- Error monitoring
- Office monitoring

4.12 External Access Control

The Kivra Platform employs a variety of security controls. These include, but are not limited to:

- Receiving Users log in to the Kivra Platform using Mobile Bank-ID.
- Senders log in to the Kivra Platform using Google Authentication or OTP.
- All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Kivra does not use persistent cookies for sessions.
- Sessions expire after a few hours of inactivity.
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

- Kivra's REST APIs are accessed with separate API keys, which can only be provisioned by Kivra Sender user accounts with administrative access. API keys are granted access to specific API endpoints when created.

4.13 Development and Maintenance

Kivra uses third party tools to effectively manage the development lifecycle. During testing, Kivra generates sandbox accounts and fake data for testing. Kivra does not use production data in sandbox accounts.

Application source control is accomplished through private repositories. Kivra has controls in place to ensure that all code changes are reviewed and implemented by at least two developers before being merged to Kivra's main code branch.

Kivra maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

4.14 Malware Prevention

As a mitigating factor against malware, all Kivra servers run LTS editions of Operation Systems, as well as malware protection functionality.

Kivra provides proper change management to ensure that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Kivra employee workstations are provided with virus scanners and updated definitions sent out from a central device management platform.

4.15 Information Security Incident Management

Kivra maintains written and regularly tested incident management instructions and procedures. Kivra has 24x7x365 on-call incident management staff. Kivra uses tools to ensure complete coverage with defined escalation policies.

4.16 Data Encryption

The Kivra Platform uses industry-accepted encryption practices to protect Sender data and communications during transmissions between a Sender's network and the Kivra Platform and at rest.

4.17 Return and Deletion of Kivra User Data

The Kivra Platform allows import, export, and deletion of Kivra User data by authorized users at all times during the term of a Kivra User's subscription. Following termination or expiration of the Kivra User subscription, Kivra shall securely overwrite or delete Kivra User data within 20 days following any such termination, in accordance with Kivra's General Terms and Conditions.

4.18 Reliability and Backup

All networking components, SSL accelerators, load balancers, web servers and application servers are configured in a redundant configuration. All Sender data submitted to the Kivra Platform is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

4.19 Business Continuity Management and Disaster Recovery

Kivra has documented Business Continuity procedures. Normal backups are stored in backup servers on-site.

Clusters containing User data use replication to other sites and duplication factors to ensure data redundancy. We also use life-cycle policies to ensure a "delete all scenario" is impossible.

4.20 Mobile Device Management Policies

Kivra uses Mobile Device Management ("**MDM**") platforms to control and secure access to Kivra resources on mobile devices such as phones, tablets, and laptops. Kivra enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe.

4.21 Blocking Third Party Access

The Kivra Platform has not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access data. We do not provide any government or other third party with encryption keys, or any other way to break our encryption.

5 CONTACTS

Kivra's Security Team can be reached by emailing security@kivra.com.