42GEARS PRIVACY NOTICE

We 42Gears Mobility Systems Private Limited and its affiliates and subsidiaries (“Referred to as “we”, “us”, “our”) is the sole owner of (i) the domain 42Gears.com, (ii) its associated websites(s) (Referred to as “Website(s)”) (iii) and any of its corporate business entities or affiliates.

We are committed to respect the privacy and security of its users’ (Referred to as “User(s)”/ “you”/” your”/” yourself” /customer”).

We have established this Notice to inform you about how we handle and process the information that you share with us. Unless otherwise defined in this Privacy Notice, the terms used in this Privacy Notice have the same meanings as in our terms and conditions. The purpose of this Privacy Notice is to outline how we gather, handle, and share your Personal information on our digital places like our website (all together called the "Services"), also through social media, marketing, and other contexts and channels explained in this Privacy Notice. This Privacy Notice doesn't cover or restrict the use or sharing of non-personal details we might collect from you when you use our Services.

Further, we carry out processing of your Personal information in accordance with all the applicable legal statutes and regulations which includes the EU General Data Protection Regulation (“EU GDPR”) i.e. Regulation (EU) 2016/679, UK General Data Protection Regulation (“UK GDPR”) i.e. Regulation (EU) 2016/679 as it forms part of law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act, 2018 and the Data Protection Act, 2018 (UK) as well as the ***Digital Personal information Protection Act, 2023 (India)*** (together “Applicable Law”), as amended, replaced or superseded.

This Privacy Notice also enumerates the measures we take to safeguard the personal information which we obtain and how you can contact us about our privacy and security practices and to exercise your rights regarding your personal information.

By using our services and this website, you acknowledge that you have read and understood the contents of this Privacy Notice.

This Privacy Notice doesn't apply where we handle personal information as a Data Processor (or a similar role like a "Service Provider" under California Consumer Protection Act (CCPA)) on behalf of our business customers or otherwise. When we process personal information for business customers, it is governed by the Data Processing Agreement between us and the customer, and the privacy statement of the relevant customer will apply to you. Please note that we are not accountable for the privacy or data security practices of such business customers, the partners, or other third parties and you should refer to the privacy notice of the data controller on whose behalf we are acting.

Our Role in Processing Personal information

*Depending on the context in which Personal information is processed, 42Gears may act either as a **Data Controller** or a **Data Processor**.*

- *We act as a **Data Controller** when we determine the purposes and means of processing, such as when processing data for website operations, marketing communications, event registrations, recruitment, billing, and customer relationship management.*
- *We act as a **Data Processor** when we process personal information on behalf of our enterprise customers in connection with the use of our products and services. In such cases, the customer acts as the Data Controller, and our processing is governed by the applicable Data Processing Agreement and customer instructions.*

WHAT IS PERSONAL INFORMATION?

With regards to this Privacy Notice, “Personal information”, for the purpose of better understanding, shall include but not be limited to:

- **“Personal information”** i.e. any information relating to an identified or identifiable natural person (Referred to as “Data Subject”); wherein an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Information relating to Your account and use of the Services**, including information provided during registration, purchase, or administration of the Services;
- Information that customers or their authorized users choose to upload, configure, store, or manage through the Services to the extent necessary for the provision and operation of the Services; ;
- **Information collected when You visit our Website(s)**, including information provided voluntarily through website forms, **such as contact details, communication requests, or other information submitted by you**, and **technical information such as Internet Protocol (IP) address, browser type, and interaction with our website**.

WHAT PERSONAL INFORMATION DO WE COLLECT, HOW DO WE COLLECT IT, AND WHY?

a. Data You Share With Us:

When you visit our website or seek to conduct business with us or sign-up for the services, you may be prompted to provide certain personal information including name, email address, mobile number, and geographic location etc. This information is used by us in the following ways:

- To connect with you or to establish communication at your request.
- To collect your email address to subscribe to our newsletters.
- Register for webinars.
- Enquire about our products and services.
- Register or apply to our partner program
- Complete order forms
- Participate in a promotion or other website features
- To administer your account (including when you subscribe and sign up to any of our services).

b. ***Who This Notice Applies To***

This Privacy Notice applies to individuals whose personal information we process, including but not limited to:

- *Website visitors and platform users*
- *Customers and end users of our products and services*
- *Prospective customers and business contacts*
- *Partners, resellers, and service providers*

If You interact with us in any capacity where we collect or process your personal information, this Notice applies to you. Generally, the personal information you provide to us is necessary to provide you with the information you have requested for and to resolve a complaint or address Your query.

We may also collect the personal information disclosed by you on our forums, blogs and testimonials or to any platforms to which you are able to post information and materials including third party services (such as social media channels) and through our any other offerings. We will obtain prior consent to post your name and photograph along with the testimonial. In case, you are not providing us with a consent, we are merely permitted to use your testimonial in a fully anonymized way.

Please note that providing personal information to us is voluntary on your part. If you choose not to provide us certain information, we may not be able to offer you certain products or services, and you may not be able to access certain features provided on our website and products.

In general, the personal information that you are asked to provide, and the reasons why you are asked to provide it, will be made clear to you at the point we ask you to provide your personal information.

c. Automatic Data Collection:

We may collect certain data automatically from your computers or devices (including mobile devices) when you use our website and services. This information does not necessarily reveal your identity directly, but it may include information about the specific device used, such as the hardware model, operating system version, web-browser software (such as Firefox, Safari, or Internet Explorer) and the IP Address/MAC address/device identifier and other technical information. In some countries, including the European Economic Area, this information may be considered personal information under the GDPR. **We process this information for purposes such as operating, maintaining, securing, and improving our website and services, as well as for system administration, analytics, and diagnostics. This information may be stored in log files and used to help us understand how visitors interact with our websites and to ensure the security and reliability of our systems.** Further, we gather information on how your device interacts with our website, products, or services. This includes details such as which pages or features your access, links clicked, time spent on specific pages, interaction data, interaction timestamps, error logs, referring and exit pages, and URLs. Understanding these interactions help us gain insights into our user's behaviors, origins, and interests. We utilize this data for internal analytics and service improvement purposes to enhance the quality, relevance, functionality and security of our offerings.

We may also use this information to **detect, prevent, and investigate potential security incidents or** block IP addresses where there is a breach of the **terms and conditions governing the use** of the website. Some of the data may be collected automatically using tracking technologies, as explained further under the heading “COOKIES”.

REQUESTING INFORMATION OR EVENT REGISTRATION

You may sign up to receive information about our company, our products and services, industry news and information, access our partner portal and register to attend an event. **Where permitted by Applicable Law and based on your consent or our legitimate business interests** , we may send you electronic communications to keep you informed of changes to our products and services **and other relevant updates**.

Your personal information will be accessed by our authorized personnel only to the extent necessary to deliver the requested information **and to**

communicate with you regarding our products, services, or events, in compliance with this Privacy Notice.

We may also provide your personal information to carefully selected third party service providers **who support us in operating our website, hosting webinars or events, managing communications, or providing marketing and customer engagement services**.
These third party service providers **process Personal information solely on our behalf and under contractual obligations that require them to protect the information and use it only for the purposes specified by us and in compliance with applicable Data Protection laws**.
You may opt-out of receiving marketing communications from us at any time by using the unsubscribe link included in such communications or by contacting us using the details provided in this Privacy Notice.

COOKIES

Our website uses "cookies", which are files in text format placed on your (user's) computer, to help the website analyze how users use the site. The cookie provides information about your use of the website for the purpose of evaluating and compiling reports on website activity and internet usage. You may refuse the use of cookies by selecting the appropriate settings on your browser, however, please note that if you do this you may not be able to use the full functionality of this website.

