

ZAFERSIGN PRIVACY POLICY

Effective Date: September 14, 2026

Welcome to ZaferSign, a digital transaction management platform operated by ZaferSign (Pvt) Ltd. This ZaferSign privacy policy ("Privacy Policy") describes how we collect, use, protect and share information about you that we obtain when you access and use our Platform (defined below) whether through a Website or the App, including when you register for an account, use our Services, request customer support, submit questions or feedback. This Privacy Policy also applies to information that we obtain when you communicate or interact with us outside of the Platform, including by e-mail, telephone and otherwise.

Please read this Privacy Policy carefully to understand how we will treat your information before you start to use our Platform or communicate with us outside the Platform. This Privacy Policy also is intended to explain the conditions under which ZaferSign uses and discloses that information, and your rights in relation to that information.

Changes to this Privacy Policy are discussed at the end of this document.

The sections below explain our privacy practices in more detail.

DEFINITIONS

For purposes of this Privacy Policy, the following defined terms mean:

"Customer" means an individual, business or organization that subscribes to, purchases, administers or otherwise enters into an agreement to use the Services.

"Customer Content" means documents, data, messages and other content submitted to, stored through or otherwise processed by ZaferSign on behalf of a Customer or at a Customer's direction. Customer Content may include User Content.

"Personal Data" means information that identifies, relates to, describes or can reasonably be linked to an identified or identifiable individual, or that is otherwise treated as personal data, personal information or personally identifiable information under applicable law. References in this Privacy Policy to "Personal Information" or "Personally Identifiable Information" have the same general meaning unless applicable law provides otherwise.

"Sensitive Personal Data" means Personal Data that is treated as sensitive or specially protected under applicable law, which may include government-issued identifiers, financial-account information, biometric information used for identification, health information, precise location information and information revealing certain personal characteristics or beliefs.

"App" means any and all downloadable applications (including, any mobile or tablet applications) owned or operated by ZaferSign through which access to ZaferSign's Services are available. References to the "App" include any and all related features, functionality, tools, and content.

"Platform" refers, collectively, to any and all Websites, Apps and other technology through which ZaferSign provides the Services.

"Services" means any and all digital transaction management and electronic signature services, and related services and promotions, provided by ZaferSign, including support services.

"User" means any person or entity who accesses or uses the Platform in any manner. References to "access" and/or "use" of the Platform (and any variations thereof) include the acts of accessing or browsing the Platform and accessing or using the Services.

"User Content" refers to text, information and other content uploaded, stored, shared or otherwise made available or caused to be made available by Users on or through the Platform.

"Your Content" refers to User Content that is provided or made available or caused to be made available by you.

"Website" means any and all websites owned or operated by ZaferSign, including the website currently located at <https://www.zafersign.com/>, through which access to ZaferSign's Services is available. References to the "Website" include any and all related features, functionality, tools, and content.

OUR ROLE IN PROCESSING PERSONAL DATA

ZaferSign acts as a data controller when it determines how and why personal data is processed, including for account registration, authentication, billing, security, customer support, service communications, marketing and administration of the Platform.

When a business or organizational customer submits documents or other personal data to ZaferSign for processing through the Services, ZaferSign generally processes that information on the customer's behalf and in accordance with the customer's instructions. In these circumstances, the customer is generally the data controller and ZaferSign acts as its data processor or service provider, as those terms are defined under applicable law.

The customer is responsible for establishing an appropriate legal basis, providing required privacy notices and ensuring that it has the authority to provide personal data to ZaferSign. Questions or requests concerning personal data contained in customer-controlled documents should normally be directed to the relevant customer. Where required, ZaferSign will assist the customer in responding to those requests.

ZaferSign may process limited transaction, authentication, audit and security information as a data controller where necessary to operate and secure the Platform, comply with legal obligations, prevent fraud, maintain evidence of electronic transactions, and establish, exercise or defend legal claims.

HOW WE COLLECT INFORMATION

ZaferSign collects information from you, including personally identifiable information, when you use the Platform or Services. This information is collected and stored electronically by us. This information may be provided to us voluntarily by you, information that is generated from the use of the Platform automatically, and information that is provided to us from other sources.

Information You Provide to Us Voluntarily

ZaferSign collects Personal Data that Users or Customers provide directly when they create or administer an account, use the Services, prepare or sign an electronic document, purchase a subscription, enable an optional feature, request support or otherwise communicate with ZaferSign.

