

Data Privacy Framework (“DPF”) Program Notice

Effective 12th November 2025

This policy

CafeX Communications Inc. and its affiliates (the “Company,” “We” or “Us”) offer a hosted service that enables our business customers (“Customers”) who subscribe to our communication technology and/or other engagement technology services (“Online Services”) to better communicate and interact with, and deliver content to, visitors to their websites and other prospective customers (“Users” or “You”) in real-time via co-browse, voice, video and other communication and delivery methods. In this policy “DPF” refers to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Who are we?

CafeX creates software that makes it amazingly simple for people to collaborate in ways that work best for them.

In this policy “CafeX”, ‘we’, ‘us’ or ‘our’ means;

CafeX Communications Inc. 1460 Broadway, Suite 9054, New York, NY 10036

Data Privacy Framework

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), 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.

We have officially attested to the U.S. Department of Commerce our strict adherence to the Data Privacy Framework (DPF) Principles concerning the handling of personal data.

In the event of any discrepancy between the provisions outlined in this privacy policy and the DPF Principles, it is the Principles that will take precedence and govern.

For further information about the Data Privacy Framework (DPF) program, as well as to access our certification, please visit <https://www.dataprivacyframework.gov/>.

Sharing Data with Third Parties

We collaborate with a limited selection of third-party partners and service providers to facilitate the availability of our websites and Online Services. These partners and service providers, in the course of delivering their services (such as invoice processing), may access, handle, or securely store personal data. We exclusively share personal information with partners and service providers who share our unwavering commitment to privacy and security. Moreover, we maintain contractual agreements that restrict the usage and divulgence of personal data.

In the event that one of these partners or service providers processes personal data in a manner inconsistent with the Data Privacy Framework, we bear liability unless we can demonstrate that we are not responsible for the incident leading to the damage.

It is important to note, however, that we may be compelled to disclose personal data in response to lawful requests by governmental authorities, including those related to national security or law enforcement obligations.

Information We Collect

In the course of utilizing our Online Services, there may be a necessity to provide certain information to facilitate the smooth operation of these services. This information may include personal details like your name, address, email, or telephone number. It is essential to obtain this information, for instance, in order to process payments or to enable integrations of software components.

Furthermore, we may gather information related to your internet connection, which encompasses your IP address and the equipment you employ (such as the specific web browser or mobile device in use), as well as usage particulars. In addition to this, we utilize cookies and other advanced technologies to automatically collect and securely store data that is generated as you interact with our service. This data encompasses your preferences and anonymous usage statistics.

It's important to note that, while utilizing our Online Services, data is stored securely at rest, employing advanced AES 256-bit key encryption.

Rights to Access, Limit Use and Limit Disclosure

Individuals covered by this policy have rights to access personal data about them, and to limit use and disclosure of their personal data. Because our personnel have limited ability to access personal data our Customers submit to the Online Services,

if a User wishes to request access to or to limit use and/or disclosure of his/her/its personal data, please contact Us at compliance@cafex.com with the name of Our Customer through which the User used the Online Services. We will refer the request to that Customer, and will support them as needed in responding to the request.

Inquiries, Enforcement and Resolution

In accordance with the DPF Principles, we pledge to address complaints that pertain to DPF Principles. Individuals seeking information or wishing to express grievances concerning our management of personal data are encouraged to initially reach out to compliance@cafex.com.

We are subject to the investigative and regulatory authority vested in the Federal Trade Commission (FTC). We are obligated to engage in arbitration proceedings and adhere to the stipulations delineated in Annex I of the DPF Principles, on the condition that you have initiated binding arbitration by providing formal notice to us and have followed and comply with the processes with the terms set forth in Annex I of the DPF Principles.

In alignment with the DPF, we undertake to transfer unresolvable complaints regarding our treatment of personal data, which have been submitted in adherence to the DPF principals, to JAMS. JAMS is an alternative dispute resolution provider situated in the United States. Should you not receive a prompt acknowledgment of your complaint pertaining to the DPF Principles from us, or if we fail to satisfactorily address your DPF Principles-related grievance, please visit <https://www.jamsadr.com/dpf-dispute-resolution> for additional details or to initiate a formal complaint. It is important to note that the services provided by JAMS are entirely free of charge to you.

How long do we retain your information?

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations (for example, to comply with obligations relating to invoicing and taxes). We will hold your personal information on our systems for as long as is necessary for the relevant activity, or as long as is specified in any relevant contract between you and us.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not reasonably possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information on hardened servers

that are hosted on highly secure data centers, and isolate it from any further processing until deletion is possible.

Your choices.

We will not contact you for marketing purposes by email or phone except (i) as necessary to enter into a contract or fulfil our obligations under a contract, (ii) with your permission, or (iii) for legitimate purposes permitted by applicable law. We will provide an unsubscribe option on all marketing emails you receive from us. You may also contact us at compliance@cafex.com to unsubscribe or if you have any other questions or concerns regarding your receipt of marketing materials from us.

Accessing and correcting your information.

You may contact us at compliance@cafex.com with any request to access, correct or delete any personal information that you have provided to us. We make good faith efforts to honour reasonable requests to access, correct or delete your personal information. If you request that we delete your personal information, your Service account information will also be removed. We may not accommodate a request to remove personal information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

Data Security.

We have implemented measures designed to secure your personal information from accidental loss and from unauthorised access, use, alteration and disclosure. All information you provide to us is stored on our secure, hardened servers that are hosted on highly secure data centers. Access to this data is protected by multiple layers of controls, including firewalls, authentication mechanisms and monitoring.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of the Service or our websites, you are responsible for keeping this password confidential. We urge you to be careful about giving out information in public areas of our website like message boards. The information you share in public areas may be viewed by any user of our website.

Unfortunately, the transmission of information via the Internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to the Service. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Service.

Consent to transfer, process and store Personal Information.

As CafeX is a global organisation, we may transfer your personal information to CafeX in the United States, to our subsidiary in the United Kingdom, or to third parties and business partners as described above that are located in various countries around the world. By using the Service or providing any personal information to us, where applicable law permits, you consent to the transfer, processing, and storage of such information outside of your country of residence where data protection standards may be different.

CafeX bears the responsibility for the processing of personal data acquired under the Data Privacy Framework and the potential of subsequent transfers to a third party acting as an agent on CafeX behalf. We comply with the Data Privacy Framework for all onward transfers of personal data including the onward transfer liability provisions.

Last updated: Neil Ellis - 20251112