The following are types of cookies we use on our website, For more detailed information, please refer to our Cookie Policy here : *https://www.42gears.com/trust-center/legal/cookie-policy/*

a. ***Essential Cookies:*** These cookies are essential for the website's operation and cannot be disabled within our systems. They are typically activated in response to actions you take, such as adjusting privacy preferences, logging in, or completing forms. While you can configure your browser to block or notify you about these cookies, certain areas of the site may become unavailable. Importantly, these cookies do not retain any personal information.

b. ***Personalized Cookies:*** The website utilizes cookies to enhance user experience by remembering your preferences, like your username, language, or geographic region.

c. ***Analytic Cookies:*** Analytic cookies track and analyze user interactions with a website, including the number of visitors, pages visited, and duration of visits. This data helps website owners understand user behavior, improve site performance, and tailor content to enhance the user experience. Importantly, analytic cookies do not collect personal information. For example, we use Google Analytics cookies to understand how visitors arrive at our website, what they spend their time on, and identify areas such as website navigation and user journey.

1. **How to opt-out**: We provide several options to help you to manage your cookies preferences as detailed in our cookies policy.
   Also, certain third-party service providers, such as Google and YouTube, also offer tools and settings that allow you to control how your data is used for analytics and marketing. For example, you may manage how Google uses cookies and other data through your Google account settings
   You may also directly manage or opt out from third-party service providers using the following links:

Google / YouTube

i. Google Ads Settings: https://adssettings.google.com
ii. Google Analytics Opt-Out Add-on: https://tools.google.com/dlpage/gaoptout
iii. YouTube Privacy Controls: https://myaccount.google.com/yourdata/youtube

LinkedIn

i. Ad Settings: https://www.linkedin.com/psettings/advertising
ii. Cookie Policy: https://www.linkedin.com/legal/cookie-policy

Facebook (Meta)

i. Ad Preferences: https://www.facebook.com/adpreferences

For Customers in the European Union, our processing (use) of your personal information is justified on the following legal basis:
The processing is necessary to perform a contract with you or take steps to enter into a contract at Your request; This is the primary basis of our processing. Further we provide you with the option to disable the cookies before visiting our website However, necessary cookies will be active for the functioning of the website.

DATA COLLECTED THROUGH OUR PRODUCTS AND SERVICES

SUREMDM

a. Usage Data

Where our customers subscribe to our products and services, we collect certain information obtained from downloaded, installed, or accessed software, systems hosting the services, or products and devices accessing these products and services which do not directly identify the end user herein referred to as usage data. We collect this information for business analytics to identify how our products and services are used by our customers in our system or service. The extent of this collection is configurable by our customers, but as an indication, our collection of technical information that constitutes personal data includes (but is not limited to):

IP Address, Email address, Company name, Mobile number, Device Time, Device Model, RAM (Random Access Memory) Information, Storage Information (Used/Free), Bluetooth Information (Name/ Bluetooth MAC), Data Usage details (Wifi, Mobile, Roaming, Non-roaming), Password Strength (Policy on device), Device Notes (Custom entered by user or admin of our system having access to this feature) and, other usage statistics.

We do not collect usage data about Customer's end users, except as necessary for support or to provide the services requested by customers (in which case we are a Data Processor of such data). The information is only processed to provide the service requested by the customer.

b. Location Related Information

We give our users more control over how our applications collect location data from their devices.

Whenever you elect to provide access the location-based information while using our SureMDM Agent, we collect such location data for purposes including, but not limited to location tracking, Geo-Fencing, etc.

With your consent, our products may also collect additional asset-related information such as IMEI, IMSI, Phone Number, Serial Number, etc only for the purpose necessary for support or to provide the services requested by the user.

In addition, some of the features of our product may enable us to access your location in order to customize your experience with the service based on your location ("Location-based Services"). In order to use certain Location-based Services, you must enable certain features of Your device such as GPS, WiFi, and Bluetooth, which will enable us to identify your location through a variety of means, including GPS location, IP Address, and geo-fencing technology, as available. The Location-based Services feature in our products is powered by Google Maps (Please make sure you check and agree with Google Maps https://policies.google.com/privacy?hl=en-US and its terms of use).

In case the user enables the location services and provides explicit consent by enabling the device settings while using our Service, our application will collect location data even when the application is running in the background.

The data stored on your mobile device and the location information to which the mobile applications have access will be used in the context of the mobile application and transferred to and associated with your account in the corresponding services.

c. **Collection and Usage of Installed Application Data**

With clear and explicit consent, the IT administrator may configure SureMDM Agent, SureMDM Agent for Smartwatches, and SureLock for Smartwatch to collect and store information about the applications installed on your managed mobile devices or smartwatches. This includes names of the installed applications, their types, sizes, version names, version codes, and application icons.

We collect this data to perform various operations, such as managing application data, uninstalling apps, enforcing compliance rules based on app installation or removal, initiating app launch on device startup, and facilitating in-house app analytics. These actions help enhance the functionality and security of your mobile devices while providing valuable insights for optimizing your organization's app usage.

Please note that the information we collect, including the names of installed applications, their types, sizes, and version names, will be securely stored on our servers. This information will be available even when the application is running in the background or not actively in use. Such stored information will never be shared with any third party or other applications.

d. **Call Logs Related Information**

With the clear and explicit prior consent of our users, we may further request access or permission to certain features from your mobile devices, including but not limited to your device's call logs, contacts, etc. for the purpose of collecting data for inventory management, call tracking, incoming/outgoing call restrictions and accessing SIM card information for IT administrators.

The administrators may configure SureMDM Agent to collect usage information, such as the number of calls, and statistics (number of calls made or received, duration of calls, contact details, etc.).

The SureMDM Agent will be able to read your call logs including contact name, phone number, and duration of the call which is transmitted and stored in our secure SureMDM server. This information is available even when the application is running in the background or is not actively used. The call log information stored in the server will never be shared with any third party or applications for any reason whatsoever.

e. **SMS Related Information**

With clear and explicit prior consent, the SureMDM may be configured by the IT administrator to collect the text messages sent or received. This information may assist the administrator in managing SMS limits on the user's cellular plan.

Based on how the administrator has configured SureMDM Agent, the data may include:

1. The number of SMS sent or received;
2. Contact name date and time; and
3. Content of the SMS, etc.

The aforesaid collection of the SMS logs is limited to the legitimate purpose(s) mentioned herein and stored in our secure SureMDM server which is never shared or transferred to any third party or applications. This information is available even when the application is running in the background or is not actively used.

f. **Storage Usage**

This is a SureMDM functionality that allows access to a device's internal and external storage. When enabled, SureMDM may collect the contents of the storage device, including the SD card and locally stored files. Also, based on how the user has configured SureMDM Agent, certain functionality may allow administrators to have read, write, delete, modify, and execute access to the device file system.

The Storage Usage information is transmitted and stored on our secure SureMDM server. This allows administrators to download, upload, and execute files on the device remotely, even when the application is running in the background or is not actively used.

For further information about SureMDM Agent's other data collection and purpose(s), kindly have a look at our Security and Compliance Page which talks about the Required App Permissions.

g. **Contacts**

If you choose to enable the functionality of "Contacts", the SureMDM Agent will be able to collect your contact information including contact name, and phone number, even when the app is running in the background or is not actively being used. This will allow your SureMDM Administrator to allow or block the incoming and outgoing calls based on the contact information and remotely delete a contact. Further, contact details will be transmitted and stored on our SureMDM secure server for purposes of generating reports for SMS and Call logs. The data stored in the server is never shared with any third party or applications and is processed only in accordance with applicable privacy regulations, including Art. 6 Para. 1 (f) GDPR based on our legitimate interest.

SURELOCK

We provide our users the ability to control the types of information they collect about user's device:

SureLock will collect the SMS content, Call Logs, Storage, Location, All Files Access in order to function properly and for the purpose of the administrator to change passwords through received SMS Commands, block or allow phone calls, and SMS and others.

Based on how the administrator configured the runtime permissions, the data may include but is not limited to:
SureLock will collect only the "Phone Number" to allow/block the incoming and outgoing calls with call log permission.
SureLock will collect "Name of contact", "content of the SMS" in order to change the android lock screen PIN with SMS permission.
The details are mentioned below:

a. Collection and Usage of Installed Application Data:

SureLock collects detailed information about the apps installed on your device to ensure effective device management and security. This includes data such as app names, icons, package names, app permissions, app types, sizes, version numbers, and version codes. If your device is enrolled in SureMDM, SureLock will securely upload this app information to the SureMDM server. This process occurs automatically, even when the SureLock app is running in the background or when you are not actively using it.

