DPA (Data Processing Agreement)

In case of concerns related to data protection or sharing, contact us anytime via email to support@krispcall.com or riskmanagement@krispcall.com.

This Data Processing Agreement, including its Exhibits and Appendices ("DPA") forms an addendum to the Subscription Agreement or Terms of Use between KrispCall and Customer for the purchase of Services, including any applicable number purchase, member add, Purchase Orders, exhibits and/or schedules (the "Agreement").

In the course of providing the Services to Customer pursuant to the Agreement, KrispCall may process Personal Data on behalf of Customer. This DPA reflects the parties' agreement with regard to the processing of Personal Data.

The parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. The DPA regulates the collection, use, transfer, and sharing of personal data with the vital purpose of protecting it. KrispCall is dedicated to complying with the European General Data Protection Regulation (GDPR) by accessing, identifying, governing, protecting, and auditing user data.

1. Data Protection Laws

1.1 Compliance with Data Protection Laws:

The Customer affirms that this Data Processing Agreement (DPA) adheres, to the best of its knowledge, to all relevant Data Protection Laws and includes all required provisions. Given the nature of the services, the Customer acknowledges that the processing of Personal Data under this DPA might be subject to various Data Protection Laws, even those not explicitly mentioned here. This depends on how extensively the Customer uses the services in different regions. The Customer is responsible for promptly informing KrispCall of any inconsistencies between this DPA and the requirements of Data Protection Laws.

1.2 EEA data protection

Both parties recognize that the General Data Protection Regulation (GDPR) applies to the processing of Personal Data, provided that the conditions outlined in Article 3 of the GDPR are met. Additionally, they acknowledge that the Federal Act on Data Protection (FADP) applies to the processing of Personal Data, provided that the conditions set forth in the FADP are satisfied.

Roles and Responsibilities. The parties recognize their roles and responsibilities under the GDPR and other laws. To the extent Customer acts as a data processor, Customer will:

(a) Ensure KrispCall assumes the same obligations as between the Customer and its data controller

(b) Ensure its instructions align with agreements between Customer and its data controller

(c) Assume the rights and duties of a data controller under this DPA

(d) Remain liable to its data controller if KrispCall breaches obligations

1.3 HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations restrict KrispCall's abilities to use and disclose protected health information.

As per the requirement of HIPAA standards, the Covered Entities must:

- Ensure the confidentiality, integrity, and availability of all electronic personal health information (ePHI) that the Covered Entity creates, receives, maintains, or transmits.
- Protect yourself against any reasonably anticipated threat or danger to the security or integrity of this information.
- Protect yourself against any reasonably anticipated threat or danger to the security or integrity of this information.
- Protect yourself against any reasonably anticipated use or disclosure of this information that is not permitted or required by privacy regulations.

KrispCall is HIPAA compliant and follows all the practices to meet HIPAA criteria, which include;

Authentication: Each agent is assigned a specific role so that they are required to use their own unique account to access the services of KrispCall.

Encryption: Transport Layer Security (TLS), virtual private networks (VPN), and other encryption technologies are used to protect data.

1.4 Australian Data Laws:

Both parties acknowledge that Australian Data Protection Laws apply to any Personal Data collected from or held within Australia.

1.5 U.S. Federal Trade Commission enforcement

Both parties acknowledge that the U.S. Federal Trade Commission (FTC) enforcement may apply to consumer privacy, data protection, and fair business practices collected from or held within the USA. KrispCall and the Customer collectively commit to complying with FTC regulations, guidelines, and enforcement actions pertaining to the following areas:

- Adhere to FTC regulations concerning consumer data privacy and security. This involves safeguarding personal information, responding promptly to breaches, and ensuring transparency in data practices.

- Comply with the Children's Online Privacy Protection Act (COPPA) when applicable, especially if their services involve collecting data from children under 13 years old. Measures will be taken to protect children's privacy rights.

- Commit to accurate representation and adherence to the EU-U.S. Privacy Shield Framework, as enforced by the FTC.

- Respect the National Do Not Call Registry, refraining from contacting individuals who have opted out of telemarketing calls.

2. Data Processing

Customer and KrispCall agree that Customer may act as either a controller or processor regarding the processing of Customer Data, while KrispCall acts as a processor. KrispCall will process Customer Data only on instructions from the Customer.

