Privacy Policy

This Privacy Policy describes how we collect, use and share your personal data when you use our services or otherwise interact with us. This Privacy Policy covers your rights and choices regarding how we process your personal data and your right of access and correction of your personal data. If you do not agree with our policies and practices, please do not use our services or interact with any other aspect of our business.

Information We Collect About You

When you visit, use, or navigate our services, we may process your personal data depending on how you interact with us and our services, the choices you make, and the products and features you use.

The personal data we collect may include the following:

- names
- email addresses
- domain and user names
- device data (such as device ID, device name, operating system and IP address)
- usage data

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

We automatically collect certain information when you visit, use, or navigate the services. This information may include your name and email address, device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, browser type, hardware model, country, location, information about how and when you use our services, and other technical information. This information is primarily needed to maintain the security and operation of our services, and for our internal analytics and reporting purposes.

We may collect information through cookies and similar technologies to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

Usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called “crash dumps”), and hardware settings).

How We Process Your Personal Data

We process your data to provide, improve, and administer our services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your prior consent.

We process your personal data for a variety of reasons, depending on how you interact with our services, including:

a) to provide our services

We process your personal data to provide you with the requested services. For example, we process your personal data to facilitate account creation and authentication and otherwise manage user accounts. We may process your data so you can create and log in to your account, as well as keep your account in working order.

b) to improve and develop our services

We process data about how you interact with our services. For example, we may use usage data to identify usage trends and process the data to better understand how our services are being used for development and improvement purposes.

c) for security and fraud prevention

We process your personal data to protect our services. We may process your information as part of our efforts to keep our services safe and secure, including fraud monitoring and prevention.

d) for marketing and promotional purposes

Upon registration to our services, we process your contact information and data about how you interact with our services in order to send marketing and promotional communications that may be of specific interest to you via email. These communications may include information about new services, offers and promotions.

Legal Basis For Processing Your Personal Data (for EU/EEA and UK users)

If you are a user located in the European Union ("EU")/European Economic Area ("EEA") or the United Kingdom ("UK"), this section applies to you. We process your personal data only where we have legal basis for doing so under the General Data Protection Regulation no 2016/679 ("GDPR") and UK's Data Protection Act.

The legal basis for processing your personal data described above, will depend on the personal data concerned and the specific context in which we process it. We may rely on the following legal bases to process your personal data:

- *Consent*. We may process your information if you have given us your consent to use your personal information for a specific purpose. You can withdraw your consent at any time.

- *Legitimate Interests*. We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not outweigh your interests and fundamental rights and freedoms. For

example, we may process your personal information for some of the purposes described in order to:

- Analyse how our Services are used so we can improve them to engage and retain users
- Diagnose problems and/or prevent fraudulent activities

- *Legal Obligations*. We may process your data where we believe it is necessary for compliance with our legal obligations, such as to respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.

- *Performance of a contract*. We may process your information when it is necessary to provide you the services, including to provide customer support and to protect the safety and security of the services.

How We Disclose Your Personal Data

We may share your data with third-party vendors, service providers, contractors, or agents ("third parties") who perform services for us or on our behalf and require access to such information to do that work. For protection of your personal data, we have contracts in place with our third parties. This means that they cannot do anything with your personal data unless we have instructed them to do it. They will also not share your personal data with any organisation apart from us unless instructed by us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct. Here below is a list of our Sub-Processors.

- Google Cloud Platform - for cloud computing services
- Sendgrid - for emailing
- Zendesk - for helpdesk
- Google Analytics - for web and mobile analytics

How We Store and Secure Your Personal Data

In relation to your personal data, we have implemented appropriate technical and organisational measures to ensure a level of security appropriate to risk, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR.

Your personal data is encrypted at rest in Google Cloud Platform, using Google encryption keys. Your personal data is only accessible through a bastion host, designed and configured to withstand attacks from external networks.

We employ least privilege access mechanisms to control access to your personal data. Role-based access controls are employed to ensure that access to personal data required for service operations is for an appropriate purpose and approved with management oversight.

Third party penetration testing of our systems is carried out yearly in order to identify security vulnerabilities and mitigate risk. We employ a point-in-time restore of data.

In assessing the appropriate level of security, we take into account in particular the risks that are presented by processing, especially from a Personal Data Breach.

How Long Do We Keep Your Information?

How long we keep your personal data, depends on the type of data and how we process it. We will only keep your personal data for as long as it is necessary for the purposes set out in this privacy policy and our legitimate business interests, such as where a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements).

When we have no ongoing legitimate business need to process your personal data, we will either delete or anonymize such data, or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your personal data and isolate it from any further processing until deletion is possible. As described in the section below, “Your Privacy Rights and Choices”, your personal data will be deleted at an earlier date, if you request us to do so.