This information may include:

- Account and Contact Information. Name, email address, telephone number, organization name, role or job title, and other information necessary to create, manage or support an account.
- Signature and Transaction Information. A User's name, title, electronic signature, signing actions, authentication events and other information necessary to prepare, execute, verify or maintain evidence of an electronic transaction.
- Customer Content. Documents, messages, form entries and other content submitted to or processed through the Services by a User or Customer.
- Payment and Subscription Information. Limited transaction and subscription records, as described in the Payment and Subscription Information section.
- Identity-Verification Information. Information collected only when a User chooses to use an optional KYC or premium identity-authentication feature, as described in the Identity Verification and KYC section.
- Support and Communication Information. Information included in support requests, questions, complaints, feedback or other direct communications with ZaferSign.
- Administrator Information. Information provided when a Customer authorizes a User to administer an organizational account, workspace or related User permissions.
- Sensitive Personal Data

ZaferSign does not routinely request sensitive personal data for standard account registration or use of the core Services.

ZaferSign may process limited sensitive personal data where necessary for an optional KYC or premium identity-authentication feature, as described in the Identity Verification and KYC section; to comply with applicable law; to prevent fraud or protect the security of the Services; or where the User has provided appropriate consent. Payment-card information is submitted directly to the applicable payment provider as described in the Payment and Subscription Information section.

Documents and other content submitted by customers or Users may contain medical, financial, identification or other sensitive personal data. Where ZaferSign processes this information on behalf of a customer, the customer is responsible for determining whether the information may lawfully be submitted, providing required notices, obtaining necessary consent or authorization, and configuring appropriate access controls.

Users should not provide sensitive personal data through support requests, feedback forms or other unrestricted communication channels unless ZaferSign specifically requests it or it is necessary to resolve the relevant matter.

Information Generated from Use of the Platform

When a User accesses or uses the Platform, ZaferSign may automatically collect limited technical and operational information necessary to provide, secure, maintain and troubleshoot the Services.

This information may include:

- Device and Connection Information. Device type, operating system, browser or application version, IP address, language, time zone, mobile carrier and technical identifiers associated with the browser, application or device.
- Operational and Security Information. Login events, authentication activity, request dates and times, error reports, system events, security alerts and other information reasonably necessary to detect fraud, prevent unauthorized access, maintain audit records and diagnose technical problems.
- Service-Use Information. Information about the features accessed, actions performed, documents or transactions initiated or completed, and general interaction with the Services. This does not mean that ZaferSign uses customer document content for advertising or unrelated profiling.

Necessary technical, operational and security information may be collected regardless of a User's analytics preference where required to provide and protect the Services. Optional Google Analytics information is collected only when the User enables analytics, as described in the Cookies and Analytics section.

Information from Other Sources

- ZaferSign may receive personal data from a business or organizational customer that administers an account, invites a User to the Platform, sends documents for signature or otherwise instructs ZaferSign to process information through the Services.
- When a User chooses to use a third-party identity provider, such as UAE Pass, ZaferSign may receive the account and authentication information authorized by the User and necessary to complete registration or authentication.
- ZaferSign may receive limited transaction or subscription information from payment providers, including Stripe for Website transactions and Apple for iOS in-app purchases. ZaferSign does not receive full payment-card numbers or card verification codes from these providers.
- ZaferSign may also receive limited technical, fraud-prevention, security or service-delivery information from providers acting on its behalf where necessary to operate, protect and support the Platform.
- ZaferSign does not purchase third-party contact lists or obtain personal data from data brokers for direct-marketing purposes.

Information from UAE Pass

- If you choose to register for or sign in to our Platform using UAE Pass, we will collect certain personal information from your UAE Pass profile, including your full name, email address, and a unique user identifier (UUID). This data is securely stored in the United Arab Emirates (UAE) to comply with local data residency regulations and is governed by applicable UAE privacy laws. We do not access or store additional UAE Pass data beyond what is required for authentication and secure account setup.

HOW INFORMATION MAY BE USED

ZaferSign may use Personal Data for the following purposes:

- To create, administer and secure accounts and organizational workspaces.
- To authenticate Users, including through approved third-party identity providers such as UAE Pass.
- To provide the Services, process electronic documents and signatures, maintain transaction records and audit evidence, and perform instructions submitted by Users or Customers.
- To administer subscriptions, receive payment confirmations and maintain billing, accounting, tax, refund and transaction records.

- To provide customer support and respond to questions, requests, complaints and feedback.
- To send transactional, security, account, legal and service-related communications.
- To detect, investigate and prevent fraud, unauthorized access, security incidents, misuse and violations of applicable agreements.
- To monitor, maintain, troubleshoot and improve the reliability, functionality, accessibility and performance of the Platform.
- To perform analytics where the User has enabled optional analytics, as described in the Cookies and Analytics section.
- To provide AI-powered functionality when expressly invoked by a User, as described in the AI Features and Model Training section.
- To comply with applicable laws, regulations, court orders and valid governmental requests and to establish, exercise or defend legal claims.
- To send ZaferSign marketing communications where permitted by applicable law and subject to the choices described in the Email Communications section.
- To evaluate or complete a corporate transaction as described in the Change of Control section.
- For another purpose disclosed when Personal Data is collected, with consent where consent is required by applicable law.

