eSign App Privacy Policy

You can see our previous Privacy Policy here and here.

Effective date: October 9, 2025

INTRODUCTION AND SCOPE

This ESign App Privacy Policy ("**Privacy Policy**") is delivered on behalf of Municorn Limited ("**Municorn**," "**we**", "**us**", and "**our**") and governs the Personal Data (as defined below) and other data collected from or processed about you when you use the ESign App mobile application, which provides a professional and easy way to e-sign documents, save and share documents from phone ("**ESign App**"), including by downloading, installing, registering with, accessing or otherwise using the application (collectively referred to herein as "**Use**").

We provide this Privacy Policy to explain our practices for collecting, using, processing, and disclosing the Personal Data we process about ESign App users ("**users**", "**you**", or "**your**", as applicable), and to tell you about the rights you may have in relation to your Personal Data and choices you may be able to make in relation to it. By Personal Data we mean (i) information that is associated with an identified or identifiable natural person, and (ii) protected as personal data under applicable data protection laws.

Please read this Privacy Policy carefully to understand our privacy practices. We also encourage you to get acquainted with our Terms of Use to understand how we provide services to you.

When you create or use a unified account, the same login credentials may be used to access all Municorn applications included in your Bundle Subscription (eSign App, Scanner App, and PDF Forms App). Personal data collected through your account may be shared and synchronized among these applications to enable authentication, subscription verification, and seamless access to the full set of services. Each application is governed by its own Terms of Use and Privacy Policy, which we encourage you to review before starting to use the Bundle Subscription.

By accepting this Privacy Policy, you acknowledge that you understand and agree to the processing of your Personal Data and other information as described in this Privacy Policy. You consent to our collection, use, and sharing of data to provide and improve the functionality of the ESign App. This includes the processing of Personal Data and other information necessary for the operation of the ESign App.

Please note that if you choose to limit or withhold certain data, some features of the ESign App may not function as intended, and you may experience a reduced user experience.

If you do not wish to have your data processed in accordance with this Privacy Policy, please refrain from using the ESign App.

Questions? If you have any questions about this Privacy Policy or ESign App, please contact us at support@e-sign.co. For additional. contact information, please see *Section 15: How to Contact Us*.

U.S. State Supplements:

This Privacy Policy is designed to comply with data privacy laws across the United States, including:

- California Consumer Privacy Act (CCPA),
- Colorado Privacy Act (CPA),
- Connecticut Data Privacy Act (CTDPA),
- Virginia Consumer Data Protection Act (VCDPA),
- Texas Data Privacy and Security Act (TDPSA),
- Tennessee Consumer Privacy Act (TCPA),
- Oregon Consumer Privacy Act (OCPA) and other applicable state laws.

If you are a resident of California, please see our **California Notice at Collection and Privacy Notice**, which provides detailed information about your rights and additional disclosures specific to California.

If you are a resident of Colorado, Connecticut, Virginia, Texas, Oregon, Tennessee, or any other U.S. state with privacy laws, please see our **U.S. State Privacy Supplement (Non-California)**. The rights granted to you under these laws are also outlined in this Privacy Policy. These include:

- The right to access, correct, delete, or receive a copy of your personal data.
- The right to opt out of the sale or sharing of your personal data, targeted advertising, and profiling with legal or significant effects.

You may exercise these rights by contacting us at support@e-sign.co or through the in-app privacy settings, where available.

TABLE OF CONTENTS

1. PERSONAL DATA WE COLLECT AND HOW WE COLLECT IT

We may collect Personal Data from and about you:

- Directly from you when you provide it to us.
- Automatically when you Use ESign App. Information collected automatically may include Usage details and Internet Protocol ("**IP"**) addresses.
- From third parties, for example, our service providers, partners and vendors.

2. PERSONAL DATA YOU PROVIDE TO US DIRECTLY

You may provide Personal Data to us directly, or to service providers that act on our behalf, when you Use ESign App. The Personal Data you provide depends on which features of ESign App you Use and how you interact with the app.

- **Authentication Data. When you create or access your personal account:**
  - If you're using Google, we may collect your name and email address through Google's authentication API.
  - If you're using Apple, we may collect your name and email address based on your Apple ID sharing settings.

- If you're signing up via email, you provide your email address and verify it with a one-time password sent to your inbox.

These credentials are stored in ESign App to maintain your account and profile.