Your Privacy Rights and Choices

You have certain rights and choices regarding our processing of your personal data.

You have the right to:

- access, rectification or erasure of your personal data
- restrict processing of your personal data
- data portability
- object to the processing of your personal data
- withdraw your consent
- complain to a data protection authority

If you want to exercise your rights, you can do so by contacting us. You can find our contact details below, in the section “How To Contact US?”. We will consider and act upon any request within a reasonable timeframe in accordance with applicable data protection laws and notify you of the action we have taken.

If you believe we are unlawfully processing your personal data, you have the right to complain to your local data protection supervisory authority. You can find the contact details for data protection authorities in the EEA here: https://edpb.europa.eu/about-edpb/about-edpb/members_en

If we are relying on your consent to process your personal data, you have the right to withdraw your consent at any time. However, please note that this will not affect the

lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal data conducted in reliance on lawful processing grounds other than consent.

Upon registration to our services, please be advised that you may receive marketing and promotional communications from us via email. You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, or by contacting us using the details provided in the section “How To Contact US” below. You will then be removed from the marketing lists. However, we may still communicate with you — for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

If you would at any time like to review or change the information in your account or terminate your account, you can do so by logging in to your account settings and update your user account.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

How We Transfer Your Personal Data Internationally

As we operate globally, we may need to transfer personal data to countries outside of where the personal data was originally collected. We are headquartered in the U.S. and if you are located outside the U.S., we may transfer your personal data outside of the country you reside, to the U.S. or other countries, between our group companies or between us and our third-party providers, for the purposes described in this Privacy Policy. We offer data residency within the EU/EEA or within the U.S. in accordance with our customer’s choosing.

We will protect your personal data in accordance with this Privacy Policy wherever it is processed. If we share personal data of individuals located in the EEA, Switzerland or the UK between our group companies and between us and our third-party providers we have implemented measures to protect your personal data, including by using the Standard Contractual Clauses (approved by the European Commission and Swiss authorities) as well as the UK Addendum to the Standard Contractual Clauses (approved by the UK authorities) as well as additional safeguards where appropriate. When transferring personal data to the U.S., from the EEA, the UK and Switzerland, we adhere to the Data Privacy Framework Program. Please find further information in the section “Data Privacy Framework Notice” below.

Certain third-party vendors, service providers, contractors, or agents who process your personal data on our behalf may also transfer your personal data outside the country in which you are resident. To protect your personal data, we will make sure that an appropriate transfer agreement is put in place. Our Sub-Processors are listed in the section “How We Disclose Your Personal Data” above.

Data Privacy Framework Notice

Keystrike Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Keystrike Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Keystrike Inc. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/

If you are located in the EU, UK or Switzerland, you have the right to request access, rectification or deletion of your personal data. Further, you have the right to object to the processing of your personal data, such as if Personal Data we control about you is to be disclosed to an independent third party or used for purposes that are materially different from those set out in this Privacy Policy. If you want to exercise your rights, you can do so by contacting us. You can find our contact details below, in the section “How To Contact US?”.

In compliance with the DPF Principles, we commit to resolve DPF Principles-related complaints about our processing of your personal Data. We will investigate and strive to resolve any DPF Principles-related complaints within 45 days. If individuals located in the EEA, the UK or Switzerland have inquiries or complaints regarding our processing of personal data received in reliance on the DPF Principles, they should first contact us.

We commit to refer unresolved complaints concerning our handling of personal data received in reliance on the DPF to an alternative dispute resolution provider based in the U.S. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

As further described on the DPF website, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted. The Federal Trade Commission has jurisdiction over our compliance with the DPF Principles.

If we transfer data received under the DPF Principles, to a third party acting as our agent, we assume responsibility for processing of the Personal Data. If our agent handles your Personal Data in a manner inconsistent with the DPF Principles, we will remain liable, unless we are not responsible for the specific event that caused the damage.

Please be aware that, under certain circumstances, we might be required to disclose your Personal Data in response to lawful requests by public authorities. This includes instances where disclosure is necessary to fulfil national security or law enforcement requirements.

Changes to our Privacy Policy

This Privacy Policy will be updated continuously so that it is always up-to-date. If the changes are significant, we will notify you through the service and/or by e-mail. Your continued use of the service following the amendment will confirm your consent thereto.

How To Contact Us

If you have questions or comments regarding this Privacy Policy, you may contact us by email at privacy@keystrike.com, or by post to:

KeyStrike Inc.,
att. Valdimar Oskarsson, CEO
8 The Green, Suite # 1128,
Dover, DE 19901,
Kent County,
Delaware USA

or to our establishment in the EEA:

KeyStrike ehf.
att. Valdimar Oskarsson, CEO
Urdarhvarf 8
203 Kopavogur
Iceland