ZaferSign does not use Customer Content for targeted advertising or to train general-purpose, generative or foundation models.

IDENTITY VERIFICATION AND KYC

ZaferSign does not routinely collect Social Security numbers or equivalent government-issued identifiers from Users who use the standard Services.

If a User chooses to enable a Know Your Customer (KYC) verification feature or another premium identity-authentication feature, ZaferSign may request and process a Social Security number or equivalent government-issued identifier where necessary to provide that feature. ZaferSign will provide appropriate notice and obtain the User's consent before collecting this information. Declining to provide the information may prevent the User from using the relevant KYC or premium authentication feature but will not prevent access to Services that do not require identity verification.

This information will be used only to verify identity, authenticate the User, prevent fraud, protect transactions and comply with applicable legal or regulatory requirements. It will not be used for advertising or unrelated marketing purposes. ZaferSign will retain it only for as long as reasonably necessary for these purposes or as required by applicable law.

Notwithstanding the above, we may use information that does not identify you (including information that has been aggregated or de-identified) for any purpose except as prohibited by applicable law. For information on your rights and choices regarding how we use information about you, please see the "Your Choices" section below.

AUTOMATED DECISION-MAKING AND PROFILING

ZaferSign does not use solely automated decision-making, including profiling, to make decisions that produce legal or similarly significant effects concerning Users.

Automated tools may support authentication, security monitoring, fraud detection, KYC verification or other Platform functions, but ZaferSign does not rely solely on those tools to automatically approve or reject KYC verification, account access, premium-feature eligibility or transactions without appropriate human involvement.

If ZaferSign introduces solely automated decision-making that produces legal or similarly significant effects, we will provide any notice, explanation, consent mechanism, opt-out right, human-review process or other protection required by applicable law before applying that processing to affected Users.

LAWFUL BASES FOR PROCESSING

Where applicable law requires us to identify a lawful basis for processing personal data, ZaferSign relies on one or more of the following bases:

- **Performance of a Contract.** We process personal data when necessary to provide the Services you or an organization acting on your behalf has requested, including creating and managing accounts, authenticating Users, processing electronic transactions, providing customer support and administering subscriptions.
- **Compliance with Legal Obligations.** We process personal data when necessary to comply with applicable legal, regulatory, accounting, tax and reporting obligations, respond to legally valid requests, and maintain records required by law.
- **Legitimate Interests.** We process personal data when necessary for our legitimate business interests or those of a third party, provided those interests are not overridden by your rights and interests. These interests include operating, securing and improving the Platform, preventing fraud and misuse, maintaining evidence of electronic transactions, communicating with Users, and establishing, exercising or defending legal claims.
- **Consent.** Where appropriate, ZaferSign processes Personal Data based on a User's freely given, specific, informed and unambiguous consent. This may include optional Google Analytics and certain optional KYC or premium identity-authentication processing where consent is required by applicable law. A User may withdraw consent at any time through the relevant Platform controls or by contacting privacy@zafersign.com. Withdrawal will not affect the lawfulness of processing performed before consent was withdrawn.

Withdrawing consent may prevent access to the particular optional feature that requires the information, but it will not prevent access to unrelated core Services. Where Personal Data is treated as sensitive or specially protected under applicable law, ZaferSign will satisfy any additional legal condition required for that processing, such as obtaining explicit consent where appropriate.

ZaferSign may rely on another lawful basis where permitted or required by applicable law. Where ZaferSign processes personal data on behalf of a business or organizational customer, that customer is generally responsible for determining the appropriate lawful basis for the processing.

CHANGE OF CONTROL

In the event ZaferSign is involved in a merger, acquisition, sale of assets, or other corporate transaction (a "Change of Control" event), your personal data and User Content (including any data stored in the UAE for UAE Pass users or government clients) may be transferred to the acquiring entity. By accepting this Privacy Policy, you consent to such transfer. We will require that the acquiring entity or successor adhere to the terms of this Privacy Policy, or that they provide you with prior notice if their policy materially changes. ZaferSign will remain responsible for your data in accordance with this policy until the successful completion of the transfer.

DATA RETENTION

ZaferSign retains personal data only for as long as reasonably necessary to fulfil the purposes described in this Privacy Policy, provide the Services, comply with legal and regulatory obligations, resolve disputes, prevent fraud, maintain security, enforce agreements and establish, exercise or defend legal claims.