- **Photos that you upload to ESign App**. If you grant us permission to access your camera or your device's photo library, we will process the photos you select to upload to ESign App to provide features of the app that you choose to Use.
- **Documents that you upload to ESign App.** If you grant us permission to access files on your device, we will process the documents you select to upload to the ESign App to enable the app's features, such as signing, editing, and sharing them in various formats like PDF or JPG.
- If you contact us or communicate with us, we will collect and receive **records and copies of your correspondence with us and contact details that you have provided us with while making your inquiries** (such as your name, postal addresses, email addresses and phone numbers or any other identifier by which you may be contacted).
- **Sensitive data**. We do not intentionally use or process sensitive data beyond what is necessary to provide the core functionality of the app. Sensitive data may include, but is not limited to:
    - Personally Identifiable Information (PII), such as names, addresses, phone numbers, or financial information.
    - Medical, biometric, or other confidential information.

  Sensitive information is provided solely at the user's discretion and under their control. If sensitive data is uploaded voluntarily, it is done at the user's own responsibility, and we encourage users to avoid including such data in their documents.

  In cases where sensitive data is uploaded unintentionally:

  - We do not knowingly collect or process any sensitive personal data except to the extent strictly necessary to provide you with the service you have requested.
  - We do not analyze the content you upload; therefore, we cannot actively monitor or identify sensitive data within your uploads.

  If we become aware that sensitive data has been uploaded unintentionally, we will make reasonable efforts to delete it promptly, where technically feasible.

  Please note we rely on you to avoid uploading sensitive personal data (such as health information, biometric data, or data revealing racial or ethnic origin) unless it is strictly necessary for your Use of the service. By uploading documents, you acknowledge that the decision to include sensitive information is yours, and we are not liable for any sensitive data uploaded without request or consent.

3. PERSONAL DATA AND OTHER DATA WE COLLECT AUTOMATICALLY

When you Use ESign App, we or third parties we permit to do so, may automatically collect certain information, including Personal Data, from you (this is subject to your consent where this is required by law). The information collected from you automatically when you Use ESign App may include:

- **Account and Authentication Data.** When you create or log into a unified account (for example, using email, Apple ID, or other supported login methods), we collect identifiers such as your name, email address, authentication tokens, and subscription status. This data enables single sign-on (SSO) and unified access across all Municorn Apps included in your Bundle Subscription.
- **Cross-App Usage Data.** When you access multiple Municorn Apps through the same account, limited technical and usage data (for example, login timestamps, subscription verification, and device identifiers) may be synchronized between these apps to maintain your session and ensure subscription validity.
- **Log file information.** Log file information is automatically reported by your browser each time you make a request to access (ie, visit) a web page or app. It can also be provided when the content of the webpage or app is downloaded to your browser or device. When you use ESign App, our servers automatically record certain log file information, including your web request, IP address, browser type, referring / exit pages and URLs, number of clicks and how you interact with links on the ESign App, domain names, landing pages, pages viewed, and other such information. We may also collect similar information from emails sent to our Users which then help us track which emails are opened and which links are clicked by recipients. The information allows for more accurate reporting and improvement of our services.
- **Subscription and device data**. Information related to your subscription and device used for technical authorization.
- **Marketing and cookies data**. Collected through cookies and analytics services integrated into the app.
- **Device information**. Information about your mobile device and internet connection, including your IP address, the device's unique device identifier, operating system and version, mobile network information, device type and device language.
- **App and country information**. Information regarding the version of the app that you are using and the country version of the app store from which you downloaded ESign App.
- **Geolocation data.** the state or country associated with your IP address.
- **Usage details**. Details of your Use of ESign App, including frequency of Use, areas and features of the application that you access and information regarding engagement with particular features of the app.
- **Details about your in-app purchases**. For example, details regarding the time you made certain purchases.

- **Uploaded documents**. Files provided by users, such as contracts, tax forms, or images in JPG or PDF format.
- **Third-party emails**. Email addresses of third parties provided for document signing or sharing.
- **Payments**. When enabling payment processing, you may integrate with Stripe. The payment account details are stored by Stripe, not by us. Payment links or QR codes may be generated and shared to facilitate client payments.
- **Permissions for Camera, Photos and videos, Files.** After you grant us the relevant permission, we may have technical access to your camera, which is required to be able to scan documents via the ESign App and/or to take photos you want to add to your documents. Additionally, if you try to upload any image, photo or file from your Photo Library/Gallery or Files to the ESign App, the relevant technical access of the ESign App to your Photos and videos or Files is required. The technical access you provide to your Photos and videos (whether limited or full) and Files is necessary solely to enable you to upload photos, images, or files from your device to the ESign App, and to use them for signing and editing documents within the App. This access is required to operate the ESign App services and provide you with its full functionality. You can manage, change access permissions to your Camera, Photos and videos, Files at any time via the Settings.
- **User signatures**: Stored locally on user devices unless explicitly shared for processing.
- **(If you have provided your consent) IDFA or Android Advertising ID**, whichever is applicable to your device. If you want to disable the collection of IDFA and/or Android Advertising ID by ESign App, please follow the instructions below.