The collection and uploading of app data enables your administrator to efficiently manage the apps installed on your device. Specifically, the data allows your administrator to:

- Create App Allow lists and Blocklists: Control which apps are allowed or restricted on the device, ensuring compliance with corporate or organizational policies.
- View and Modify App Permissions: Monitor app permissions to ensure sensitive data is protected and adjust permissions when necessary to meet privacy and security standards.
- Clear App Data: Remotely clear data stored by apps to free up storage, protect sensitive information, or troubleshoot issues without the need for direct access to the device.
- Run Applications at Device Boot: Enable critical applications to automatically run when the device is restarted, ensuring seamless and uninterrupted functionality.
- In-House App Analytics: Analyze app usage patterns for internal purposes, such as optimizing resource allocation, improving user experience, or ensuring compliance with usage policies.
- Uninstall Apps: Remotely uninstall apps that are unauthorized, outdated, or pose security risks.

SureLock is committed to ensuring the privacy and security of your data. We do not share this information with any third-party applications, services, or vendors. The collected app information is used solely for the purposes of device management, security, and optimization as outlined above and is not used for any other purposes.

b. **Telephone:**

SureLock collects your phone number to support essential device management functions. This is done to ensure that your device can be effectively managed and monitored as part of your organization's mobile device management system. If your device is enrolled in SureMDM, SureLock will securely upload your phone number to the SureMDM server. This process occurs automatically, even if the SureLock app is running in the background or when you are not actively using it.

The collection and secure transmission of your phone number enable your administrator to:

- Manage Device Inventory: Accurately track and maintain an inventory of devices based on unique identifiers such as phone numbers, ensuring the efficient management of organizational resources.
- Configure Device Names: Use the phone number as part of the process to configure or update device names, allowing administrators to easily identify devices within the SureMDM system.
- Monitor SIM card Changes: Detect and receive alerts when a SIM card change is detected on your device, which helps maintain security by preventing unauthorized usage or access.

This telephone data is critical to ensure that your device remains compliant with your organization’s policies and is effectively secured against potential risks, such as unauthorized access through SIM swapping.

Please rest assured that SureLock does not share your phone number with any third-party applications, services, or vendors. The collected phone number is strictly used for the purposes outlined above.

c. **Call Logs Related Information:**

With the clear and explicit prior consent of our users, we may further request access or permission to certain features from your mobile devices, including but not limited to your device's Call logs, Contacts, etc. for the purpose of collecting data for inventory management, call tracking, incoming/outgoing call restrictions and accessing SIM card information for IT administrators.

The administrators may configure SureLock to collect usage information, such as the number of calls, statistics (number of calls made or received, duration of calls, contact information etc.). The SureLock will be able to read your call logs including contact name, phone number, duration of the call which is transmitted and stored in our secure server. This information is available even when the application is running in the background or is not actively used. The call log information stored in the server will never be shared with any third party or applications for any reason whatsoever.

d. **SMS Related Information:**

With clear and explicit prior consent, SureLock may be configured by the IT administrator to collect the text messages sent or received. This information may assist the administrator in managing SMS limits on the user cellular plan.

Based on how the administrator has configured SureLock, the data may include:

- The number of SMS sent or received
- Contact name date and time
- Content of the SMS, etc.

The aforesaid collection of the SMS logs is limited to the legitimate purpose(s) mentioned herein and stored in our secure server which is never shared or transferred to any third party or applications. This information is available even when the application is running in the background or is not actively used.

e. **Contacts:**

If you choose to enable the functionality of “Contacts”, SureLock will be able to collect your contact information including contact name, phone number, even when the app is running in the background or is not actively being used. This will allow your SureLock Administrator to allow or block the incoming and outgoing calls based on contact information and remotely delete a contact.

Further, contact details may be transmitted and stored on our secure server for purposes of generating reports for SMS and Call logs. The data stored on the server is never shared with any third party or applications and processed only in accordance with applicable privacy regulations, including Art. 6 Para. 1 (f) GDPR based on our legitimate interest.

To gain a comprehensive understanding of our SureLock’s privacy information, please refer here. It contains all the necessary details and will provide you with a clear understanding of our privacy practices.

SUREVIDEO

a. Access to All Files Permissions

SureVideo has the ability to read all your files on the device storage (including all the documents, pictures, and music), which allows the administrator to remotely configure application settings, set up a custom album view, and add playlists.
Allowing SureVideo to have file system access allows you to use the full functionality for the aforementioned purpose(s).
SureVideo will request this access, and you can choose to allow or deny the request as per your preference. SureVideo maintains privacy by not sending or storing this data to its server. Further, SureVideo doesn't transfer or share this information with any other third-party application for any reason whatsoever.

b. **Location Permission**

If enabled, SureVideo will be able to read your location data which includes access to your precise and approximate location. The location data is collected to allow your SureVideo administrator to search and connect to the desired network via the Wi-Fi center plugin. The location data captured shall never be shared by SureVideo with any other third-party application.
No location data is sent or stored in the server as the data is merely required to derive the scan results to connect to the desired Wi-Fi network.

c. **CamLock Permissions**

We use similar app permissions such as Accessibility settings, background location, runtime permissions, etc to function Camlock properly which is a part of our SureMDM Product. For further details, please refer here.

Product/ Platform	Processing Activity/ Feature	Personal information Collected	Purpose(s) of Processing	Conditions/ Configuration	Hosting/ Storage Location	Sharing/ Disclosure	Additional Notes
SureAsset	Asset Management	Asset Tag; Serial Model; Supplier; Purchase information	Asset lifecycle management for IT	Permission based (user should have required permissions)	MongoDB	Not shared externally	
	Admin User Management	Name; email; role; ; phone; time zone; language; last login; IP Address; User agent; creation and modification Metadata	Platform administration ; system management; support operations	Super admin and admin roles	MongoDB	Not shared externally	Separate admin database; authorized login via Google; tracking of admin sessions
	User Synchronization (LDAP/AD)	Username; email address; LDAP attributes	Directory integration	Configured per customer	MongoDB/LDAP	LDAP/AD systems	Encrypted credentials
	License Management	Software Name; Category; Company; No of license; serial number; supplier; order number; purchase date; Termination Date	License Management	User should have required permissions	MongoDB	Not shared externally	
	Components and Accessories	Name; serial number; category; quantity; model no.; purchase date; purchase cost; order number	Components & Accessories Management	User should have required permissions	MongoDB	Not shared externally	

	Email Service (AWS/SES)	Sender email; recipient email(s); CC recipients; reply-to address; email content	Transactional emails; notifications; alerts	Email (email_service_enabled: true)	AWS/SES	Emails processed through AWS SES	Credentials: email_key_ID; License tracking for email quota
	Custom SMTP Email Service	Sender email; recipient email(s); SMTP configuration details	Alternative email delivery using customer SMTP servers	Configured per customer in Account Settings)	Customer SMTP servers	Emails routed through customer-configured SMTP	Supports custom SMTP for email-sensitive organizations
	Lead Generation Integration (Odoo CRM)	Name; email; company name; contact details; country; state; zipcode; phone	Sales lead tracking; customer relationship management	Enabled if odoo_lead_generation_enabled:	Odoo CRM instance (odoo_url configured)	Customer signup data shared with Odoo CRM for lead management	Odoo endpoint: 42Gears stage/production; configurable per environment
SureMDM Hub	Intercom Integration (Optional)	Full name, work email, password, company name, phone number, country, state, zip/postal code	Registration; account creation; billing; invoicing; license issuance	-	Hosted in Singapore and United States	-	Retained while active; suspension up to 6 months + 3-month grace; then deleted
	Administrator Activity Logs	Email addresses of partner administrators and end customers	Chat support; Customer communication	Disabled by default; enabled at the option of partner	Shared with Intercom (United States)	Shared with Intercom	Partner responsible for notice
	Marketing Preferences	User actions; login timestamps	Console auditing; accountability	-	Hosted in India	-	-
	End Customer Registration	Consent preferences	Marketing communications	Opt-in	Hosted in Singapore	-	-
	Security Measures	Company name; first name; last name; work email; password; domain name; phone number; country; state; zip/postal code	Registration; account creation; enable access	Data residency selected by partner	AWS/GCP in selected region	Accessible to partner admin & 42Gears system admins	Governed by DPA; partner responsible for lawful basis
	Distributor Sign Up	-	Data protection	-	Geo-redundant AWS/GCP	-	RBAC; TLS/HTTPS; secure API keys; audit trails; disaster recovery; encryption at rest;