2.1 Customer’s Processing of Personal Data:

The customer determines the purposes and means for processing Personal Data under this DPA. Customers shall provide instructions for KrispCall to process Personal Data only as necessary for providing the Services. Customer's instructions must comply with applicable data protection laws. The Agreement and Customer's use and configuration of the Services constitute Customer's complete instructions. Any additional instructions require KrispCall's prior written agreement.

2.2 Processing of Personal Data:

For Customer Data, the parties acknowledge Customer is a controller and KrispCall acts as an independent controller, not a joint controller with Customer in compliance with Applicable Data Protection Laws. As a controller, KrispCall may process Customer Data for purposes such as:

(a) Managing the customer relationship

(b) Security monitoring, fraud prevention, and misuse investigation

(c) Identity verification

(d) Complying with legal obligations for data retention

(e) Other processing permitted under applicable data protection law

Such processing will comply with this DPA, the Agreement, and KrispCall's Privacy Policy.

2.3 Purpose Limitation:

KrispCall ("Processor") agrees to process data on behalf of the Customer ("Controller") for the purpose of providing communication services as described in Section A of this Agreement.

2.4 Customer’s Liability:

The customer has sole responsibility for the accuracy, quality, and legality of the Personal Data it provides to KrispCall. Where European or Australian data protection laws apply, the Customer is responsible for:

- Notifying data subjects about processing under this DPA, including notice of KrispCall's Privacy Policy.
- Complying with its obligations as a data controller
- Obtaining consent if required
- Ensuring it and KrispCall are authorized to process the data per this DPA

2.5 Customer Instructions:

The Customer instructed KrispCall to process and handle Customer Data for the provision of services. KrispCall will carry out this processing in compliance with the Customer's instructions, as outlined in Section A of this Agreement. Any additional instructions necessary for providing the Services to the Customer need a separate written agreement. This encompasses tasks like investigating security incidents and implementing measures to prevent spam, fraudulent activities, and breaches of the KrispCall Terms and Conditions.

2.6 Confidentiality

In accordance with applicable data protection laws, KrispCall warrants and agrees to:

(a) Maintain confidentiality commitments from personnel authorized to process Personal Data and grant access only on a need-to-know basis.

(b) Notifies Customer if any instruction infringes applicable laws

(c) Implements appropriate technical and organizational measures to ensure data security and confidentiality as described in this DPA

(d) Provide reasonable assistance to Customers related to security, breach notification, impact assessments, and consulting with regulators, considering the nature of processing and information available.

(e) Discloses information necessary to demonstrate KrispCall's compliance with its obligations under this DPA and applicable laws.

3. Data Subject Rights

KrispCall, upon the customer's request, will promptly offer reasonable assistance. This assistance aims to help the customer meet their data protection obligations related to data subject rights as defined by Applicable Data Protection Laws. The Customer agrees to collaborate closely with KrispCall, offering the necessary support and pertinent information to effectively address Data Subject requests. You have the following rights with respect to your Personal information:

3.1 Right to Know

You have the right to know and see what data we have collected about you, including:

- Categories of personal information that we have collected related to you.
- Categories of sources from which personal information is collected.
- Commercial or business purpose of collecting your personal information.
- Categories of third parties to whom we have shared your personal information.
- Personal information that we have collected about you.

3.2 Right to Access

You have the right to obtain a copy of your personal information, along with the explanation, purpose, and details of the collected data. You can have information on;

- Categories of personal information that we have collected related to you.

- Categories of sources from which personal information is collected.
- Commercial or business purpose of collecting your personal information.
- Categories of third parties to whom we have shared your personal information.

3.3 Right to Correct

You have the right to correct or update your personal information stored by us.

3.4 Right to Report

You are entitled to report complaints to the supervisory authority if you believe your privacy is being violated.

3.5 Right to Delete

You are entitled to suspend the processing of your personal data if the data processing is unlawful or the accuracy of your data is contested. For instance, you can delete call recordings, and SMS/Call logs by connecting to our API, which will be removed entirely from our databases.