  If you use an iOS device:

  1. Go to Privacy settings to see a list of apps that request to track your activity. On iPhone or iPad, go to Settings > Privacy > Tracking.
  2. Tap to turn off or turn on permission to track for ESign App.

  If you use an Android device:

  1. Open Settings app
  2. Navigate to “Privacy” > “Ads”
  3. Tap “Delete Advertising ID”
  4. Tap it again on the next page to confirm.

Other than with respect to Image Data, we and third-parties we engage may use cookies, Software Development Kits (**SDKs**), and other tracking technologies to automatically collect the Personal Data set forth above. For more information regarding our use of these technologies, please see *Section 6: Cookies, Software Development Kits, and Other Tracking Technologies*.

4. THE PURPOSES AND OUR LEGAL BASES FOR PROCESSING YOUR PERSONAL DATA

We may use your Personal Data for a variety of purposes depending on the category of Personal Data and the way you Use and interact with the ESign App, including the following:

- To present to you and others with ESign App and its contents and any other information, products or services that you request from us, including to provide various features of the app and its functionality. We do so to provide you with the services according to our contractual obligation.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us in relation to ESign App (e.g., the Terms of Use). This is for the performance of our contract with you and for our legitimate interests in performing and enforcing our contracts with you.
- To provide you with customer and technical support, investigate your concerns, respond to your inquiries and to monitor and improve our responses to your and other users' inquiries in relation to ESign App. It is our legitimate interest to provide you with high-quality support.
- To communicate with you, such as to notify you about changes to ESign App or any products or services we offer or provide through ESign App, including by sending you technical notices, notices about your account/subscription, including expiration and renewal notices, updates, security alerts and support and administrative messages, which we may send through an in-app or a push notification (you may opt-out of push notifications by changing the settings on your mobile device). It is our contractual obligation to keep you informed about your subscription and your account and otherwise in our legitimate interests of keeping you informed about your ESign App account.
- To conduct research, analytics and monitor performance and other metrics regarding ESign App and your Use of ESign App. This may include data regarding the total number of users of our app, traffic, and demographic patterns related to the use of our app. Where this data is collected through the technologies described in *Section 6* where required by law, we rely on your consent; otherwise, it is our legitimate interest to conduct analytics as it helps us understand our business metrics and improve our product.
- To improve, test, and monitor the effectiveness of ESign App. It is our legitimate interest to conduct such analyses to understand our product and business metrics.
- To provide personalized content and information to you in relation to ESign App and so that we, and third parties on which we rely, can advertise to you. This may include using your Personal Data to build advertising audiences that we believe are similar to our user base, serving online ads to you, or engaging in other forms of advertising. Where required by law, we rely on your consent to engage in such activities and/or offer you the opportunity to opt-out. Please see *Section 3 and Section 6* for more information.

- To send marketing and promotional communications to you, such as via email, push notification or in-app messaging either with your consent or as otherwise permitted by law. Please see *Section 8: Your Choices About Our Communications With You* for more information.
- We use your account and authentication data to enable unified login and access to all apps included in your bundle subscription. This allows you to move between Scanner App, ESign App, and PDF Forms App without creating separate accounts or subscriptions. We also use shared data to verify your subscription status, provide consistent service access, and maintain accurate billing records across participating applications.
- In any other way, as we may describe when you provide the information or otherwise at your direction or with your consent.
- As permitted or required by law, including for auditing, fraud and security monitoring purposes.
- We may use automated decision-making technologies, including profiling, to improve app functionality, provide personalized content, and optimize advertising. For example, automated profiling may be used to recommend features based on your usage patterns.

  You have the right to:

  - Request more information about any automated decision-making processes,
  - Object to profiling that significantly affects you, and
  - Request human intervention in cases where automated decisions impact your rights under applicable laws.