							vulnerability management; security monitoring; incident response procedures
SuperHub	Hub Account Creation	Full name; company name; country; phone number; optional state/zip	Account provisioning; onboarding; license management; platform administration	-	AWS location as opt-in by the Distributor and Odoo		No sensitive data; no automated decision-making; automated order approval disabled by default
	User Creation	Company name; email; password; name; country; phone; optional state	Same as above	-	AWS location as opt-in by the Distributor and Odoo	-	-
AstroContacts	Contact Directory	Username; first name; last name; email; password; phone number	Platform administration	-	Google Firebase	-	-
	Account & Credentials	Employee names; phone numbers; email addresses; job titles; department; designation	Shared directory; internal communication	Admin controlled	Google Firebase		Removed upon logout/account removal; retained during subscription
	Partner & Lead Data	Organizational account information; administrator credentials	Platform operation and security	-	Odoo	-	-
	Custom Directory	Username; First Name; Last Name; email; Password; Phone Number; Custom Fields	Contact management; internal directory services; user-defined data capture based on organizational needs	End User / Admin controlled (including creation and management of custom fields)	Google Firebase	Not Shared, Stored on User Local Device	-
COSMOS Partner Portal	Partner & Lead Data	Name; business email; job title; company name; telephone number;	Partner management; billing; forecasting;	-	Odoo CRM	Accessible to authorized internal teams	-

		voluntarily submitted information	trend analysis; renewal management; marketing; sales; lead/opportunity management				
Artificial Intelligence (AI) Chatbots	Chat Interaction Data	Message text; any Personal information contained in messages	Operate; improve; monitor chatbot; escalation; QA; troubleshooting; security	User interaction	Customer data processed by our AI systems is stored in secure, dedicated environments and maintained in strict logical isolation. Reasonable technical and administrative safeguards are enforced at the infrastructure level to ensure data confidentiality and integrity, and to prevent any unauthorized access, disclosure, or cross-customer data visibility."	Reviewed by authorized personnel if required	Authorized personnel may contact user if necessary
SureIdP	User Management	Username; Email ID; Phone Number; User ID; Domain	Creation and management of user identities	Configured via Admin Console or synced from external IdPs	As opt-in by the customer while sign up in SureMDM	Shared with integrated services (MDM; Single Sign-On (SSO) applications)	Supports manual and automated provisioning
	Authentication (Login & MFA)	Username; Password (hashed); MFA data (TOTP secret; email; phone)	User authentication and secure access control	MFA enabled at domain or user level; method configurable	As opt-in by the customer while sign up in SureMDM	Not shared externally except with MFA delivery providers (Email/SMS gateways)	Data stored securely with encryption; supports TOTP; Email; and SMS-based MFA
	Device Binding	Device Identifiers (IMEI; Serial Number; MAC Address); Username	Association of users with devices for access enforcement	Configured manually; via CSV upload; or automated enrollment		Shared with SureMDM for device-level policy enforcement	Supports single-device and multi-device policies
	OS Login Integration	Username; Device ID; Login Activity	Enable OS-level	Requires device enrollment and policy		Accessible to authorized admin	Supports Windows; macOS; and Linux

Note: For more information on product-related privacy, visit Our Trust Center, where You'll find detailed privacy policies for some of our products, covering privacy practices adopted comprehensively within the product. Please refer to the link: https://www.42gears.com/trust-center/privacy/

INFORMATION FROM APPLICATION LOGS AND MOBILE ANALYTICS

We collect certain technical and usage information about your use of our products, services and mobile applications from application logs and in-house usage analytics tools. We use this information **to operate, maintain, secure, troubleshoot, and improve the performance and**

functionality of our products and services, and to better understand how our customers use the services. This information may include **technical and usage data such as** clicks, scrolls, features accessed, access time and frequency, errors generated, performance data, storage utilized, user settings and configurations and **information about the devices used to access the services, such as device type, operating system, and approximate location derived from IP Address.**

Such information is generally collected in aggregated or pseudonymized form where feasible and is used primarily for product analytics, service reliability, and security monitoring

OTHER DATA

42Gears may record and process communications between you and our sales or customer support representatives, including communications conducted via email, telephone, chat, or other electronic channels, for legitimate business purposes. These purposes include service quality assurance, training, dispute resolution, security monitoring, compliance, and improving customer support and service delivery.

Such processing is conducted in accordance with Applicable Law and, where required, subject to appropriate notice and consent obligations.

Where permitted by Applicable Law and, where required, based on your consent, we may disclose your personal information to third parties that act as separate and independent Data Controllers.

These third parties independently determine the purposes and means of processing your personal information. Accordingly, their processing is governed by their own privacy notices and policies, and not by this Privacy Notice.

We do not exercise control over, and shall not be responsible or liable for, the processing of personal information carried out by such independent controllers. Each such party is solely responsible for ensuring compliance with applicable Data Protection laws, including the handling of data-subject rights requests.

You should consult the relevant third party's Privacy Notice for further information on how your personal information is processed.

INFORMATION THAT WE COLLECT FROM THIRD PARTIES

- ***Signups using federated authentication service providers:***

  You can log in to our services using supported sign in services such as Microsoft and Google. These services will authenticate your identity and provide you with the option to share certain personal information with us, such as your name and email address and any other personal information you have authorized in your profile settings.

  We collect this information to give you access to the services and personalize our services.

- ***Referrals:*** In case if someone has referred any of our products or services to you through any of our referral programs, that person may have provided us your name, email address and other related personal information. you are free to ask us for the deletion of this data. The information collected will merely be used for the specific purpose for which it was collected.

- ***Information from our resellers and service providers:*** If you contact one of our authorized resellers, distributors, or service partners or otherwise express interest in any of our products or services to them, they may pass your name, email address, company name and other information to us. If you register for or attend an event that is sponsored by us, the event organizer may share your information with us subject to the organizer's privacy practices. We may also receive information about you from review sites if you comment on any review of our products and services, and from other third party service providers that We engage for marketing our products and services.

- ***Information from social media sites and other publicly available sources:*** We may collect your publicly available information, including profile information such as when you provide your feedback or reviews about our products, interact, or engage with our marketplaces, review sites or social media sites such as Facebook, Twitter, LinkedIn, Google and Instagram through posts, comments, questions and other interactions.

  We collect such information to allow us to connect with you, improve our products, better understand customer's reactions and issues, or publish your feedback on our websites. Further, in case You delete the data from the mentioned sites, the information may remain with us to update it.
  We retain such publicly available information only for as long as necessary to fulfil the purposes described in this Privacy Notice or as required by Applicable Law.

  For Customers in the European Union, our processing (i.e., use) of your personal information is justified based on one or more of the following legal grounds:

- **Your consent,** where you have provided consent for a specific purpose; or
- **Our legitimate interests**, including our interest in communicating with prospective customers, improving our products and services, and conducting and developing our business activities, **provided that such interests are not overridden by your fundamental rights and**

freedoms.

SHARING OF THE DATA

We do not sell your personal information under any circumstances to the third parties and do not intend to disclose personal information about you unless stated herein, at the time of collection, or where required or permitted by Applicable Law. 42Gears may share personal information in the following circumstances:

- with our Affiliates and subsidiaries, in connection with any of the uses of your personal information set out in this Privacy Notice;
- third-party services providers, suppliers, agents, and other organizations who provide data processing services to us (for example, to support the delivery of, provide functionality on, or help to enhance the security of our services), or who otherwise process personal information on our behalf for purposes that are described in this Privacy Notice or notified to you when we collect your personal information (such as payment processing, tech support, CRM, marketing tools, analytics, research, customer support, fraud prevention and legal services);
- to our authorized resellers, distributors, and other channel partners in order to process your order or sales enquiry, manage your subscription, provide technical or customer support, advise of upcoming product or service subscription expiry and renewal dates, or as otherwise notified to you when we collect your Personal information;
- when sharing your data is essential to deliver a product, service, or requested information;
- to keep you informed about the latest product releases, software updates, special offers, or other relevant information from our business associates;
- with our customers and partners to inform them about their users' utilization of our services, such as credential acquisition or course completion;
- with our collaborative marketing and sales partners, as well as other business associates who aid in our business operations or other facets of our enterprise, for purposes outlined in this Privacy Notice;
- to any other person with your consent to the disclosure

All such sharing is conducted under contractual, technical, and organizational safeguards consistent with applicable Data Protection laws.