After 15 days post-termination, KrispCall will delete all Customer data processed solely on behalf of and for Customer, unless applicable law requires retention. Customer consents to such deletion after the 15-day export period and understands exported data will be Customer's sole record of their data after that point.

Any of Customer's data that KrispCall holds or processes as an independent data controller will be retained and deleted in accordance with KrispCall's Privacy Policy.

3.6 Regulatory Actions

If KrispCall receives any claims, complaints, requests, or other regulatory actions relating to Personal Data processed under this DPA, then to the extent required by applicable law, KrispCall will:

(a) Send a notification to Customer via email to the designated contact address, providing reasonable details to allow Customer to respond appropriately;

(b) Deliver reasonable assistance and cooperation to Customer in relation to the Regulatory Action;

(c) Refrain from responding to the Regulatory Action unless required by law or authorized in writing by Customer, in which case Customer will provide reasonable cooperation and assistance to KrispCall.

4. Sub-Processors

Customer acknowledges that KrispCall may involve subprocessors to facilitate its services. A comprehensive list of the Sub Processors currently employed by KrispCall can be found here. By accepting this Data Processing Agreement (DPA), the Customer grants KrispCall the authority to engage the Sub Processors listed on the provided webpage.

4.1 Authorization:

By accepting this Data Processing Agreement (DPA), Customer additionally grants KrispCall to involve other sub processors (add or replace) in the list. KrispCall will promptly inform the Customer of any modifications related to changes in sub-processors.

4.2 Objection Right

Customers have the right to raise objections to KrispCall's selection or replacement of a sub-processor, provided such objections are made in writing and are based on valid data protection concerns. In such a situation, the Customer and KrispCall will engage in good-faith discussions to explore reasonable alternative solutions. If no resolution is reached within 15 days from the date of the Customer's written objection, the Customer may discontinue the use of the affected KrispCall services by providing written notice to KrispCall. Such discontinuation will not affect any fees incurred by the Customer before the discontinuation of the affected services. If no objections are raised prior to KrispCall replacing or appointing a new sub-processor, the Customer will be considered to have authorized the new sub-processor.

5. International Data Transfer Policies

5.1 Data processing Location:

KrispCall hereby assures that the processing of Personal Data under this Data Processing Agreement (DPA) will occur solely within KrispCall's country of operation and in locations specified in the list of KrispCall's Sub Processors in this DPA.

The location and transfer of data may include countries outside the EEA, UK, and Switzerland where data protection laws might differ. KrispCall acknowledges that certain locations referred to as "Locations Subject to Appropriate Safeguards" may not provide the same level of data protection as required by European Data Protection Laws. In such cases, KrispCall commits to implementing necessary measures to ensure compliance with European Data Protection Laws before transferring Personal Data. This includes adopting safeguards to protect data during international transfer

56.2 EU Standard Contractual Clauses

When KrispCall processes personal data transferred from a customer subject to EU GDPR or Swiss FADP, the EU Standard Contractual Clauses for Data Transfers to Third Countries are applied to ensure data protection compliance, even if KrispCall operates in a different region with its own data protection measures. This safeguards the privacy and security of the data during international transfers.

For data transfers falling under the scope of the EU Standard Contractual Clauses, these clauses shall be considered:

- Module one: Transfer controller to control: will apply when the Customer acts as a controller for account usage data.
- Module two: Transfer controller to processor: will apply when the Customer acts as a controller for Customer Content.
- Module three will apply when the Customer acts as a processor of Customer Content.
- Module four will apply when the customer acts as a processor of Customer usage data.

For each applicable Module:

(i) Clause 7 of the EU Standard Contractual Clauses (Docking clause) will apply;

(ii) Clause 9 of the EU Standard Contractual Clauses will apply, and the advance notification period for changes related to subprocessors shall be 10 business days.

(iii) Clause 11 of the EU Standard Contractual Clauses (Redress, the optional language) will not apply;

(iv) Clause 12 of EU Standard Contractual Clauses will apply to the liability terms. However, neither party will limit their liability with regard to data subject rights

(v) In Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Singaporean law;

(vi) In Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved in the courts of Singapore;

(vi) Annex I, Part A of the EU Standard Contractual Clauses will be completed as follows:

1. Contact details of Data Exporter: Customer (Owner user email address)
2. Contact details of Data Importer: KrispCall (legal@krispcall.com)
3. Signature and date: By entering in the agreement, the data importer is automatically bound by the EU Standard Contractual Clauses.