5. TO WHOM WE DISCLOSE PERSONAL DATA

We may disclose the information we process about you, including any Personal Data, as follows:

- We may disclose your Personal Data, and other data and collected information to trusted third-party organizations such as **contractors, business partners, service providers, and vendors that we use to support our business operations** and who assist us in providing ESign App. These service providers may include:
  - **Microsoft Azure** – subject to their Terms of Use.
  - **OpenAI** – subject to their Business Terms.
- We may disclose your Personal Data to **third-party analytics providers and advertising partners** or otherwise permit them to collect or access it. For more information, please see *Section 6: Cookies, Software Development Kits, and Other Tracking Technologies*.

  These analytics providers may include:
  - **Amplitude** – subject to their Terms of Service.

- **AppsFlyer** – subject to their Terms of Use.
- **Firebase** – subject to their Terms of Service.
- **Appfigures** – subject to their Terms of Use.
- **Facebook Pixel** – subject to their Facebook Terms and Policies.
- **Google Ads** – subject to their Google Ads Terms and Conditions.

- We may disclose your Personal Data in the event that we or any of our affiliates, subsidiaries or lines of business is **merged, acquired, divested, financed, sold, disposed of or dissolved**, including in the course of a transaction like a merger, divestiture, restructuring, reorganization, acquisition, bankruptcy, dissolution, or liquidation. In such cases, your Personal Data and any other collected information may be among the items sold, transferred, or otherwise disclosed as part of that transaction or proceeding.
- We use **Stripe** as our third-party payment processor. All payment-related information, including card details, billing address, and other financial data, is provided directly by you to Stripe and is not stored, processed, or accessed by us at any point. Stripe independently collects, processes, and stores your payment information in accordance with its own privacy policy and terms of service**.** We do not retain any sensitive payment data submitted through Stripe forms. For more information, please refer to Stripe's Privacy Policy and Stripe Connected Account Agreement.
- We may disclose your Personal Data **in response to legal requests and for purposes of preventing harm.** We may access, preserve and share your information in response to a legal (like a search warrant, court order or subpoena), government or regulatory request if we have a good faith belief that the law requires us to do so. This may include responding to legal, government or regulatory requests from jurisdictions where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: (i) detect, prevent and address fraud and other illegal activity; (ii) protect ourselves, you and others, including as part of investigations; and (iii) prevent death or imminent bodily harm. Information we receive about you may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm.
- **Payments and Data Processing**. We do not collect, store, or directly process sensitive payment details such as credit card numbers, expiration dates, or CVV codes. All payment transactions are securely handled by third-party payment providers, including Stripe, in accordance with their respective terms of service and privacy policies. We recommend reviewing the Stripe Privacy Policy for detailed information.

  While payment details are exclusively processed by these providers, we may process limited metadata related to transactions. This includes transaction IDs, payment status,

or non-sensitive identifiers necessary for order confirmation, fraud prevention, service continuity, and compliance with applicable legal or regulatory requirements. These activities are carried out with strict adherence to data protection laws and solely for purposes directly related to service provision.

We encourage you to review the privacy policies of Apple Pay and Stripe for comprehensive details on how your sensitive payment data is managed. For questions or further assistance, please contact our Support team at support@e-sign.co.

- If you use Bundle Subscription, your personal data may be shared between Municorn Limited's affiliated applications (Scanner App, ESign App, and PDF Forms App) solely for authentication, subscription verification, and technical support purposes. This data is never shared with third parties for unrelated purposes.

6. COOKIES, SOFTWARE DEVELOPMENT KITS, AND OTHER TRACKING TECHNOLOGIES

Analytics providers. When you Use ESign App, we and our service providers, vendors, and partners, including third parties, may use technologies to collect or receive certain information about you and/or your Use of ESign App. We also use third-party analytics tools like Google Firebase, AppsFlyer, and Amplitude to help us measure traffic and usage trends for ESign App and for other purposes. Such analytics tools collect information via third-party SDKs incorporated into ESign App, which includes information about features of ESign App you visit or Use, your actions in ESign App, and information about your subscription. Such information may be used to provide content, advertising, or functionality or to measure and analyze ad performance on ESign App or other websites or platforms. Third parties may also use such information for their own purposes. For the avoidance of doubt, we do not use Image Data for advertising purposes.

Interest-based Advertising. We may partner with ad networks and other ad-serving providers that serve ads on behalf of us and others on non-affiliated platforms. Some of those ads may be personalized, meaning that they are intended to be relevant to you based on information ad networks and ad serving providers collect about your Use of the app over time, including information about relationships among different browsers and devices. This type of advertising is known as interest-based advertising.

