GOVERNMENT REQUESTS GUIDE

Last updated: January 1st, 2021

TELAWORKS supports the free and open exchange of thoughts and ideas. We are proud to facilitate meaningful conversations and professional collaboration around the world. TELAWORKS provides a high-quality portal to domestic and cross-border communication that, in some places, we understand might not otherwise exist. We take this responsibility and the privacy, security and safety of our users and their data extremely seriously.

Accordingly, TELAWORKS will subject any government request to a careful and thoughtful review, prioritizing the privacy, security, and safety of our users and their information at all times.

In all geographies:

- Government requests must be issued pursuant to applicable laws and rules and through official channels, including by requiring an official, signed document, or a request by email sent from the official email address of a government entity.
- Each request must be clear, not overly broad, and have a valid legal basis.
- We will reject or challenge requests that do not meet these requirements.
- We will apply additional scrutiny to certain government requests for user information based on our principles and interest in promoting meaningful collaboration around the world, as described below.

This Guide is intended for government authorities seeking information from TELAWORKS about our users, accounts, and services. Nothing within this Guide is meant to create any enforceable rights against TELAWORKS and our policies may be updated or changed in the future without further notice to government authorities.

What types of data does TELAWORKS have?

We obtain data that users provide to us, as well as data that our system collects. We may also obtain some data from visitors to our marketing websites. For more information, please see below and visit our privacy policy.

We have not built a mechanism to decrypt live meetings for any purpose, including lawful intercept, and we do not have the means to insert our employees or others into meetings without that person being visible as a participant. As such, we do not collect or maintain information related to meeting content unless requested by the meeting host, for example, to record and store the meeting in our cloud.

TELAWORKS does not sell user data and we have no intention of selling user data going forward.

Data that users provide to TELAWORKS:

Depending on whether or not a user has a registered TELAWORKS account and which product or service is used, we may collect the following data from our users, which we may or may not retain depending on the type of data and our applicable retention policy:

- **Identifying information:** including, name, username, email address, or phone number, as well as account owner name, billing name and address, and payment method (we do not store any user credit card information);
- **Other account data***:* including language preference, hashes of the password, title, department, profile photo; and
- **User content**: that a user chooses to store to the cloud or provide to us, including cloud recordings, transcripts, chat and instant messages, files, and whiteboards.

We cannot determine or guarantee the accuracy of information provided by our users. Unless required by local law, we do not require real-name use or identity authentication to create a TELAWORKS account or join a meeting.

Data that TELAWORKS collects about users and its products and services:

Depending on whether or not a user registered an account with TELAWORKS, the TELAWORKS product used, and the method of user access, our system may collect the following data about users and products and services, which we may or may not retain depending on the type of data and our applicable retention policy:

- **Technical information**: about a user's device, network, and internet connection, including the user's IP address, MAC address, other device ID (UDID), device type, how the user connected, network performance, operating system type and version, client version, type of camera, microphone, or speakers;
- **Approximate location**: to the nearest city;
- **Metadata**: including duration of the meeting; email address, name, or other information that participants enter to identify themselves in a meeting, join and leave time of participants, meeting name, the scheduled date and time of a meeting.

TELAWORKS data retention practices:

We retain different types of information for different periods of time, and in accordance with our Terms of Service, Privacy Policy, and retention policies. Some stored information is collected automatically, while other information is provided at the user's discretion. For example, meeting metadata is automatically captured when a participant joins a meeting, whereas communications that occur during meetings are encrypted and cannot be accessed by TELAWORKS. More information on the data we may collect may be found in our privacy policy.

Our account owners and administrators can delete discretionary content such as cloud recordings and chat logs (text messages, photos, and files). Once an account owner or administrator deletes this content, we cannot retrieve this data.

We may facilitate the deletion of personal data pursuant to data subject rights available to users, if directed to do so by our users, or as required by law. More details concerning how we address data subject requests can be found in found in our privacy policy.

Once an account has been deactivated, there is a brief period in which we may be able to access account information and content if stored on our cloud.

Preservation requests:

We accept requests from government authorities to preserve records that potentially constitute relevant evidence in legal proceedings. We will preserve, but not disclose, a temporary snapshot of the relevant records for 90 days pending service of the required legal process. A preservation request will not result in our recovering user data that has already been deleted.

Preservation requests, in accordance with applicable law, should include the following information:

- The name and signature of the requesting official;
- A valid, government-issued email address;
- Official letterhead; and
- Identify the specific information you are requesting to be preserved, including, at a minimum:
    - For user records, the user's display name, email address, or IP address;
    - For account records, the account owner's email address or account number;
    - For meeting records, the meeting ID, the meeting host's email address and meeting date and time, or the meeting registration URL.