(vii) Annex I Part B of the EU Standard Contractual Clauses will be completed as follows:

1. The categories of data subjects, purposes of data transfer, and data retention periods are all detailed in Section A of this DPA.
2. Transfer of personal data is detailed in Section A; If sensitive data is involved, strict safeguards are applied, including limited use, access restrictions, and maintaining access records.
3. Frequency of data transfer: Continuous basis.
4. Details about the processing and sub-processors are found in the list of sub-processors of the DPA.
5. Signature and date: By entering the agreement, the data importer is automatically bound by the EU Standard Contractual Clauses.

(viii) Annex I Part C of EU Standard Contractual Clauses (Competent Supervisory Authority) The Singapore Data Protection Commission will be the Competent Supervisory authority.

(ix) Annex II encompasses Technical and Organizational Measures, ensuring data security. Details are available in Section B of this DPA.

(x) Annex III pertains to the List of Sub-processors. The data exporter has granted authorization for the use of Subprocessors as outlined in the list.

5.3 UK Data Transfers

This section outlines the application of the UK International Data Transfer Addendum in scenarios where Personal Data is transferred from a Customer subject to the UK GDPR to KrispCall, located in a region with appropriate safeguards and not subject to the UK GDPR.

As allowed by clause 17 of the mentioned addendum, the Parties have mutually agreed to modify the structure of the details presented in Part 1 of the addendum in the following manner:

a) Party details in Table 1 of the UK International Data Transfer Addendum are considered completed with information provided or referenced in the Agreement, including Section 5.2 of this DPA.

b) For Table 2, the UK International Data Transfer Addendum is appended to the EU Standard Contractual Clauses for Data Transfers as defined in Section 5.2 of this DPA. This includes module selection, options, and the exclusion of optional clauses per Section 5.3 of this DPA.

c) Information in Table 3 is considered completed with data provided or referenced in Section 5.2 of this DPA.

d) Parties may terminate this addendum as outlined in clause 19 of the Addendum, with either the data importer or data exporter having the option to do so.

5.4 Singapore Data Transfers

The term "Applicable Data Protection Law" encompasses the Personal Data Protection Act 2012 ("PDPA"). KrispCall will handle personal data in compliance with the PDPA, ensuring a high standard of protection. This includes the implementation of suitable technical and organizational measures outlined in Section 11 of this PDPA (Applicability to Inbound Data Transfers) and strict adherence to the terms specified in the Agreement.

5.5 Australian Data Transfers

The locations outlined in Section 5.1 encompass countries situated beyond the borders of Australia, which may not benefit from the safeguards prescribed by Australian Data Protection Laws. Consequently, the Parties are prohibited from transferring Personal Data governed by Australian Data Protection Laws to any destination outside of Australia, unless they are reasonably assured that the recipient adheres to a legal framework or binding scheme that offers data protection on par with the Australian Privacy Principles. Alternatively, the Parties must demonstrate that appropriate measures have been diligently undertaken to ensure the recipient's compliance with the Australian Privacy Principles, excluding APP1.

5.6 Governing Laws

While adhering to the mandatory application of Applicable Data Protection Laws, and acknowledging their potential mandatory precedence, the regulations within this Data Processing Addendum (DPA) will be subject to and interpreted in accordance with the laws of the country or territory specified in the Agreement for this purpose. Furthermore, both parties agree to accept the chosen jurisdiction as specified in the Agreement concerning any claims or issues arising from or related to this DPA.

5.7 Conflict Resolution

Any conflict or inconsistency arises between the provisions outlined in this Data Processing Addendum (DPA) and the EU Standard Contractual Clauses for Data Transfers to Third Countries, which are integrated herein, the EU Standard Contractual Clauses for Data Transfers to Third Countries will take precedence and govern the matter in question.

To address any disputes related to the interpretation, performance, or termination of this Data Processing Addendum (DPA), both parties agree to engage in negotiations once one party sends a notice about the dispute. If, within thirty (30) days after receiving the notification of the dispute and explicit reference to this provision, the parties cannot reach an amicable settlement by signing

a settlement agreement, the dispute will be brought before the appropriate court with jurisdiction to settle it.

