42GEARS PRIVACY POLICY

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 policy 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 (called "Personal Data/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 Policy. This Privacy Policy 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 Data 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the Data Protection Act, 2018 (UK) as well as the Laws of India (together “Applicable Law”), as amended, replaced or superseded.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 Data.

By using our Services and this website, You acknowledge that You have read and understood the contents of our e with this Privacy Notice.

This Privacy Policy doesn't apply where we handle Personal Data as a data processor (or a similar role like a "service provider" under CCPA) on behalf of our business customers or otherwise. When we process Personal Data for business customers, it is governed by the data processing agreement between us and the customer and also the privacy statement of the relevant customer will apply.

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.

WHAT IS PERSONAL INFORMATION?

With regards to this Privacy Policy, "Personal Information", for the purpose of better understanding, shall include but not be limited to:

- "Personal Data" 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 about Your use of the Services purchased and sign up by You;
- Any data/ information uploaded, posted, exhibited, displayed, linked, saved, shared, communicated, updated, downloaded or transmitted by you through the Services, including your search queries and commands;
- when you visit any of our Website(s) and the information captured or uploaded and posted by you voluntarily either through our website forms or otherwise.

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)

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.

In general, the Personal Data 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 data.

b. 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 Internet Protocol (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. Hence, we do not use this information to identify You, and do not process this information actively. The collection is a by-product of using the website. We include these in our log files to understand more about visitors to our websites.

Further, we gather information on how your device interacts with our website, products, or Services. This includes details such as which pages or features you access, links clicked, time spent on specific pages, mouse movements, interaction timestamps, error logs, referring and exit pages, and URLs. Understanding these interactions helps us gain insights into our User's behaviors, origins, and interests. We utilize this data for internal analytics to enhance the quality, relevance, and security of our offerings.
We may also use this information to block IP addresses where there is a breach of the terms and conditions for 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. Based on your consent, we may send you electronic communications to keep you informed of changes to our products and services.

Your personal data will be accessed by our authorized personnel to deliver the requested information and market to you in compliance with this Privacy Notice. **We may also provide your personal data to third-party service providers to help us deliver the information you requested, support event activities, or provide updates about our products and services.** Third-party service providers are not permitted to use Your information for any other purposes and are required to adhere to personal data protection laws.

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:

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, spend their time on, identify areas such as website navigation and user journey.

In addition to our own cookies, We use some third-party cookies to report usage statistics of the service, and so on. We also use a third-party application Crazy Egg for tracking and analyzing the activities of our website visitors. To find out Crazy Egg 's Privacy Practice and data security, please refer to the link here https://www.crazyegg.com/privacy. However, in case you wish to opt-out of the Crazy Egg's services click on the link provided: https://www.crazyegg.com/opt-out

- ***How to opt-out:*** To opt-out from the cookies, you can configure your browser through appropriate settings. However, you will not be able to opt-out from cookies which are "absolutely necessary" for our services.

Links to third-party cookie providers and their privacy/opt-out pages:

- Google Analytics: Google Analytics Cookie Policy
- LinkedIn: LinkedIn Cookie Policy and LinkedIn Ads
- Intercom: Intercom Cookie Policy
- Facebook: Facebook Cookie Policies

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 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

- ***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 into 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.

- ***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 for the location-based information while using our SureMDM Agent, we collect such location data for the 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, 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 their 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 their 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.

- ***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 and version code and application icon.

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.

- ***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, 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, 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 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.

- ***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 cellular plan.
Based on how the administrator has configured SureMDM Agent, the data may include:

1. The number of SMS sent or received; and
2. Contact name date and time

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 background or is not actively used.

- ***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 device storage, 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 in 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"**.

- ***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 on the basis of our legitimate interest.

SURELOCK

We provide our users the ability to control the types of information they collect about user's devices:
SureLock will allow us to capture 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 run-time permissions, the data may include but is not limited to:

a. SureLock will read only the "Phone Number" to allow/block the incoming and outgoing calls with Call log permission.
b. SureLock can read "Name of contact", "content of the SMS" in order to change the Android lock screen PIN with SMS permission.

The details are mentioned below:

- ***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.

- ***SMS Related Information:***

  With clear and explicit prior consent, the 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:

  1. The number of SMS sent or received; and
  2. Contact name date and time
  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 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.

- ***Contacts:***

  If You choose to enable the functionality of "Contacts", the 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 the 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 in 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 on the basis of 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

- ***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.

- ***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 wifi network.

- ***CamLock Permissions:***

  We use the 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 https://www.42gears.com/security-and-compliance/.