Consumption Information. We collect and process consumption data by default to assist Apple in evaluating refund requests, ensuring compliance with applicable laws and regulations, including GDPR and CCPA. By accepting our Privacy Policy, you agree to this data collection and sharing practice.

If we receive a refund request for an in-app purchase, we may provide Apple with information about your in-app purchase activity.

This data may include:

- **Account Tenure**: the duration of your account's existence;
- **App Account Token**: an anonymous account identifier used for the transaction;

- **Consumption Status**: the extent to which the in-app purchase was used or consumed;
- **Delivery Status**: confirmation of whether the purchased content was successfully delivered;
- **Lifetime Dollars Purchased**: the total amount spent on in-app purchases in our app, in USD;
- **Lifetime Dollars Refunded**: the total amount refunded to you for in-app purchases, in USD;
- **Platform**: the platform where the in-app purchase was consumed;
- **Play Time**: the total time spent using our app;
- **Sample Content Provided**: whether a free trial or sample of the in-app purchase was available before purchase;
- **User Status**: the current status of your account.

We process this data solely to assist Apple in evaluating refund requests, ensuring compliance with applicable laws and regulations, including GDPR and CCPA. Users can withdraw their consent to this processing at any time through the app settings or by contacting us.

Users can withdraw their consent to this processing at any time by adjusting the app settings: **Open the App > Go to Settings > Analytics > Toggle Off "Share consumption information".**

For further assistance or to withdraw consent directly, users can also contact us via support@e-sign.co.

Your Choices. Most browsers and devices are configured to accept cookies and similar tracking technologies automatically. You may be able to set your browser and device options so to limit such technologies. You can visit the Digital Advertising Alliance ("DAA") Web choices tool at www.aboutads.info to learn more about this interest-based advertising and how to opt out of this kind of advertising by companies participating in the DAA self-regulatory program, and http://www.aboutads.info/appchoices for information on the DAA's mobile app opt-out program. You can also opt out of receiving interest-based ads from members of the Network Advertising Initiative ("NAI") by visiting the NAI consumer opt-out page at http://optout.networkadvertising.org/?c=1#!/. Opting out of receiving interest-based ads does not mean that you will no longer receive ads from us, but rather that the ads will not be tailored to your perceived interests.

For users in the European Economic Area, United Kingdom and United States. You can opt out from processing of Personal Data via cookies, SDKs and other tracking technologies by clicking sending a request to support@e-sign.co.

You may find that some parts of the app may not function properly if you have refused certain tracking technologies, and you should be aware that disabling certain tracking technologies may

prevent you from accessing some of our content. Your choices are typically device and browser-specific.

We honor Global Privacy Control (GPC) signals as required by U.S. and international privacy laws. GPC is a browser or device setting that allows you to control the sale or sharing of your personal data. If GPC is enabled on your device, we will process it as a valid opt-out request under applicable laws. For more information on enabling GPC, please visit globalprivacycontrol.org.

7. YOUR RIGHTS IN RELATION TO YOUR PERSONAL DATA

Access, modification, correction and erasure. You can send us an email at support@e-sign.co to request access to, modification, correction, update, erasure or portability of any Personal Data that you have provided to us and that we have about you. You can also request deletion of your account inside the app, both for iOS and Android users. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

EEA/UK individuals. Individuals in the European Economic Area ("**EEA**") and the United Kingdom ("**UK**") have certain statutory rights in relation to their Personal Data including under the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EEA GDPR**") and the UK version of the EEA GDPR ("**UK GDPR**") (collectively, the "**GDPR**"), including the rights specified below. You can exercise these rights by contacting us (for contact information, please see *Section 15: How to Contact Us*. We will do our best to accommodate your request or objection, but please note that not all rights are absolute.

- **Access to your Personal Data:** You have a right to request information about whether we have any Personal Data about you, and to receive a copy of such Personal Data.
- **Rectification of your Personal Data:** You are responsible for ensuring the accuracy of your Personal Data that you provide to us. Inaccurate information may affect your experience when Using ESign App features and our ability to contact you as described in this Privacy Policy. If you believe that your Personal Data is incomplete or inaccurate, you have a right to contact us and ask us to correct such Personal Data.
- **Restriction of processing:** You also have the right to demand restriction of processing of your Personal Data, for example, if you contest the accuracy of the Personal Data which inaccuracy is verified by us.
- **Erasure of your Personal Data:** In certain circumstances, you may ask us to erase your Personal Data. Please be aware that erasing some Personal Data may affect your ability to Use ESign App.