Except as set out above we will not disclose your personal information save where we need to do so in order to enforce our End User License Agreement, our rights generally, or where required or permitted by Applicable Law.

Whenever we share personal information, we take all reasonable steps to ensure that it is treated securely and in accordance with this Privacy Notice.

SUPPORT SERVICES AND THIRD-PARTY PLATFORMS

When you contact us through our customer support channels, (42Gears Website or Knowledge Base), we collect and process certain personal information to address your inquiries, resolve issues and improve our support services.

1. *Live Chat (Intercom)*

When you initiate a chat session via the SureMDM console or Our Website (including Knowledge Base), the following information is automatically collected:

- Identity & Contact Details: Name and email address
- Technical & Device Information: IP Address, browser type and version, operating system, and device identifiers
- Location Data: Approximate location derived from your IP Address
- Session & Conversation Metadata: Timestamps, session activity and interaction history

When you are logged into the SureMDM console, certain account-related contextual information may also be associated with your conversation to facilitate effective troubleshooting.

2. *Email & Web-Based Support (Freshdesk)*

(a) Email Support

When you contact us via our support email address, the following information is captured upon ticket creation:

- Email address of the requester
- Email subject line and message content
- Ticket metadata (ticket ID, timestamps, status)

Additional Personal information (such as name, phone number, or job title) may be incidentally collected if included in your email signature or message body.

(b) Support Request Form

When you submit a request through our online support form (https://www.42gears.com/support/submit-a-ticket/), we collect:

- Name
- Email address
- Phone number
- Details of your support request

3. Contact Enrichment & Profile Management

Freshdesk includes a Requester Widget that displays contact profile information such as name, email address, and configured custom fields (e.g., department or internal identifiers) within the ticket interface. Our support team may update or maintain these fields to organize customer records and streamline support operations.

The messages and data exchanged are stored within the Intercom application and Freshdesk systems in accordance with their respective Data Protection and retention practices. For more information on the privacy practices of Intercom and Freshdesk, please visit https://www.intercom.com/terms-and-policies#privacy and https://www.freshworks.com/privacy/1-jan-2020/ respectively.

We do not make use of these messages or data other than to follow up on users registered issues or inquiries. Your personal information will be processed and transmitted in accordance with applicable regulation, and you can also request us to delete the stored data as provided in this Privacy Notice.

We may also use Intercom as a medium for communications, either through email, or through messages within our services. As part of our service agreement, Intercom collects publicly available contact and social information related to you, such as your email address, gender, company, job title, website URLs, social network handles and physical addresses, to enhance your user experience.

Intercom's visitor data is automatically deleted after 9 months from the last incidence of you visiting our websites.

Intercom is committed to and has implemented GDPR compliance in their tools, you may read Intercom's privacy policy and GDPR commitment here: https://docs.intercom.com/pricing- privacy-and-terms/data-protection/how-were-preparing-for-gdpr.

"DO NOT TRACK" SIGNALS UNDER CALIFORNIA ONLINE PROTECTION ACT (CalOPPA)

Some internet browsers have enabled Do Not Track (DNT) features, which sends out a signal (called the DNT signal) to the website that you visit indicating that you don't wish to be tracked. This is different from blocking or deleting cookies, as browsers with a Do Not Track feature enabled may still accept cookies. No industry standard currently exists on how companies should respond to Do Not Track signals, although one may develop in the future. our website is not currently designed to recognize and respond to Do Not Track signals.

SECURITY

The nature of our services is such that we share responsibility with our customers for the security of data.

We aim to safeguard and protect your personal information from unauthorized access, improper use or disclosure, unauthorized modification or unlawful destruction or accidental loss, and have adopted reasonable technical and organizational security measures.

It is nevertheless important that our customers recognize their responsibility in maintaining effective security in the use of our services. While we will use all reasonable efforts to safeguard your personal information, you acknowledge that the use of the internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any Personal information that is transferred from you or to you via the internet.

In the event of a personal information breach that is likely to result in a risk to the rights and freedoms of Data Subjects, we will assess the incident promptly and take appropriate remedial action. Where required under applicable Data Protection laws, we will notify the relevant supervisory authority and affected individuals within the prescribed timelines. We maintain internal incident response procedures to ensure timely identification, investigation, containment, and reporting of such incidents.

NOTICE TO END USERS

Many of our products or services are intended to be used by the organization or made available through an organization (e.g., Your employer), that organization is an administrator of the services who is responsible and has control over how personal information is processed within all the related accounts and/or services. In such a scenario, please direct your data privacy related questions to your administrator, as your use of the services is subject to that organization's policies. We don't hold any responsibility for such privacy or security practices of an administrator's organization, which might be different from this Notice.

Administrators are able to:

- require you to reset your account password.
- restrict, suspend or terminate your access to the services.
- access information in and about your account.
- access or retain information stored as part of your account.
- install or uninstall third party apps or other integrations

In some cases, administrators can also:

- modify account settings, including the email address associated with your account; change the email address associated with your account
- change your information, including profile information
- restrict your ability to edit, restrict, modify or delete information

Please contact your organization or refer to your administrator's organizational policies for more information.

If you use an email address provided by an organization (for example, a work email address) to register for or access the services, **the owner of the domain associated with that email address may later assert administrative control over your account.** If this occurs, we will notify you where reasonably practicable.

If you do not want an organization to have administrative control over your account, you should register using a personal email address instead of an organizational email address.

If an administrator has not yet asserted control over your account, you may be able to change the email address associated with your account through your account settings. **Once administrative control has been established, changes to the account email address may require administrator approval.**

For more information about how your organization manages your data, please contact your administrator or review your organization's internal policies.

POLICY TOWARDS MINORS OR CHILDREN

We do not knowingly collect or solicit personal information from anyone under the age of 18 or knowingly allow such persons to register for the services. It has also been provided in our terms and conditions for using our website.

In case we become aware that we have inadvertently collected Personal information from a child under 18 without appropriate authorization, we will take reasonable steps to delete such information as soon as practicable, many of our services are provided to organizations (such as businesses, educational institutions, or other entities) that administer the services on behalf of their users. **In such cases, the organization using the services is responsible for determining whether the Services are appropriate for individuals under the age of 18 and for ensuring compliance with applicable laws relating to the processing of children's Personal information.**

If you believe that a child under 18 has provided personal information to us without appropriate authorization, please contact us so that we can take appropriate action.

THIRD PARTY LINKS

Our site and services may contain links to third party websites. For example, occasionally, at our discretion, we may include or offer third party products or services on our site. These third parties have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of those linked sites, including their information practices and data deletion procedures.

TRANSACTIONAL EMAILS

We may send you emails relating to Your use of our services. These communications may include **service-related communications (transactional emails)** as well as **marketing or promotional communications.**

a. Marketing Communications

We may occasionally send You marketing or promotional emails about product updates, new features, events, or other information about our products and services. You may **opt-out of receiving marketing communications at any time** by using the unsubscribe link provided in the email or by contacting us

b. Service and Transactional Communications

We may send certain **service-related or transactional emails that are necessary to provide the services or fulfil our contractual and legal obligations.** These communications are considered essential and you may **not be able to opt-out of receiving them** while you maintain an active account with us.

Examples of such communications include:

- Updates to our Privacy Notice. (*You need to know about the changes and may be required to give consent if such changes are made in future that impacts Your ability to use the service*)
- Updates in Terms of Service. (*Changes in Terms of Service may impact Your usage of services*)
- Payment confirmations, invoices or failure notification. (*You have the right to receive the invoice or confirmation of your payment*), in case of failure our Support team may get in touch with You.
- Subscription expiry and other service-related concerns. (*These two types of emails are necessary for you to effectively use the service*)
- **Customer support communications**, including responses to support requests or service-related inquiries.
- Notification of a data-breach. (*We're required by law to inform you about this in case such an event happens in future*)
- Account Notification emails. (Changes in Password, renewal reminders etc.)