6. Data Breach Notification

In the event of a personal data breach, KrispCall shall cooperate in good faith with and assist the Customer in any way necessary for the data controller to comply with its obligations under Articles 33 and 34 of the GDPR and Article 24 of the FADP, as applicable, taking into account the nature of processing and the information available to the processor.

KrispCall will promptly inform the Customer of any identified Data Breach. If European Data Protection Laws are applicable, KrispCall will ensure to notify the Customer within 24 hours of detecting such a breach. KrispCall commits to offer the Customer full cooperation and support, along with all necessary information regarding the Data Breach.

Further, Customer agrees to furnish KrispCall with all reasonable cooperation and support, as well as pertinent details regarding the Data Breach, necessary for KrispCall to adhere to its obligations under the applicable Data Protection Laws concerning the Data Breach.

7. Updates

This Data Processing Agreement (DPA) will continue to be in effect as long as the Agreement. The customer acknowledges that KrispCall can modify this Data Processing Addendum (DPA) as agreed for changes to the main Agreement, and KrispCall may update terms and policies at its discretion, with prior notice to the Customer.

Section A

Detail of Processing

Nature and Purpose of Processing

KrispCall will handle personal data exclusively for the purpose of providing the services as specified in the Agreement. KrispCall confirms that it does not engage in the sale of Customer's personal data or the personal data of Customer end users, and it does not share such data with third parties in return for compensation or for the business interests of these third parties. KrispCall will process customer data in accordance with this DPA.

Processing Activities

KrispCall engages in various processing activities that are crucial for the operation and functionality of its services. These activities are conducted with a strong commitment to data protection and in compliance with relevant legal frameworks.

- **Data Switching:** KrispCall facilitates the transfer of personal data between Public Switched Telephone Network (PSTN) and Voice over Internet Protocol (VoIP) networks. This process is fundamental to enabling seamless communication.
- **Data Storage:** Personal data is securely stored within KrispCall's backend infrastructure. Stringent security measures are in place to safeguard this data.
- **Data Processing:** KrispCall processes data for various purposes, including visualization and personalization settings. This processing is essential for providing a tailored and user-friendly experience.
- **Data Monitoring:** KrispCall continually monitors data streams to proactively identify and address potential errors or issues, ensuring the reliability of its services.
- **Statistical Analysis:** User data is analyzed to generate comprehensive statistics, which are made available on the platform's dashboard. This analytical insight aids users in understanding their usage patterns.
- **User Account Management:** KrispCall is responsible for creating and maintaining user accounts, including the allocation of phone numbers to users. This process ensures proper access and identity management.
- **Identity Verification:** In compliance with local regulations, KrispCall conducts client identity verification when necessary for the provision of telephone numbers. Additionally, an identity validation stamp may be created for future number procurement in the same location.
- **Call Routing:** KrispCall manages call routing processes and conducts manual analysis of call logs to maintain service quality and promptly address any issues.
- **Issue Resolution:** Data extracted from API sources is analyzed to detect and resolve system crashes and bugs, thereby enhancing service reliability.
- **Communication Content Analysis:** KrispCall may analyze communication content to provide users with deeper insights into their conversations, particularly for customers who have subscribed to AI Features.
- **Integration with Other Tools:** KrispCall integrates its product with various third-party tools. This entails sharing customer personal data with integration partners when users install and authorize these integrations. Data transfers between KrispCall and the respective tool providers are limited to processing within the KrispCall environment.

These processing activities are vital for delivering high-quality services, ensuring data security, and meeting the needs of KrispCall users while upholding legal and regulatory compliance.

Categories of Data Subjects

The categories of data subjects whose personal data may be processed by KrispCall include: representatives of customers, end users, their contacts, and individuals involved in communication via KrispCall SMS/Call sender, caller, recipients, employees, and agents.