- **Right to portability of your Personal Data:** In certain circumstances, you have the right to request us to receive any Personal Data you provided us in a structured, commonly used and machine-readable format. You may further ask us to give that Personal Data to another party.
- **Right to object to processing or otherwise using your Personal Data:** Where we are processing your Personal Data based on our legitimate interest, you may object to the processing or otherwise using your Personal Data. Please be aware that our inability to process or otherwise use some of your Personal Data may affect your ability to Use ESign App. If you have opted in to receiving marketing communications, you have the right to opt out of those at any time.
- **Right to withdraw your consent at any time:** Where you may have provided your consent to the processing of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. The withdrawal of your consent does not affect the lawfulness of the processing based on your consent before its withdrawal.
- **Right to lodge a complaint with a supervisory authority:** Subject to the GDPR, you have the right to lodge a complaint with a local data protection authority in the country of your residence, where you work or where an alleged infringement of the applicable data protection law took place. Please see a list of EU member states' supervisory authority here, and the UK's supervisory authority (ICO) here.
- **Rights related to Automated Decision-Making and Profiling.** You have the right to request more information about any automated decision-making processes. Apart from that, you may object to profiling that significantly affects you, and you may request human intervention in cases where automated decisions impact your rights under applicable laws.

Please keep in mind that we accommodate your requests free of charge. However, if your request is manifestly unfounded, excessive, or repetitive, we may charge a reasonable fee or refuse to act on the request.

Besides, in case of a vague request to exercise any of the aforementioned rights we may engage with you in a dialogue to ask for more details if so needed to complete your request. In case this is impossible, we reserve the right to refuse to grant your request.

Following the provisions of the applicable law, we might also ask you to prove your identity (for example, by requesting your username or some other proof of your identity) in order for you to invoke the mentioned rights. This is made to ensure that no right of third parties is violated by your request, and the mentioned rights are exercised by an actual Personal Data subject or an authorized person.

Consent for Third-Party Data. If you include third-party personal data in your uploaded documents, you are responsible for obtaining the necessary consent from those individuals before sharing such data with us.

Prohibited Content and User Responsibility

By using this app, you agree not to upload any illegal, harmful, or unlawful content, including but not limited to:

- **Personal data** of third parties without their consent,
- **Sensitive personal data of third parties**, such as medical, financial, or biometric data, unless you have explicit consent,
- **Infringing content**, including but not limited to copyrighted material, trademark violations, or any content that breaches intellectual property rights,
- **Defamatory or offensive material**, including hate speech, threats, or discriminatory content,
- **Pornographic,** sexually explicit, or obscene content,
- **Fraudulent or deceptive content**, such as phishing attempts, scams, or misleading information.

Uploading such content is done at your own risk and responsibility. You are solely responsible for ensuring that the documents you upload do not contain illegal or unlawful material or content you do not have the right to share.

If we become aware of any unlawful content in the documents uploaded by users, we reserve the right to report such content to the relevant authorities for further investigation. This may include providing user-uploaded content or other relevant information to law enforcement or other regulatory bodies, as required by law.

We do not bear responsibility for any legal consequences arising from the uploading of prohibited content.

Manage your privacy rights. To enhance your experience, we provide in-app tools to manage your privacy rights, such as:

- Accessing your personal data,
- Deleting your account and associated data,
- Managing consent for tracking and analytics technologies.

For additional assistance, contact us at support@e-sign.co.

Requests related to personal or other data. If you are an individual in the EEA or UK, we will respond to your requests without undue delay and at the latest within one month from the date we receive your request. If your request is complex or if we receive a large number of requests,

we may extend this period by an additional two months. In such cases, we will inform you of the extension and the reasons for the delay within the initial one-month period.

In any other case, we will process your requests related to personal data within 45 days from the date we receive them. If additional time is required due to complexity or volume of requests, we may extend this period by an additional 45 days. In such cases, we will notify you within the initial 45-day period.

You may submit your request by contacting us at support@e-sign.co or through the app's privacy settings.

8. YOUR CHOICES ABOUT OUR COMMUNICATIONS WITH YOU

Necessary communications. If you are using ESign App you may receive electronic communications from us (e.g., by posting in-app notices in ESign App, push notifications or emails). We send some of these communications to you, such as those related to your subscriptions, technical and security notices and updates to the Privacy Policy and Terms of Use, where necessary to perform our contract with you to provide ESign App or otherwise based on our legitimate interest in contacting you.