Preservation requests - continued:

We encourage government agencies to seek records with a formal request through the appropriate process promptly, as we cannot guarantee that requested information will be available. The preserved records may be deleted unless the requestor has provided a formal request through the required process within 90 days. The 90-day period may be extended for an additional 90-day period, if requested, by submitting a separate, formal extension request on government letterhead.

Government preservation requests may be submitted to: info@telaworks.com

U.S. Government requests for user information:

Requests from all government authorities must be issued pursuant to applicable laws and rules and through official channels, including by requiring an official, signed document, or a request by email from the government (provided these are transmitted from the official email address of a government entity). Please send all requests to info@telaworks.com.

With any request, we will undertake a legal review to determine if the request is legally valid (i.e., if it is made in circumstances where it has some particularized legal basis in the U.S. and pertains to the bona-fide prevention, detection, or investigation of offenses). If the request is legally valid and satisfies our other requirements, we will disclose user, account, and records associated with our products and services, if available, in accordance with and subject to applicable law. In the circumstance where we believe that there is no valid legal basis or that the request is vague or overbroad, TELAWORKS will challenge or reject the request.

Requests requiring a subpoena or court order:

A subpoena or court order, depending on the type of information requested, is required to compel the disclosure of user, account, and meeting data (not including contents of communications), which, if available, may include: name, email address, phone number, meeting metadata, IP address, MAC address, other device ID (UDID), and approximate location.

Requests requiring a search warrant:

A search warrant issued upon a showing of probable cause is required to compel the disclosure of a users' stored content data, which may include cloud recordings, transcripts, chat/instant messages, files, whiteboards, and other information shared while using our services.

Requests for real-time interception or monitoring of user meeting content:

We have not built a mechanism to decrypt live meetings for any purpose, including lawful intercept, and do not have the means to insert our employees or others into meetings without that person being visible as a participant.

International government requests for user information:

Requests from all government authorities must be issued pursuant to applicable laws and rules and through official channels, including by requiring an official, signed document, or a request by email from the government (provided these are transmitted from the official email address of a government entity). Please send all requests to info@telaworks.com.

As with any government request, we consider a foreign government request to be legally valid if it has some particular legal basis in the domestic law of the requesting country and pertains to the bona-fide prevention, detection, or investigation of offenses. A Mutual Legal Assistance Treaty request, a request from a country meeting the obligations under the CLOUD Act or letters rogatory may be required to compel the disclosure of information. In the circumstance where we believe that there is no valid legal basis or that the request is vague or overbroad, TELAWORKS will challenge or reject the request.

Importantly, we will further scrutinize all international government requests on a country-by-country and case-by-case basis in order to consider and balance our local legal obligations against our basic principles described above, including our commitments to promoting the free and open exchange of ideas, keeping our users safe, and protecting our users' privacy. We may choose to respond differently to information requests from different countries where our principles with respect to the meaningful exchange of ideas and collaboration conflict with local law. Key factors we will consider include whether we have a good faith belief that the request involves child sexual exploitation material or an emergency involving danger of death or serious physical injury to any person. We will also limit our response to only the user or meeting data deemed necessary to prevent these harms.

International government agencies may also submit requests in English to: info@telaworks.com. We cannot guarantee a response to requests in languages other than English. A request under the Mutual Legal Assistance Treaty or letters rogatory may be required to compel the disclosure of information.

Will TELAWORKS notify users of requests for user or meeting information?

Yes. Our policy is to notify users of requests for their information, which includes a copy of the request unless we are legally prohibited from informing the user (e.g., an order under 18 U.S.C. § 2705). We ask that any non-disclosure requests include a specified duration (e.g., 90 days) during which we are prohibited from notifying the user. Requests for exceptions to user notice should include a description of the exigent circumstances or potential adverse result of notice. We will evaluate each request on a case-by-case basis in accordance with applicable laws and our Privacy Policy. Where appropriate, we will reject requests, and provide reasons for the rejection. If necessary, we will also challenge requests in court.

If the request draws attention to an ongoing or prior violation of our Terms of Service, Privacy Policy, or other applicable policies, guidelines or legal requirements, we may take action to address such violations or prevent further abuse, including actions that could (explicitly or implicitly) notify the user that we are aware of the user's misconduct.

What details must be included in requests for user, account, or meeting information?

Requests for user, account, or meeting information, in accordance with applicable law, are required to include the following information:

- Identify the specific information you are requesting, including, at a minimum:
    - For user records, the user's display name, email address, or IP address;
    - For account records, the account owner's email address, or account number;
    - For meeting records, the meeting ID, the meeting host's email address and meeting date and time, or the meeting registration URL; and
- Details about what specific information is requested and its relationship to your investigation.