Retention periods vary according to the nature of the information and the purpose for which it is processed. When determining an appropriate retention period, ZaferSign considers applicable legal and contractual requirements, the sensitivity of the information, the risk of harm from unauthorized use or disclosure, and whether the relevant purpose can be achieved through anonymisation.

Account and profile information is generally retained while an account or subscription remains active. After closure or expiry, it will be deleted or anonymised in accordance with ZaferSign's retention procedures, except where continued retention is reasonably necessary or legally required.

Customer documents and related personal data are retained according to the applicable service agreement, customer instructions and account settings. Signature evidence, transaction records and audit trails may be retained for longer periods where necessary to verify the validity and integrity of an electronic transaction or to comply with legal obligations.

Billing, tax, support and security records may be retained for the periods required by applicable law or reasonably necessary for accounting, audit, fraud-prevention, dispute-resolution and security purposes.

Information stored in backups will be deleted or rendered inaccessible through ZaferSign's normal backup-replacement cycle.

ZaferSign may create and record cryptographic hashes or similar verification values on a blockchain or other immutable audit system to verify the integrity or existence of a document or transaction. These verification values are not designed to contain Customer Content, signatures or directly identifying Personal Data, and recording them does not make the underlying document or Personal Data publicly accessible.

Because blockchain and other immutable audit records cannot ordinarily be altered or deleted, verification hashes may remain after the underlying document or account information has been deleted. Personal Data and Customer Content stored in ZaferSign's systems remain subject to the other retention and deletion provisions of this Privacy Policy.

When information is no longer required, ZaferSign will delete it, anonymise it, or securely restrict access to it, as appropriate.

HOW INFORMATION MAY BE SHARED

ZaferSign does not sell or rent personal data or disclose it to third parties for their independent marketing or advertising purposes. ZaferSign discloses personal data only as described in this Privacy Policy and where reasonably necessary to provide, secure, support and administer the Services, process payments, enable authentication, comply with law, complete a corporate transaction, or follow a User's instructions.

- **Service Providers.** ZaferSign may disclose personal data to service providers that perform services on its behalf, such as cloud hosting and storage, security, technical support, customer support, optional analytics, communications and AI-powered processing. Where a provider processes personal data on ZaferSign's behalf, it is required by contract to process the information for the agreed services, follow applicable instructions and apply appropriate safeguards.
- **Payment Providers.** Payments made through the Website are processed by Stripe, and purchases made through the iOS App are processed by Apple. These providers may process payment information under their own terms and privacy policies, as described in the Payment and Subscription Information section.
- **Identity Providers.** ZaferSign may receive or exchange limited information with an identity provider selected by the User, such as UAE Pass, where necessary to authenticate the User, verify identity and provide secure account access.
- **Customers and User-Directed Recipients.** Where ZaferSign processes personal data on behalf of a business or organizational customer, it may make that information available to the customer in accordance with the customer's instructions. ZaferSign may also disclose documents and related information to signatories, recipients or integrations selected or authorized by the User or customer.
- **Corporate Transactions.** Personal data may be disclosed in connection with a proposed or completed merger, acquisition, financing, reorganization, bankruptcy, sale of assets or similar corporate transaction, subject to appropriate confidentiality and data-protection measures.
- **Legal, Security and Protection Purposes.** ZaferSign may disclose personal data where reasonably necessary to comply with applicable law, respond to valid legal process or lawful government requests, prevent or investigate fraud or misuse, protect the security of the Platform, enforce agreements, or protect the rights, property, safety or security of ZaferSign, its Users or others.
- **Consent and User Direction.** ZaferSign may disclose personal data where the User directs or authorizes the disclosure or provides consent, subject to applicable law.

ZaferSign may use or disclose information that has been aggregated or de-identified so that it cannot reasonably be linked to an individual, except where prohibited by applicable law. ZaferSign does not attempt to re-identify such information.

PAYMENT AND SUBSCRIPTION INFORMATION

ZaferSign does not directly collect or store full payment-card numbers, card verification codes or other complete payment credentials. Payments made through the Website are processed by Stripe, and purchases made through the iOS App are processed through Apple's In-App Purchase system. These providers collect and process payment information according to their own terms and privacy policies.

ZaferSign may receive and retain limited payment and subscription records necessary to process and administer transactions, provide purchased Services, manage subscriptions, issue or record refunds, maintain accounting and tax records, prevent fraud, resolve disputes and provide customer support. These records may include transaction identifiers, purchase amounts, currencies, purchase dates, subscription plans, payment status, renewal information and refund or chargeback details.

The payment information provided directly to Stripe or Apple is controlled and processed by the applicable payment provider. Users should review the provider's applicable terms and privacy policy for information about its payment-data practices.