Third-Party Recipients. If you choose to enter and use the email address of a third party (e.g., to send an invoice or estimate), you are solely responsible for ensuring that you have obtained the necessary consent from that person, as required by applicable data protection laws. We do not verify or validate the ownership of recipient email addresses entered by users.

OTP Delivery. For authentication purposes, we may send you a One-Time Password (OTP) via email. These emails are also processed via the providers mentioned above and initiated only by user request (e.g., during login or identity verification).

Marketing & Promotional Emails. If you wish to opt-out of our promotional and marketing emails, you can do so by following the opt-out links in any marketing email sent to you or by contacting us at support@e-sign.co.

If required by law, we will ask for your consent to send you promotional and marketing emails, in-app communications and push notifications about new products, features or offers from ESign App.

Push Notifications. If you wish to opt-out of push notifications, you can do so through your mobile device settings by tapping "Settings" -> "Notifications" -> Choose ESign App - > press the toggle to allow or forbid push notifications from the app.

9. DATA SECURITY

We use reasonable and appropriate information security safeguards to help keep your Personal Data secure and, in an effort, to protect it from accidental loss and unauthorized access, use,

alteration and disclosure. Unfortunately, the transmission of information via the internet is not completely secure. Although we take measures to do our best to protect your Personal Data, we cannot guarantee the security of the collected information transmitted to or through ESign App or an absolute guarantee that such information may not be accessed, disclosed, altered, or destroyed.

Any transmission of your Personal Data is at your own risk. We are not responsible for the circumvention of security measures contained in ESign App. Please understand that there is no ideal technology or measure to maintain 100% security.

The safety and security of your information also depends on you. For instance, we are not responsible for how you choose to share the photos or other information processed in your ESign App account, such as via social media services. We are not responsible for the functionality, privacy, or security measures of any other organization.

While Municorn Limited is not a covered entity or a business associate under the U.S. Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), we voluntarily adopt safeguards and security practices aligned with the HIPAA Security Rule to help protect personal and sensitive health-related data that may be shared through ESign App.

If you believe your data has been compromised, please contact us immediately at support@e-sign.co.

10. DATA RETENTION

We generally retain most of your Personal Data until you delete your ESign App account or as otherwise required by law.

Specific retention periods include:

- **User account data.** Retained until account deletion.
- **Payment and transactional data.** Retained for seven (7) years for compliance with financial and tax regulations.
- **Uploaded documents**. Retained on our servers for as long as needed to provide requested services. Users may delete documents at any time via the app’s settings.
- **Analytics and usage data.** Retained in anonymized form for business purposes.
- **Signatures**. Stored locally on user devices and never uploaded unless explicitly shared.
- **Data related to your unified account and Bundle Subscription**. Retained for as long as your account remains active and is necessary for providing access to all Municorn Apps. If you delete your account or cancel your subscription, the associated data will be removed or anonymized across all connected applications.

You may request account deletion by contacting support@e-sign.co or using the in-app functionality.

Even if we delete some or all of your Personal Data, we may continue to retain and use anonymized data previously collected that can no longer be used for personal identification.

11. CROSS-BORDER DATA TRANSFERS

Certain of our service providers are incorporated in the United States. Accordingly, your Personal Data may be transferred to and stored in the United States. Where we transfer Personal Data to organizations in the United States that are certified under the EU–U.S. Data Privacy Framework, such transfers rely on the European Commission's adequacy decision.

Where required under the EEA GDPR, in case of transfers of personal data from the EEA to countries outside the EEA, where we cannot rely on adequacy decisions adopted by the European Commission (for more information, please see here) we ensure appropriate safeguards are in place to guarantee the continued protection of your personal data, particularly by signing the Standard Contractual Clauses of the European Commission (article 46(2)(c) GDPR). For more information on these Standard Contractual Clauses, please see here.

Where required under the UK GDPR, in case of transfers of personal data to countries outside the United Kingdom, we ensure appropriate safeguards are in place to guarantee the continued protection of your personal data, particularly by signing the UK Addendum to the EU Standard Contractual Clauses or the UK International Data Transfer Agreement, whichever is more appropriate in the given situation. For more information on the UK Addendum and the UK International Data Transfer Agreement, please see here. We may also guarantee the protection of your personal data by relying on adequacy decisions adopted or approved by the authorities in the United Kingdom.

Azure servers' usage. As to the location of our servers, we use Azure servers located in the USA for ESign App operation and Google LLC multiregional servers locations, while our analytics operations are processed both on the servers provided by Azure and by Google LLC.