Category of Data

1. **Customer Account Data:**
    - **Customer Contact Information:** Includes the customer's contact name, phone number, and email address.
    - **Customer Identification:** Includes the customer's unique KrispCall ID and their legal business name.
    - **Financial Details:** Includes the customer's tax number and billing address.
    - **Contract Information:** Contains details such as pricing plans, additional terms, subscription date, and order forms.
2. **Customer Contact Data:**
    - **Contact List Information:** Consists of contact names, telephone numbers, the owner of the contact, and contact profile pictures.
3. **User Information:**
    - **User Details**: Includes a user's unique ID, their metrics (e.g., first call, last login, call history), and their role (e.g., user or admin).
    - **User Communication:** Contains information about the user's name, contact numbers, device details, and communication history.
    - **Location and Contacts:** Includes the user's location and contact book, retrieved from their device.
4. **Call/SMS Content:**
    - **Communication Content:** Comprises call recordings, voicemails, SMS messages, and voice transcriptions.
5. **Call/SMS Metadata:**
    - **Communication Metadata:** Encompasses call and SMS details such as call transfers, date and time, recipient and caller numbers, call duration, and whether calls were answered or missed.
6. **Additional Call-Related Data:**
    - **Supplementary Information:** Contains call notes, call tags, and call insight cards that provide additional context and details.
7. **Customer Identity Verification Data:**
    - **Identity Verification:** Involves customer-specific data, including physical address, birthdate, city and country of birth, parental names, nationality, personal ID type, and number, issuing authority, issuing date, representative job position, VAT number, and identity validation stamp.
8. **Customer-Provided Documentation:**
    - **Document Verification:** Includes scanned copies of customer ID, passport, proof of address, and proof of business documents provided by the customer or their representatives for verification purposes.

These data categories pertain to KrispCall's operations and the management of customer and user information within the platform. Handling and protecting this data should align with data protection regulations and best practices for user privacy and security.

Duration Of Data processing

The period for which personal data will be retained and the criteria used to determine that retention period can vary based on the specific data and the legal, regulatory, and business requirements of the organization.

- Data processed solely for the customer will be retained for the term agreed in the DPA unless the customer requests earlier deletion.
- Data needed for phone number provision will be retained until 15 days of post-termination.
- All data processed solely for the customer will be deleted on termination, after the return/deletion period.
- Data processed by KrispCall as a controller will follow retention in KrispCall's Privacy Policy.

Section B

Security & Compliance

Security and Compliance are our top priorities; therefore, we constantly improve our security every single day. Your data and VoIP services are safe with us in our modern data centers with 24/7 monitoring. To protect your data and communication, we have designed our product according to the highest security standards, capable of monitoring security threats and identifying relevant security patches.

We are committed to never disclosing your confidential information to third parties under any circumstances. You can always rest assured that your data is always safe with us.

Security measures adopted by KrispCall

Security Certification:

KrispCall has instituted effective technical and organizational security protocols to ensure the protection of your data. This encompasses data encryption, SOC 2 Type II certification, and adherence to ISO Standards.

Permissions:

Assign specific roles to each of your agents so that they are required to use their own accounts to access the services of KrispCall.

Data Encryption:

KrispCall takes reasonable and appropriate measures to protect your personal data, which includes encrypted data transfer (HTTPS). The protocol encrypts all the data sent via the websites. Phone calls made through KrispCall are also encrypted during the transfer from agents to KrispCall.

Backups:

Backups are required to be performed and stored in a secure location. Besides, data acquired by KrispCall are spread across several available zones so that KrispCall will continue to work if any of them fail.

Audits

Customer and KrispCall recognize that Customer should have the ability to evaluate KrispCall's adherence to its responsibilities under the Applicable Data Protection Laws and this Addendum, particularly when KrispCall acts as a data processor on behalf of Customer. The customer may audit KrispCall's data processing practices if:

(a) The customer provides reasonable grounds to believe KrispCall breached the DPA or laws, or a breach occurred

(b) A regulatory authority formally requests an audit

(c) Applicable law grants the customer a direct audit right

Audits may use an independent third-party auditor, provided they are suitably qualified and not a KrispCall competitor. Customer may conduct an audit at a maximum frequency of once every twelve months unless the Applicable Data Protection Laws necessitate more frequent audits.

The Customer must give at least thirty days' notice in advance of any audit unless a mandatory Data Protection Law or a competent data protection authority mandates a shorter notice period. Each Party will be responsible for covering its own costs related to audits under this agreement.