COOKIES AND ANALYTICS

ZaferSign uses cookies and similar technologies that are reasonably necessary to operate, secure and administer the Website and web-based Platform, including app.zaferSign.net. These technologies may support authentication, maintain sessions, prevent fraud, protect accounts and remember user preferences.

Google Analytics is optional. ZaferSign will not enable Google Analytics for a User unless the User actively chooses to enable analytics through the consent controls provided on the Website or web-based Platform.

When enabled, Google Analytics may use cookies or similar identifiers to collect standard analytics information, such as user and session counts, page or screen views, interactions, approximate location, browser and device information, and technical performance data. ZaferSign uses this information to understand usage, identify technical issues and improve the functionality, reliability and performance of the Services.

ZaferSign does not use Google Analytics information for targeted advertising, remarketing or creating advertising profiles. Google processes analytics information in accordance with its applicable terms and privacy practices. More information is available at <https://policies.google.com/privacy>.

YOUR CHOICES

We offer you certain choices in connection with the information we collect from you.

Account Information

Users may review and update certain profile or business information through the account controls available in the App or Website.

Mobile App users may initiate account deletion through the account settings available in the App. Website users may initiate an account-deletion request by contacting ZaferSign support or emailing privacy@zaferSign.com.

ZaferSign may take reasonable steps to verify the requester's identity and authority before completing a request. Account deletion is subject to applicable legal exceptions and the retention requirements described in this Privacy Policy. Deleting an account may not delete Personal Data contained in documents controlled by another Customer; requests concerning that information should normally be directed to the relevant Customer.

Email Communications

ZaferSign may send transactional, security, account, legal and service-related communications that are necessary to operate the Platform, administer your account, complete requested transactions or inform you of material changes affecting the Services. These communications are not marketing messages, and you may continue to receive them while you maintain an account or use the relevant Services.

Where permitted by applicable law, ZaferSign may send promotional communications concerning ZaferSign products, features or services. We will obtain consent before sending marketing communications where consent is legally required.

You may unsubscribe from marketing emails at any time by using the unsubscribe link included in the message or by adjusting the communication preferences available in your account. ZaferSign will apply the request within the period required by applicable law. Unsubscribing from marketing will not prevent you from receiving necessary transactional, security, legal or service-related communications.

Analytics Choices

Users may enable or decline Google Analytics through the analytics consent prompt. A User who enables analytics may later withdraw that choice through the cookie or privacy settings made available on the Platform. Withdrawal stops future optional analytics collection from that browser or device, subject to the time reasonably required to apply the updated choice.

Declining or withdrawing analytics will not prevent access to the core Services. Necessary cookies and similar technologies may continue to operate where required for authentication, security, session management and other essential Platform functions.

SECURING YOUR INFORMATION

ZaferSign maintains reasonable administrative, technical and organizational safeguards designed to protect personal data against unauthorized or unlawful access, use, alteration, disclosure, loss or destruction. The safeguards applied may vary according to the nature and sensitivity of the information and the risks associated with its processing.

No method of transmission or storage is completely secure, and ZaferSign cannot guarantee absolute security. If ZaferSign becomes aware of a personal-data breach, it will investigate the incident, take reasonable steps to contain and remediate it, and notify affected customers, Users, regulators or other parties where and within the period required by applicable law or contract.

Users are responsible for maintaining the confidentiality of their account credentials, using appropriate security settings and promptly notifying ZaferSign if they suspect unauthorized access, credential compromise or another security issue. Corporate customers are responsible for managing administrator and subaccount permissions and for the security of credentials under their control.

Security concerns may be reported to privacy@zafersign.com.

CHILDREN AND MINORS

The Platform is not directed to children, and individuals who have not reached the legal age of majority in their jurisdiction may not independently create or maintain a ZaferSign account.

A business or organizational customer may use the Services to send a document to, obtain a signature from, or otherwise process personal data concerning a minor where permitted by applicable law. In those circumstances, the customer is responsible for establishing an appropriate legal basis, providing required notices, obtaining any necessary consent or authorization from a parent or legal guardian, and ensuring that its use of the Services complies with applicable law. ZaferSign generally processes such information on the customer's behalf and in accordance with the customer's instructions.

If ZaferSign learns that a minor has independently created an account or that personal data has been collected directly from a child without the authorization or consent required by applicable law, ZaferSign will take reasonable steps to suspend the account and delete or restrict the information, subject to applicable legal obligations, customer instructions and the retention provisions of this Privacy Policy.

Requests concerning a minor's personal data contained in customer-controlled documents should normally be directed to the customer that submitted or controls the information. Questions concerning information collected directly by ZaferSign may be sent to privacy@zafersign.com.

ZaferSign does not use children's personal data for targeted advertising, profiling, or training general-purpose or generative artificial intelligence models.