OpenAI usage. We use OpenAI's services to process and analyze user data to improve our app's functionality and user experience. This involves sharing certain anonymized text data from uploaded documents with OpenAI, acting as our data processor. OpenAI processes this data in accordance with our instructions and a Data Processing Agreement (DPA) that complies with GDPR requirements. We ensure that appropriate security measures are in place to protect your data during transmission and processing. You have the right to access, correct, or delete your data processed by OpenAI through our app. For more information on how OpenAI handles data, please refer to their privacy policy.

For further information please contact support@e-sign.co.

12. USE OF UPLOADED DOCUMENTS AND PHOTOS FOR ANALYTICS

What Data We Collect. We may collect anonymized data from uploaded documents that you share with our app. This includes text, images, or any other content from documents that may help train our AI to improve existing features and develop new ones.

We do not intentionally collect personal data from your documents. Users are encouraged to avoid including personally identifiable information (PII) in the documents they upload. While we take steps to anonymize data and protect your privacy, we rely on users to ensure that uploaded documents do not contain sensitive personal information. In the event that such data is inadvertently uploaded, we will take reasonable measures to delete it promptly.

How We Use Your Data. The anonymized data from your uploaded documents helps us enhance our app by refining current features and developing new functionalities tailored to your needs. We do not use any identifiable information from your documents for any purpose other than improving the app's performance and user experience.

Anonymization and Data Security. We take great care to anonymize all data to ensure that it cannot be traced back to any individual. All data processing is carried out with strict adherence to privacy laws, including GDPR and CCPA, as applicable. We implement advanced security measures to protect your data from unauthorized access or misuse.

Data Retention. We retain the anonymized data only for as long as necessary to fulfil the purposes outlined in this policy. You can revoke your consent at any time, and we will cease using your data for analytics immediately.

Deletion. If you revoke your consent, we will immediately stop processing your data for analytics. You may also request the deletion of previously used data that is no longer needed.

Your Rights and Choices. You have full control over your data. You can choose to opt in or opt out of data sharing for analytics purpose through the app's settings at any time. If you choose to opt out, we will stop using your data for analytics, but you will still have full access to the app's features.

To withdraw your consent for sharing uploaded document data, follow these steps:

Open the App > Go to Settings > Analytics > Toggle Off "Share data and analytics".

Transparency and Updates. We are committed to transparency. We will notify you of any changes to our policy regarding the use of uploaded documents, and you will be asked for consent again if necessary.

13. CHILDREN'S PRIVACY

General age limitation. ESign App is not intended for or directed at children under 13, and we do not knowingly collect or solicit any information from anyone under the age of 13 or knowingly allow such persons to Use ESign App. If you are under 13, do not: (i) Use or provide any information in ESign App or through any of its features, or (ii) provide any information about yourself to us, including your name, address, telephone number or email address. If you are a parent or guardian and believe we have collected information from your child who is under the age of 13, please contact us at support@e-sign.co.

If we discover that we have collected data from a child under the applicable age without verifiable parental consent, we will promptly delete that information and take steps to prevent further access to the ESign App.

Age limitation for EEA and/or UK individuals. You must be at least 16 years old in order to Use ESign App. We do not allow Use of ESign App by EEA and/or UK individuals younger than 16 years old. If you are aware of anyone younger than 16 Using ESign App, please contact us (for contact information, please see *Section 15: How to Contact Us*), and we will take the required steps to delete the information provided by such persons.

14. THIRD-PARTY WEBSITES AND SERVICES

We are not responsible for the practices employed by any websites or services linked to or from ESign App, including the information or content contained within them. Where we have a link to a website or service, linked to or from ESign App, we encourage you to read the privacy policy stated on that website or service before providing information on or through it.

15. HOW TO CONTACT US

General contact details. If you have any questions about this Privacy Policy or ESign App, please contact us via email at support@e-sign.co.

Data protection officer. If you are an individual in the EEA or the UK and you wish to exercise your rights under *Section 7: Your Rights In Relation To Your Personal Data*, or you have any questions about this Privacy Policy or ESign App, you can contact our data protection officer via email at support@e-sign.co.

16. CHANGES TO OUR PRIVACY POLICY

The date this Privacy Policy was last revised is indicated at the top of the page. We may modify or update this Privacy Policy from time to time. Some changes do not require your consent. However, if we determine that the changes may pose a risk to your rights and freedoms, we will ask for your consent to those changes separately from this Privacy Policy.