Law Enforcement Data Request Guidelines

KrispCall is committed to protecting customer privacy while complying with valid legal requests from law enforcement agencies. Please refer to the following guidelines for the submission and processing of such requests.

Definitions

- **Authority:** Any law enforcement agency, government body, or regulatory authority legally empowered to request data.
- **Valid Request:** A request that meets all specified requirements under these guidelines.
- **Urgent (Emergency) Request:** A request related to an imminent threat, such as the risk of death or serious physical harm.
- **Preservation Request:** A request for KrispCall to temporarily retain specific records pending further legal action.

Submission Point

Kindly forward your official request to the KrispCall Legal Team at **legal@krispcall.com**. Requests must be submitted in **PDF format** and originate from the official email domain of the Authority.

KrispCall may reject requests that are incomplete, vague, or improperly formatted.

Requirements of Requests

At KrispCall, we diligently verify the authenticity of all requests received from Law Enforcement Authorities or Government Agencies ("Authorities"). We exclusively entertain requests that are precisely issued in our company's name by duly authorized Authorities without any validity issues.

A valid request must encompass the following essential details (Validity Characteristics):

- Precise identification, including the name and physical address (excluding P.O. boxes) of the Authority.
- Comprehensive contact information of the designated Authority's representative, comprising their full name, phone number (inclusive of extension), and an official government-issued email address.
- Clear identification through the badge or identification number of the Authority's representative.
- If applicable, the inclusion of a reference or case number.
- A transparent specification of the categories of records or information being sought.
- A well-defined timeframe for which the information is requested.
- Explicit identification of the phone number linked to the KrispCall account subject to the request.
- The legal basis or grounds for submitting the request.
- A date and a valid signature from the Authority's representative.
- A clear stipulation of the desired response date.

KrispCall retains the right to request supplementary information for verification or effective handling of the request.

The specific information required by the Authority may vary, depending on a reasonable interpretation of the request by the KrispCall Compliance Team. Therefore, it is imperative for the Authority to provide precise and accurate details when formulating their request.

Response Time

KrispCall endeavors to provide responses to valid requests within a 1 week time frame. Nevertheless, in instances where requests are intricate, expansive, or necessitate additional verification, the response time may be extended. Please be aware that requests submitted to KrispCall via postal mail may have significantly longer response times.

Should you require an expedited response, kindly specify the relevant deadline explicitly in your request.

Urgent (Emergency) Requests

In circumstances where there is an imminent threat, such as the risk of death or severe physical injury to an individual, KrispCall may prioritize the provision of information to prevent or

mitigate such danger. Urgent (emergency) requests will be evaluated on a case-by-case basis in accordance with applicable laws.

In addition to the standard Validity Characteristics, urgent (emergency) requests should fulfill the following criteria:

- Be grounded in a genuine belief of an imminent threat, such as the risk of death or severe physical injury to a person.
- Include a detailed description of the emergency's nature and a rationale for the perceived immediacy of the threat.
- Articulate how the requested information will aid in averting the threat and explain why the standard disclosure process would be insufficient.

These requests must be in written form (submitted via email) and originate from the official email domain of the requesting Authority.

For urgent (emergency) requests, please direct them to the designated EMAIL address, ensuring the subject line includes 'EMERGENCY' or ‘URGENT’.

Notification to Customers

KrispCall reserves the right to inform customers of valid requests received, enabling them to respond directly unless applicable laws, regulations, court orders, or other legal instruments prohibit KrispCall from doing so.

Types of Requests

1. **Data Requests:**

A Data Request pertains to inquiries for information regarding a KrispCall customer account as part of an official criminal, administrative, or civil proceeding. Acceptable legal processes to support a Data Request include, but are not limited to, subpoenas, court orders, search warrants, and civil investigative demands. Such requests may originate from government agencies, law enforcement bodies, or private parties.

2. **Preservation Requests:**

KrispCall may, upon receiving a valid preservation request, retain specified records for up to **90 days** pending further legal process. If no follow-up documentation(e.g., subpoena, court order) is provided within this period, the preserved data may be securely deleted unless an extension is legally required.

3. **Expedited Requests:**
Requests that require prompt handling must specify the required deadline and be supported by proper justification.

Data Disclosures & Legal Process Requirements

KrispCall will disclose customer data only when a valid legal process is provided. The data disclosed is strictly limited to the following categories, each subject to the corresponding legal standard:

- Customer Information

Includes identifying details such as the customer's name, contact information, and billing address, Email address(es). Disclosure is permitted only upon receipt of a **valid subpoena** issued by a competent authority within KrispCall's operational jurisdiction.

- Call Logs and Metadata
  Includes records of call activity, durations, and related metadata. Disclosure is permitted only upon receipt of a **valid court order**.
- Content Data
  Includes voicemails, call recordings, and text message content. Disclosure is permitted only upon receipt of a valid search warrant or equivalent legal instrument. KrispCall reserves the right to evaluate the nature, scope, and seriousness of the request and may, at its sole discretion and in accordance with applicable laws, determine whether to provide the requested data after assessing the circumstances.
- Other Data
  Includes any other data not specified above. Disclosure is permitted only upon receipt of a **valid legal instrument** that explicitly authorizes its release.

KrispCall reserves the right to evaluate requests for overbreadth, ambiguity, or improper jurisdiction and may challenge such requests to protect customer privacy.

Data Handling and Security

KrispCall employs strict data security measures when disclosing information, including encryption and access controls, to protect customer data from unauthorized access.