LINKS TO THIRD PARTY WEBSITES

The Platform may contain links to third-party websites, applications or services that are not operated or controlled by ZaferSign. These links are provided for convenience and informational purposes only.

Third parties may collect and process personal data under their own privacy notices and terms. ZaferSign is not responsible for the privacy, security or other practices of third-party websites, applications or services. Users should review the applicable privacy notices before providing personal data to, or using, any third-party service.

The inclusion of a link does not imply that ZaferSign endorses or is affiliated with the relevant third party unless expressly stated otherwise.

INTERPRETATION

Your use of the Platform may also be governed by ZaferSign's Terms and Conditions of Use, available at <https://www.zafersign.com/agreements/#terms-of-use>, together with any supplemental terms applicable to particular Services or features.

This Privacy Policy governs how ZaferSign collects, uses, discloses and otherwise processes personal data. If another ZaferSign notice or supplemental term conflicts with this Privacy Policy regarding the processing of personal data, the more specific privacy notice will apply only to the relevant Service, feature or processing activity.

Nothing in this Privacy Policy or any supplemental terms limits or excludes rights that cannot lawfully be limited or excluded under applicable data-protection law.

INTERNATIONAL JURISDICTIONS

Data Residency and Customer-Selected Storage

By default, ZaferSign stores eligible customer data in the United States. Where the applicable Services and subscription permit, customers may select from supported geographic locations for the storage of eligible customer data. The available locations may vary according to the Services, technical availability and applicable contractual terms.

A customer's selected data-storage location determines where the applicable customer data is primarily stored. It does not necessarily mean that all personal data associated with the customer or the Services will be processed exclusively in that location. Account information, authentication data, billing records, support information, security logs, service metadata and information processed through third-party service providers may be processed in other jurisdictions where necessary to provide, secure, support and administer the Services.

Certain categories of information, including information subject to mandatory local data-residency requirements, may be stored in a specific jurisdiction as required by applicable law or the relevant service configuration.

International Data Transfers

ZaferSign operates internationally, and Personal Data may be transferred to, accessed from or processed in jurisdictions other than the jurisdiction in which a User or Customer is located. This may include transfers to ZaferSign's service providers and other recipients described in this Privacy Policy. Data-protection laws in those jurisdictions may differ from the laws of the User's jurisdiction.

Where applicable law restricts international transfers, ZaferSign will use an approved transfer mechanism or another legally permitted basis. Depending on the circumstances, these measures may include an applicable adequacy decision, the European Commission's Standard Contractual Clauses, the United Kingdom International Data Transfer Agreement or Addendum, contractual data-protection obligations, transfer-risk assessments and appropriate technical and organizational safeguards.

A Customer's selected data-storage location does not prevent authorized international processing where necessary to provide, secure, support or administer the Services, subject to applicable law and the relevant service agreement.

Users may contact privacy@zafersign.com for additional information about the safeguards applicable to a particular transfer. Where required by applicable law, ZaferSign will provide access to a copy or summary of the relevant safeguards, subject to appropriate redactions.

CHANGES TO OUR PRIVACY POLICY

ZaferSign may update this Privacy Policy from time to time to reflect changes to our Services, data-processing practices, legal obligations or other operational requirements. The revised Privacy Policy will be published on the Website with an updated effective date.

Where changes are material, ZaferSign will provide reasonable notice through email, an in-product notification, a notice on the Website or another appropriate method, where required by applicable law. If ZaferSign intends to process personal data for a materially different purpose, we will provide appropriate notice before beginning that processing and obtain consent where consent is required by applicable law.

Your continued use of the Services after an updated Privacy Policy becomes effective will be subject to the updated Privacy Policy. However, continued use will not be treated as consent where applicable law requires ZaferSign to obtain express consent.

CONTACT US

For questions, complaints or requests concerning this Privacy Policy or ZaferSign's processing of Personal Data, please contact privacy@zafersign.com. For general enquiries unrelated to privacy, please contact info@zafersign.com.

When submitting a privacy request, please provide sufficient information to identify the relevant account or interaction and clearly describe the request. Do not send passwords, authentication codes, full payment-card information, unrequested identity documents or other unnecessary Sensitive Personal Data by email.

ZaferSign may request additional information reasonably necessary to verify the requester's identity, authority and relationship to the relevant Personal Data. Where sensitive verification information is required, ZaferSign may provide an appropriate secure submission method.

ZaferSign will review privacy complaints and requests and respond within the period required by applicable law. Nothing in this section limits an individual's right to contact an applicable data-protection authority or other regulator.