SOCIAL MEDIA WIDGETS

Our websites include social media features, such as the Facebook Like button, and widgets, such as X "tweet" buttons. These features may collect Your (IP) address, which page you are visiting on the websites, and may set a cookie to enable the feature to function properly. Social media features and widgets are hosted by a third party and your interactions with these features are governed by the privacy statement of the companies that provide them.

PUSH NOTIFICATIONS

We will push notifications through a push notification provider such as Apple Push Notification Service, Google Cloud Messaging or Windows Push Notification Services if you have enabled notification on your desktop and mobile applications. These notifications may include service updates, security alerts, or other product-related information. You can manage or disable push notifications at any time through your **application or device settings**.

OUR ONGOING EFFORTS TO BE TRANSPARENT

We continue to make available necessary information to help our users better understand 42Gears processing of personal information and how to exercise choices regarding the use of your personal information through various channels including this Privacy Notice and any other relevant information that may be made available timely on our website or Trust Center, or within our Services.

We may also provide **additional just-in-time notices or explanations** when new features or data processing activities are introduced.

FURTHER INFORMATION

This Privacy Notice applies to all the products/services offered by Us unless otherwise specified. Each of our third-party service providers/integrations available to you via our Product(s) have their own privacy policies. You acknowledge that your visit to any third-party service providers/integrations website will solely be at your own discretion and risk. We do not claim knowledge of or ownership of any content in any third-party websites nor do we endorse any third-party website.

UPDATES TO THIS NOTICE

We may update this Privacy Notice from time to time to reflect:

- Changes in Our products or services
- new security practices
- updates required to comply with applicable laws and regulations

When we make material changes to this Privacy Notice, we will update the **"Last Updated" date** and may provide additional notice where

required, such as through email notifications or notices within Our Services.

Your continued use of this website and Our Services after the updated Privacy Notice becomes effective will constitute Your acceptance to this Privacy Notice and any amendments thereto. Changes to this Privacy Notice are effective when they are posted on this Page or by sending You an email or both.

If you do not agree with any changes to this Privacy Notice, you should stop using the services forthwith.

GDPR STATEMENT

The European Union (EU) General Data Protection Regulation (GDPR), enforceable as of May 25, 2018, imposes additional requirements upon companies to enhance the protection of Personal information of EU residents. 42Gears Mobility Systems has a dedicated, core-functional team overseeing 42Gears' GDPR readiness. We discuss our efforts and commitment to GDPR below.

42GEARS' COMMITMENT TO GENERAL DATA PROTECTION REGULATION

GDPR regulates the governance of personal information for European Union citizens with a prominence on data security and data privacy. The GDPR not only applies to companies that operate in the European Union (EU) but also impacts companies operating outside of the EU, if they process any personal information of any of its customers in the EU.

42Gears has established its information security and data privacy principles to protect the privacy and information rights of its customers. We are strenuously committed to GDPR compliance.

LEGITIMATE INTEREST FOR COLLECTION AND PROCESSING

The legal bases described below apply in accordance with the Data Protection laws relevant to the jurisdiction in which the data is processed. Depending on the circumstances, our processing may be based on consent, performance of a contract, compliance with legal obligations, legitimate interests, or other lawful grounds recognized under applicable laws, including the Digital Personal information Protection Act, 2023 (India), and other applicable Data Protection regulations.

Data collected from website users

For Customers in the European Union, our processing (i.e. use) of your personal information is justified on the following legal basis:

- the processing is necessary to perform a contract with you or take steps to enter into a contract at your request; this is the primary basis of our processing.
- the processing is in our legitimate interests, subject to your interests and fundamental rights, and notably our legitimate interest in using applicable data to conduct and develop our business activities; or
- You have clearly consented to the processing of your personal information for a specific purpose.
- We need to use and disclose Personal Data in certain ways to comply with our legal obligations.
- To protect the vital interests of the individual or others: For example, we may collect or share Personal information to help resolve an urgent safety situation.

Data collected through the use of our products and services

For Customers in the European Union, our processing (use) of your personal information is justified on the following legal basis:

- the processing is necessary to perform a contract with you or take steps to enter into a contract at your request; This is the primary basis of our processing.

To be able to process the data, we may rely on different legal bases including your consent, contractual necessity, comply with the legal obligations, necessity to respond to your requests etc.

USE OF PERSONAL INFORMATION

What follows is an overview of the purposes for which we use the personal information We collect.

Data Collected from Website users

- conduct and develop our business with you and with others.
- engage and update you about events, promotions, the websites and our products and services including software updates.
- provide you with documentation or communications which you have requested.

- correspond with users to resolve their queries or complaints.
- provide you with any services you request.
- send you marketing communications, where you have subscribed and consent to receive such marketing communications or where it is lawful for us to do so;

Data collected through the use of our products and services

- conduct and develop our business with you and with others.
- process, evaluate and complete certain transactions involving our products and services.
- maintain our internal business and accounting records.
- provide you with any services you request.
- manage, protect against and investigate fraud, spam filtering, risk exposure, suspected illegal activity, claims and other liabilities, including but not limited to violation of our contract terms or laws or regulations.
- To provide customer support: We use your information to resolve technical issues you encounter, to respond to yur requests for assistance, to analyze crash information, and to repair and improve the services, including for development, training, or fine-tuning of machine learning and artificial intelligence models.

  This may include **analyzing system logs, error reports, and usage data to diagnose issues and enhance product functionality.**

We may also use generative artificial intelligence technologies or automation tools in responding to your support related requests.
We do not use customer content from customer accounts to train or improve generative artificial intelligence models. However, we may use aggregated or de-identified information to improve our products, services, and support capabilities.
Where You give Us express permission to do so, we may disclose information to a third-party expert for the purpose of responding to support related requests. Other data may be processed where necessary to provide the services, comply with legal obligations, or protect our legitimate business interests.

RETENTION OF PERSONAL DATA

We retain your personal information for as long as required to fulfil the purposes for which it was collected.

We keep your information for no longer than necessary for the purposes for which it is processed. The length of time for which we retain information depends on the purposes for which we collected and use it and/or as required to comply with applicable laws. Requests for deletion or withdrawal of consent will be honored unless legal or contractual obligations require longer retention. To dispose of personal information, we may anonymize it, delete it or take other appropriate steps. Data may persist in copies made for backup and business continuity purposes for additional time.

We store personal information using secure storage practices and appropriate safeguards consistent with industry standards to ensure its integrity, confidentiality and availability. All data is hosted and processed through trusted cloud infrastructure and authorized third party providers under strict contractual and security obligations. These measures are designed to prevent unauthorized access, loss, misuse, or disclosure of personal information.

A summary of our approach to retention is outlined below:

Data Category	**Retention Period**
Website User Data	Retained for the duration of the relationship with the customer. You may request cessation of communication at any time.
Product/Service data - on unsubscribing, non-renewal, or termination of active license	Retained for 6 months on the live system, followed by a further 3 months in secured backup (AWS, MongoDB, Atlas, GCP), after which it is permanently deleted.
Product/Service data - on user-initiated deletion requests of active license (trial and paid licenses)	Deleted within 1 month of receiving the request, unless Applicable Law requires retention of some or all data for a further period. Data is then retained for 3 months in secured encrypted backup before permanent deletion.
Billing and commercial arrangement data	Retained for as long as necessary to fulfil statutory record-keeping obligations.
Data retained for legal, regulatory, tax, or accounting purposes	Retained for as long as required by Applicable Law, legal process, or regulatory obligation, including for the purposes of establishing, exercising, or defending legal claims and

	handling complaints or disputes.
Marketing opt-out / suppression list data	Retained from the date of opt-out for as long as necessary to honor and record the opt-out preference. This data is not used for any other purpose. Fresh, unambiguous opt-in consent is required before any resumption of marketing communications.
Temporary data (specific activity, promotion, or campaign)	Not retained beyond the duration of the specific activity or campaign for which it was collected.
All other Personal information	Retained only for as long as necessary to fulfil the purpose for which it was collected, in accordance with the applicable laws and our Retention Policy. Where deletion is not immediately possible (e.g. backup archives), data is securely stored and isolated from further processing until deletion can be carried out.