We are unable to process overly broad or vague requests.

To enable us to verify that a data request is from an official government authority, we require that each request include at least the following information:

- Requesting Agency's Name;
- Requesting Agent's Name;
- Requesting Agent's Badge/Identification Number;
- Requesting Agent's Employer-Issued Email Address;
- Requesting Agent's Telephone Number (including extension);
- Requesting Agent's Mailing Address (P.O. boxes will not be accepted);
- Requested Response Date (please allow at least 2 weeks for processing); and
- Signature of the requesting official.

Production of records:

Unless otherwise agreed upon, we currently provide responsive records in electronic format (i.e., .csv, .docx, .mp4). We may seek reimbursement for the costs associated with information produced pursuant to legal process and as permitted by law. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests.

User consent:

If a government official is seeking information about a TELAWORKS user who has provided consent for government authorities to access or obtain the user's account or meeting information, the user should be directed to provide the requested information to the official to the extent possible.

Emergency requests:

We evaluate emergency requests on a case-by-case basis. If we have a good faith belief that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency, we may provide information consistent with our privacy policies and applicable law (e.g., 18 U.S.C. § 2702(b)(8) and (c)(4)). We do not commit to producing records under any set of circumstances or within a particular timeline and may request additional information to verify the nature of the request and/or the identity of the person making the request.

Emergency requests should be submitted to: info@telaworks.com with the subject line "EMERGENCY DISCLOSURE REQUEST" and include all of the following information:

- Requesting Agency's Name;
- Requesting Agent's Name;
- Requesting Agent's Badge/Identification Number;
- Requesting Agent's Employer-Issued Email Address;
- The detailed nature of the emergency involving death or serious physical injury, including how you learned of the threat, links to social media posts, chat logs, etc.;
- Identify whose death or serious physical injury is threatened;
- Describe the imminent nature of the threat, including information that suggests there is a specific deadline before which it is necessary to receive the requested information; and/or that suggests there is a specific deadline by which the harm will occur (*g.*, tonight, tomorrow at noon);
- Identify the specific information you are requesting from TELAWORKS (narrowly tailor your request – requesting all information associated with a user, account, or meeting may delay processing of your request), including, at a minimum;
    - For user records, the user's display name, email address, or IP address;
    - For account records, the account owner's email address or account number;
    - For meeting records, the meeting ID, the meeting host's email address and meeting date and time, or the meeting registration URL; and
- Explain how the information you are requesting will assist in averting the specified emergency.

Requests for TELAWORKS to restrict access to services on our platform:

- Many countries, including the United States, have laws that may restrict one or more of its residents from participating in or hosting particular TELAWORKS meetings or webinars. We will carefully review any government requests demanding we shut down a meeting and/or restrict user access to TELAWORKS. If we receive a legally valid, appropriately scoped, and sufficiently detailed request from a legitimate government agency, we may take action to limit participation from the appropriately scoped jurisdiction. We will reject or challenge requests that do not meet this standard.
- We strive to limit the actions we take to only those necessary to comply with our legal obligations. Accordingly, TELAWORKS will not shut down a meeting unless it violates TELAWORKS Terms of Service, including instances of child sexual exploitation materials or the danger of death or serious physical injury. Apart from determining a violation of our Terms of Service, we will not prevent our users from accessing our services if they are outside of the jurisdiction of the requesting government agency, or if they are not subject to applicable local law.
- Unless prohibited by law, we will attempt to notify those named in a request to restrict access. We will send notice to the email address associated with the user's account, along with the opportunity to challenge any decision regarding the account.
- Except for the circumstance where we receive a request from a legitimate government agency and we have a good faith belief that an emergency involving danger of death or serious physical injury to any person (a process for which will be outlined with governments directly), government personnel outside of the United States transmitting requests to restrict access should transmit it directly from their official government email address to: info@telaworks.com.

Expert witness testimony and authentication of records:

We do not provide expert testimony support, except to the extent required by applicable laws and regulations. Pursuant to law, our records are self-authenticating and should not require the testimony of a records custodian. If a special form of certification is required in your jurisdiction, please attach it to your records request.

Submission of requests:

All requests for data and information, preservation requests, preservation extension requests must be submitted to: info@telaworks.com. We will not accept and will promptly delete any emails not sent from an official government email address. Please include all applicable information in the email and attach all necessary legal documents to the email in PDF format. We will not accept any legal documents that are unsigned or attached to the request as an image.