NOTICE TO CALIFORNIA RESIDENTS

Where the California Consumer Privacy Act, as amended ("CCPA"), applies to ZaferSign's processing, California residents may have the right to request information about the categories and specific pieces of Personal Information collected about them; the sources, purposes and categories of recipients associated with that information; access to, correction of or deletion of Personal Information; and a portable copy of certain information. California residents may also have the right to opt out of the sale or sharing of Personal Information, limit certain uses or disclosures of Sensitive Personal Information, and receive equal service and pricing without unlawful discrimination for exercising their privacy rights.

The categories of Personal Information ZaferSign may collect, the sources from which it is obtained, the purposes for which it is used and the categories of recipients to whom it may be disclosed are described in the relevant sections of this Privacy Policy.

ZaferSign does not sell Personal Information for monetary consideration or use Personal Information for targeted advertising. Disclosures to service providers, contractors and other recipients necessary to provide the Services are not treated as a sale or sharing where the requirements of applicable law are satisfied.

California residents may submit a request through the account settings available in the App or Website or by contacting privacy@zafersign.com. ZaferSign may take reasonable steps to verify the requester's identity and authority. An authorized agent may submit a request where permitted by law, subject to appropriate verification. ZaferSign will respond within the period required by applicable law and will explain any applicable exception or denial.

NOTICE TO NEVADA RESIDENTS

Where Nevada Revised Statutes Chapter 603A applies, Nevada consumers may submit a verified request directing ZaferSign not to make a sale of covered information collected about them.

ZaferSign does not sell covered information for monetary consideration as "sale" is defined under applicable Nevada law. If ZaferSign's practices change, we will provide any notice and opportunity to opt out required by applicable law.

Nevada consumers may submit a verified request by contacting privacy@zafersign.com. ZaferSign may take reasonable steps to verify the requester's identity and will respond within the period required by applicable law.

NOTICE TO RESIDENTS OF OTHER U.S. STATES

Residents of certain U.S. states may have additional privacy rights where the applicable state privacy law applies to ZaferSign's processing. Depending on the relevant law, these rights may include confirming whether ZaferSign processes Personal Data; accessing, correcting, deleting or obtaining a portable copy of Personal Data; opting out of the sale of Personal Data, targeted advertising or certain profiling; withdrawing consent to certain processing of Sensitive Personal Data; and appealing the denial of a privacy request.

ZaferSign does not sell Personal Data for monetary consideration or use Personal Data for targeted advertising.

Requests may be submitted through the account settings available in the App or Website or by contacting privacy@zafersign.com. ZaferSign may take reasonable steps to verify the requester's identity and authority. Where required by applicable law, ZaferSign will recognize authorized agents or qualifying universal opt-out mechanisms and provide an appeal process as described in the Privacy Rights and Requests section.

ZaferSign will respond within the period required by applicable law and will not unlawfully discriminate against an individual for exercising an applicable privacy right.

NOTICE TO EUROPEAN RESIDENTS

Where the European Union General Data Protection Regulation ("EU GDPR"), the United Kingdom General Data Protection Regulation ("UK GDPR") or other applicable European data-protection law applies, individuals may exercise the rights described in the Privacy Rights and Requests section of this Privacy Policy.

Where processing is based on consent, an individual may withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing performed before consent was withdrawn. Individuals may also lodge a complaint with the data-protection supervisory authority in the country where they live or work or where an alleged infringement occurred. Individuals in the United Kingdom may contact the Information Commissioner's Office. We encourage individuals to contact ZaferSign first so that we have an opportunity to address their concerns, but doing so does not affect their right to complain to a supervisory authority.

Where ZaferSign processes personal data contained in customer-controlled documents as a processor or service provider, requests should normally be directed to the relevant customer acting as controller. ZaferSign will assist that customer as required by applicable law and the applicable service agreement.

Personal data may be transferred outside the EEA, EU or United Kingdom as described in the International Jurisdictions section of this Privacy Policy and subject to safeguards required by applicable law.

Data Usage for Model Training

When a User invokes an AI-powered feature, ZaferSign may securely transmit the User's prompts, instructions and relevant portions of selected customer content to Amazon Web Services through Amazon Bedrock solely to generate the requested output.

ZaferSign does not use customer documents, document content, signatures, authentication data, prompts, generated outputs or other personally identifiable information to train general-purpose, generative or foundation models. Amazon Bedrock is configured with model-invocation logging disabled, and ZaferSign does not separately retain AI prompts, generated outputs or AI conversation history.

AWS does not provide customer prompts or outputs submitted through Amazon Bedrock to the underlying model providers or use them to train the underlying foundation models. ZaferSign applies appropriate access controls and security safeguards to information processed through its AI-powered features.

ZaferSign may use aggregated or de-identified technical usage information that does not contain customer document content and cannot reasonably be linked to an individual to monitor and improve the functionality, reliability and performance of the Services. ZaferSign does not attempt to re-identify this information.