We continue to evolve our controls, schedules and practices for information and records retention and destruction which apply to your personal information. The above examples may vary in some cases due to local laws, liability periods and mandatory retention requirements. For example, if certain information needs to be retained for longer according to local laws, regulations or because different legal limitation periods apply, then we will keep the personal information for these longer periods.

DATA CENTERS

42Gears applications and data are hosted on Google Cloud Platform (GCP) and AWS (as opted by the customer)

For SureMDM users data may be stored in the following regions:

- North- America
- Europe
- Asia-Pacific
- Middle-East

Data is hosted in the data center region selected by the customer during the account registration or service provisioning process. The applicable hosting region is selected based on the customer's selection and is maintained subject to service availability and operational requirements.

INTERNATIONAL TRANSFERS

We will take reasonable steps to ensure the security of your personal information in accordance with applicable Data Protection laws. We are committed to ensuring that any such international transfer is conducted in full compliance with applicable privacy laws, including the EU and UK General Data Protection Regulations (GDPR), the Digital Personal information Protection Act, 2023 (India), California Consumer Protection Act (CCPA) Lei Geral de Proteção de Dados (LGPD), The Personal information Protection and Electronic Documents Act (PIPEDA) and Personal information Protection Act (PDPA) Where necessary, We implement specific legal, technical, and organizational safeguards to ensure that your personal information remains protected regardless of where it is processed.

We will comply with our legal and regulatory obligations in relation to your personal information, including having a lawful basis for transferring Personal information and putting appropriate safeguards in place to ensure an adequate level of protection for the Personal information when making any transfers of personal information from the EEA, Switzerland and the UK to countries which do not have the same Data Protection laws as the EEA, Switzerland and the UK.

When transferring your personal information outside the EEA, Switzerland and the UK, we will, where required by Applicable Law, implement at least one of the safeguards set out below:

Model Clauses: Where we use certain service providers we use Standard Contractual Clauses (SCCs) approved by the UK authorities and/or European Commission which give Personal information the same protection it has in the UK and the EEA. For further details, see https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. Further details can be found at: https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/ and https://aws.amazon.com/compliance/gdpr-center/

However, where you are using SureMDM Software-as-a-Service solutions provided by 42Gears, you can select whether processing of

device-specific information takes place in the **European Union or the United States** when you first register for such service. **Your selection of a hosting region during service registration determines where certain data will be processed or stored.**

We take appropriate contractual or other measures to protect the personal information in accordance with the applicable laws pertaining to Data Protection and ensure that no transfer of your personal information will take place to an organization or a country unless there are adequate controls in place including security of your data and other personal information.

In certain conditions, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements but the same shall be subject to the strictest confidential terms agreed.

Data Processing Addendum: To enable you to be compliant with the data protection obligations under the GDPR, we have an updated Data Processing Addendum which includes Standard Contractual Clauses (SCCs) which you agree and sign at the time of logging in our product(s).

Transfers in Compliance with DPDPA 2023

Where Personal information is subject to Indian Data Protection laws, including the Digital Personal information Protection Act, 2023, we ensure that any cross-border transfer of such data is conducted in accordance with applicable legal requirements and government notifications, and that appropriate safeguards are implemented to protect the data during transfer.

TIME LIMIT TO RESPOND

We try to respond to all legitimate requests within one month. Occasionally it takes us longer than a month if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

If you have any questions in respect to this Privacy Notice, or would like to exercise your right please write to Us at privacyinfo@42gears.com.

OTHER DATA PROTECTION LAWS

We operate across multiple jurisdictions and are committed to protecting personal information in accordance with applicable Data Protection and privacy laws wherever you are located. Our privacy practices are designed to meet the requirements of key frameworks including, among others, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), the Lei Geral de Proteção de Dados (LGPD), the Personal Data Protection and Electronic Documents Act (PIPEDA), the Personal information Protection Act (PDPA), and the Digital Personal Data Protection Act (DPDP Act). Where the laws of your jurisdiction grant rights or impose obligations beyond those described in this Notice, we honor those requirements in full.

YOUR PRIVACY RIGHTS

Where applicable under the laws of your jurisdiction, you may have the right to:

- Access your personal information and request information about how it has been used or disclosed;
- Correct personal information that is inaccurate, incomplete, or outdated;
- Delete personal information We hold about you, subject to applicable legal exceptions;
- Port your personal information in a structured, commonly used, machine-readable format;
- Withdraw consent to processing at any time where processing is based on consent, without affecting the lawfulness of processing carried out prior to withdrawal.
- Object to or restrict certain processing activities.

Not all rights listed above apply in every jurisdiction. The rights available to you are determined by the laws applicable in your country or state of residence. To exercise any applicable right, please contact our Privacy Team at privacyinfo@42gears.com. We may need to verify your identity before processing your request and will respond within the timeframe prescribed by Applicable Law.

ADDITIONAL RIGHTS APPLICABLE IN CERTAIN JURISDICTIONS:

- **California (CCPA/CPRA)**

  California residents have the right to opt-out of the sale or sharing of personal information for cross-context behavioral advertising, and to limit the use and disclosure of sensitive Personal information to purposes permitted under Applicable Law. We will not discriminate against you for exercising your rights under the CCPA/CPRA.

- **India (DPDP Act)**

  Residents of India have the right to access information about their personal information and how it is being processed, to request correction or

erasure of inaccurate or unnecessary personal information, and to withdraw consent at any time, subject to applicable legal obligations. They also have the right to grievance redressal through designated mechanisms provided by the Data Fiduciary, to nominate another individual to exercise their rights in case of death or incapacity, and to file a complaint with the Data Protection Board of India if their concerns are not adequately addressed.

- **Brazil (LGPD)**

  Brazil residents have the right to request anonymization, blocking, or deletion of Personal information that is unnecessary, excessive, or processed in non-compliance with the LGPD; to obtain information about public and private entities with whom their personal information has been shared; and to be informed of the consequences of withholding or withdrawing consent.

- **Canada (PIPEDA)**

  Canadian residents have the right to withdraw consent to the collection, use, or disclosure of personal information at any time, subject to legal or contractual restrictions and reasonable notice. Concerns regarding Our compliance with PIPEDA may be directed to Us at privacyinfo@42gears.com

- **Thailand (PDPA)**

  Thailand residents have the right to object to processing activities, including direct marketing, and to request suspension of the processing of their Personal information in certain circumstances.

DATA USE AND ACCESS ACT 2025

The Data Use and Access Act 2025 (DUAA) is a UK law that reforms Data Protection and digital services legislation. It amends the UK GDPR and Data Protection Act 2018 to simplify compliance, support innovation, and strengthen protection. Key changes include streamlined DSARs, broader use of automated decision-making, a new lawful basis for processing under "recognized legitimate interests" and the replacement of the ICO with a new Information Commission.

To support your rights under the UK GDPR and the Data Use and Access Act 2025, we've introduced a dedicated Data Protection Complaint Form. This ensures transparency, fairness in automated decisions, and stronger protection.

You may submit Your complaint using the following link: **Data Protection Compliant Form**

SUB-PROCESSORS

We engage third parties termed as "Sub-processors" to support the services we deliver to you. These third parties assist us in providing information, products or services to you, in conducting and managing our business, or in managing and improving our Products/Services or our websites.

We share your personal information with these third parties to render services for which they have been engaged by us to perform on our behalf, subject to appropriate contractual obligations and security measures, or if we believe it is reasonably necessary to prevent harm or loss, or we believe that the disclosure will further an investigation of suspected or actual unlawful activities or if required to do so by law or in response to a valid request by public authorities (e.g. a court or a government agency)

In addition, we reserve the right to transfer your personal information we hold about you to the relevant third parties in the event of actual or potential sale or transfer for all or portion of our business or assets including the event of merger, acquisition, joint venture, reorganization, dissolution, liquidation or other similar business-related transaction.