User Control and Data Management

Depending on your location and applicable law, you may have the right to request access to or a copy of your personal data; correct inaccurate or incomplete personal data; request deletion of personal data; restrict or object to certain processing; receive certain personal data in a portable format; and withdraw consent where processing is based on consent. You may also have the right to lodge a complaint with an applicable data-protection authority.

These rights are not absolute and may be subject to legal exceptions. For example, ZaferSign may retain or continue processing certain information where necessary to comply with legal obligations, maintain transaction and audit evidence, prevent fraud, protect security, resolve disputes, or establish, exercise or defend legal claims.

You may submit a request through the account settings available in the App or Website or by contacting privacy@zafersign.com. ZaferSign may request information reasonably necessary to verify your identity and authority to make the request. We will respond within the period required by applicable law and will explain any decision not to fulfil a request.

Where ZaferSign processes personal data contained in customer-controlled documents on behalf of a business or organizational customer, requests concerning that data should normally be directed to the customer. ZaferSign will assist the customer where required by applicable law and the applicable service agreement.

If ZaferSign denies a privacy request in whole or in part, we will explain the basis for the decision where required by applicable law. Where applicable law provides a right to appeal, the response will include instructions for submitting an appeal.

An appeal may be submitted by replying to ZaferSign's decision or by emailing privacy@zafersign.com with the subject "Privacy Request Appeal." ZaferSign will review the appeal and communicate its decision within the period required by applicable law. If the appeal is denied, we will provide information about any further complaint options required by applicable law.

Third-Party Data Sharing Transparency

ZaferSign does not sell or rent Personal Data or disclose it to third parties for their independent marketing or advertising purposes. ZaferSign discloses Personal Data only to service providers and other recipients reasonably necessary to provide, secure, support and administer the Services, process payments, enable authentication, comply with applicable law, complete a corporate transaction or follow a User's or Customer's instructions.

Providers processing Personal Data on ZaferSign's behalf are subject to contractual data-protection obligations. Certain providers, including Stripe and Apple, may independently determine how they process information submitted directly to them and process that information under their own terms and privacy policies.

Minor Data Handling and Parental Consent

The Platform is not directed to children, and individuals who have not reached the legal age of majority in their jurisdiction may not independently create or maintain a ZaferSign account.

A Customer may use the Services to send a document to, obtain a signature from or otherwise process Personal Data concerning a minor where permitted by applicable law. The Customer is responsible for establishing an appropriate legal basis, providing required notices and obtaining any necessary authorization or consent from a parent or legal guardian.

If ZaferSign learns that a minor independently created an account or that Personal Data was collected directly from a child without required authorization or consent, ZaferSign will take reasonable steps to suspend the account and delete or restrict the information, subject to applicable legal obligations, Customer instructions and the retention provisions of this Privacy Policy. ZaferSign does not use children's Personal Data for targeted advertising, profiling or training general-purpose or generative artificial intelligence models.

Data Retention Clarification

ZaferSign retains Personal Data only for as long as reasonably necessary for the purposes described in this Privacy Policy or as required by applicable law, contractual obligations, Customer instructions or legitimate security, audit, dispute-resolution and legal-claims requirements. When information is no longer required, ZaferSign will delete it, anonymize it or securely restrict access to it, as appropriate.

Customer Content is retained according to the applicable service agreement, Customer instructions and account settings. Signature evidence, transaction records and audit trails may be retained for longer where necessary to verify the validity and integrity of an electronic transaction or comply with legal obligations. Data subject to mandatory local residency or sovereignty requirements will be handled according to the applicable law and service configuration.

ZaferSign may retain immutable cryptographic hashes or similar verification values used to verify a document or transaction. These values are not designed to contain Customer Content, signatures or directly identifying Personal Data and do not make the underlying document or Personal Data publicly accessible.

Data Handling in the Event of Service Discontinuation

If ZaferSign discontinues the Platform globally or in a particular region, ZaferSign will provide reasonable notice where practicable and, subject to the available functionality and applicable service agreement, a reasonable opportunity for Customers or Users to export eligible Customer Content.

During an orderly wind-down, ZaferSign may retain Personal Data only for as long as reasonably necessary to facilitate authorized data export, maintain security, complete the discontinuation process and comply with applicable legal, regulatory, contractual and audit obligations. After those requirements have been satisfied, Personal Data will be deleted, anonymized or securely restricted in accordance with this Privacy Policy.

Customer Content stored in a Customer-selected region, or information subject to mandatory local data-residency or sovereignty requirements, will continue to be handled in accordance with applicable law and the relevant service agreement. Immutable cryptographic hashes or similar verification values may remain as described in the Data Retention section, but they do not make the underlying documents or Personal Data publicly accessible.