The third parties may include:

- Cloud infrastructure providers such as Amazon Web Services (AWS).
- Cloud application and productivity providers to support Our internal office operations such as email and document management.
- Administration and support: to enable customer support and assist in sales management.
- With auditors, lawyers, accountants and other professional advisers who advise and assist Us in relation to the lawful and effective management of Our organization and in relation to any disputes.
- When you connect your Gmail mailbox with your SureMDM Account (see section (Google API Disclosure) below).
- Marketing and Newsletter: To manage Our email communication with our customers for marketing purposes such as newsletters etc.
- Payment Gateways: We work with commercial payment gateways such as PayPal, Stripe, Chargify and BlueSnap. Customers can select the payment gateways, upon selection you will be redirected to systems controlled by these service providers to complete the payment transaction. The payment gateways render the payment services as an independent Data Controller and comply with all the obligations for processing the data under the applicable Data Protection laws and their respective Privacy Notice. We do not store or collect your payment card details in any manner whatsoever.

That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Notice. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI- DSS requirements help ensure the secure handling of payment information.

The payment processors we work with are:

- Stripe: Their Privacy Notice can be viewed at https://stripe.com/us/privacy
- PayPal: https://www.paypal.com/en/webapps/mpp/ua/privacy-full

We do not sell, rent, or trade any of Your Personal information to third parties. These third parties don't have any independent right to use, share or sell any of Your Personal information.

For the further details please refer Our sub-processor's list here: https://www.42gears.com/trust-center/legal/list-of-sub-processors/

GOOGLE API DISCLOSURE

We offer a feature that allows you to connect your Gmail account to your 42Gears account using secure OAuth authorization provided by Google.

When you choose to enable this integration, we may access limited information from your Google account, such as your email address and email content, **strictly for the purpose of**:

- retrieving emails to create support tickets within our platform; and
- enabling you to view, respond to, manage, or delete such emails directly from within our product.

We do **not access or process your Gmail data beyond what is necessary** to provide this functionality, and such access is performed only with your authorization.

You may disconnect your Gmail account at any time through your account settings or your Google account permissions.

42Gears' use and transfer of information received from Google APIs will comply with the Google API Services User Data Policy, including the **Limited Use requirements**, which restrict the use of such data to providing or improving user-facing features.

YOUR RIGHTS

For Customers in the European Union, your rights under the GDPR are outlined below. For customers outside the European Union, you may have some or all of the following rights available to you in respect of your personal information, depending on the reason for processing this data:

a. Right To Be Informed

You have the right to obtain a copy of your personal information together with information about how and on what basis that personal information is processed.

We do not sell your data to any third party. You can request for a copy of your PII processed with us through the DSAR FORM. The said information provided to you after placing this request through the DSAR Form serves as evidence of how we process your PII data and the legal purposes for which your PII data is processed by us.

c. ***Right of Access***

You have the right to access your personal information and supplementary information that we hold about you at minimal or no cost in accordance to the applicable laws and guidelines issued in this regard. In certain circumstances, and depending on applicable laws, we may not be able to provide access to the personal information that we hold about you if:

- access may adversely affect the rights and freedoms of others.
- would likely reveal Personal information about a third party;
- would reveal 42Gears or third party confidential information;
- could reasonably be expected to threaten the life or security of another individual; or
- includes information that was processed in relation to the investigation of a breach of an agreement or a contravention of a law.

In order to safeguard your personal information from unauthorized access, we may ask that you provide sufficient information to identify Yourself prior to providing access to your Personal information.

Depending on the circumstances and subject to applicable laws, we may deny processing your request if:

- We are unable to verify and authenticate your identity;
- it is unreasonably repetitive or automated; or
- it would be overly broad, ill-defined, or require disproportionate effort which renders the request manifestly excessive.

You have the right to request for restriction on processing of your data by Us through the DSAR Form. In any event, we may need to process your data for purposes of storage in accordance with our internal Retention policy and/or in compliance with Applicable Law or court orders, we may reject your request for restriction of processing of Your data.

d. Right of Rectification

You have the right to update or rectify inaccurate personal information (including the right to have incomplete personal information completed) that we hold about you.

We have a full right to consider the request in the context in which it is made and can deny if found manifestly unfounded or excessive.

e. Right to Erasure

You have the right to request that we delete the personal information we hold about you. Upon your written request and to the extent authorized by the Applicable Law, we will erase your personal information using the reasonable technical measures (except on the grounds mentioned in this Privacy Notice or unless a lawful basis exist to retain it) when:

- You withdraw your consent to processing unless some other lawful basis exists for us to continue to process your personal information;
- It is no longer necessary to process your personal information
- You object to the processing and no overriding legitimate grounds exist for us to process your personal information;
- The personal information has not been lawfully processed by us; or
- You have a legal obligation imposed under applicable data privacy law to which we might be subject to.

f. Right to Data Portability

You have the right to transfer your data in machine-readable format to a third party when we justify our processing on the basis of your consent or the performance of a contract with you.

g. Right to Object

You have the right to object, on grounds relating to your particular situation, at any time to any processing of your personal information by us. You also have the right to object at any time to any processing of your personal information for direct marketing purposes, including profiling for marketing purposes.

In case of Indian users, you may also designate another individual to manage your account or exercise your rights on your behalf (Right to nominate) in the event of your incapacity or death. We acknowledge such requests promptly and respond within a reasonable timeframe according to applicable Data Protection laws.

If you have any grievance relating to the processing of your personal information, you may submit a complaint to our grievance redressal officer using the contact details below. We will endeavor to address and resolve such grievances within the timelines prescribed under the Digital Personal Information Protection Act, 2023. Where a grievance remains unresolved, you have the right to escalate the matter to the Data Protection Board of India in accordance with Applicable Law.

Grievance officer:

Name: Ms. Shruti Sharma

Email: shruti.sharma@42gears.com

Address: (of the registered office)

h. Right to Lodge a Complaint to Your Local Data Protection Authority

You may have the right to lodge a complaint with your National Data Protection Authority or Equal Regulatory Body.

In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which overrides your rights and freedom.

i. Rights where 42Gears acts as a Data Processor

We provide many services that are used by our customers to collect or direct us to collect personal information about you. If that is the case, we are processing such information only on behalf of our customers and if you seek to exercise your rights should first direct your query to our customers (the “Controller”)

You have the right to terminate the contract if an objection raised by you in relation to your rights, as outlined herein or submitted through the DSAR Form, is not resolved to your satisfaction within a reasonable timeframe. However, we reserve the right to reject the objection(s) raised by you if such request is in violation of Applicable Law, court orders etc.

EU Representative:

We value your privacy and your rights as a data subject and have therefore appointed Prighter Group with its local partners as our privacy representative and your point of contact for the following regions:

- European Union (EU)
- Turkey

If you want to contact us via our representative, please visit the Prighter website.

If you have any questions or concerns about this Privacy Notice, please feel free to email us at privacyinfo@42gears.com.

AUTOMATED DECISION-MAKING

Automated decision-making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- a Data Subject has Explicitly Consented;
- the processing is authorized by law; or
- the processing is necessary for the performance of or entering into a contract

At present we do not use automatic decision-making or AI to make decisions that produce legal effects or similarly significantly affect individuals without human intervention.

USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS

We may use AI tools in limited contexts such as data analysis, or service enhancement to improve efficiency and decision support. These tools are designed to assist human decision-making, not replace it. Where AI involves the processing of Personal information, we ensure it is done transparently and in compliance with our obligations under the applicable privacy laws. ***However,*** we do not use customer Data to train our models by default. To improve system accuracy and responsiveness, our AI models may learn from anonymized operational patterns and system usage data.

CONTACT DETAILS

- We recognize that you may have questions on how we process your data, or you may want to change either the data we hold or how we communicate with you in the future.
- You may unsubscribe from receiving marketing or commercial communications about 42Gears or 42Gears products and services by clicking the unsubscribe link at the end of the marketing or commercial communication from 42Gears or by writing Us at privacyinfo@42gears.com apprising us what particular types of marketing or commercial communications you no longer wish to receive.
- If you have any questions or concerns about this Privacy Notice, please feel free to email Us at legal@42gears.com
- 42Gears has appointed Mr. Murgananda A, as its ISMS manager and he can be reached at murgananda.a@42gears.com