Note: For more information on product-related privacy, visit our Trust Center, where you'll find detailed privacy policies for each product, 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 information about your use of our products, services and mobile applications from application logs and in-house usage analytics tools and use it to understand how your business use and needs can improve our products. This information includes clicks, scrolls, features accessed, access time and frequency, errors generated, performance data, storage utilized, user settings and configurations, and devices used to access and their locations.

OTHER DATA

42Gears shall record, analyze and use your interactions with us, including email, telephone, chat conversations or any other electronic medium with our sales and customer support professionals, for improving our interactions with you and other customers.

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 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 any of our reselling partners, or otherwise express interest in any of our products or services to them, the reselling partner 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. 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 us 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.

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 in our legitimate interests, subject to Your interests and 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 data for a specific purpose.

SHARING OF THE DATA

We do not sell Your Personal Data under any circumstances or intend to disclose personal information about you unless stated here or at the point of collection. 42Gears may share personal data in the following circumstances:

- 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.
- Internally within 42Gears Organisation, including affiliates and subsidiaries, for the purposes outlined in this Privacy Policy.
- With our customers and partners to inform them about their users' utilization of our services, such as credential acquisition or course completion.
- With service providers contracted to perform services on our behalf, such as payment processing, tech support, CRM, marketing tools etc. These providers are bound by contract to protect the provided information and are restricted from using or disclosing it except as necessary to fulfil services or comply with legal obligations.
- With approved 42Gears Partners to offer and deliver our products and services to you.
- 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 Policy.

TRUSTED THIRD PARTY TOOLS WE USE

INTERCOM AND FRESHDESK

We also use "Intercom", a live chat platform that connects Users with our customer support team and during this process we collect some personal information such as name, email address and contact number with the express consent of the Users in order to start the conversation. The messages and data exchanged are stored within the Intercom application and Freshdesk. 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 are not making use of these messages or data other than to follow up on Users registered issues or inquiries. Your personal data 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 can 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 a responsibility with our Customers for the security of data.

We aim to safeguard and protect Your personal data 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 data, 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 data that is transferred from You or to You via the internet.

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 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:

- restrict, suspend or terminate your account access.
- 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.

Even if the Services are not currently administered to you by an organization, if you use an email address provided by an organization (*such as your work email address*) to access the Services, then the owner of the domain associated with your email address (e.g. *your employer*) may assert administrative control over your account and use of the Services at a later date. You will be notified by us on the happening of such an event.

- If you do not want an administrator to be able to assert control over your account or use of the Services, use your personal email address to register for or access the

Services. If an administrator has not already asserted control over your account or access to the Services, you can update the email address associated with your account through your account settings in your profile. Once an administrator asserts control over your account or use of the Services, you will no longer be able to change the email address associated with your account without administrator approval.

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

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 a child under 18 has provided us with Personal Information, we will take steps to delete such information forthwith. However, in case knowingly or unknowingly You collect or process any information related to children while using our products, You acknowledge and agree to be legally responsible for complying with the applicable laws and regulations related to protection of such personal information without any legal claims against us.

TRANSACTIONAL EMAILS

We may occasionally send you emails about product updates, changes in privacy policy, updates in terms of service, to offer customer support and marketing emails. You shall have the ability to unsubscribe or opt-out from some of these emails from the link provided at the below in the mail.
There may be some transactional emails which we might be necessary in order to provide effective service and to fulfil our contract (including not limited to):

- Updates in Privacy Policy. (*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 complete 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*)
- Notification of a data-breach. (*we're required by law to inform you about this in case such unfortunate 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 Internet protocol 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 in case where You have enabled notification on our desktop and mobile applications. You may turn off notifications in the application or device settings to manage Your push notification preferences or deactivate these notifications.

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 on Your devices.

FURTHER INFORMATION

This Privacy Notice applies to all the products/services offered by us. Each of our third-party service providers have their own privacy policies/notice. You acknowledge that Your visit to any third-party service provider 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

This Privacy Notice may be updated from time to time to bring in new security measures (if required) or to comply with applicable laws. You should review this page periodically to ensure that You accept and are compliant with the amended Privacy Notice. Your continued use of this website will constitute Your agreement 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.

If You do not agree with any changes to this Privacy Notice, You should stop using the Services forthwith.
To Exercise your data subject rights or privacy related rights, please fill the subject access request form.

Further, 42Gears has appointed IPTECH LEGAL CONSULTANCY LIMITED COMPANY as our turkey representative as per Turkish Data Protection Law. We have been officially published at VERBIS- Data Controller Registry Information System, refer the following link for your perusal:
https://verbis.kvkk.gov.tr/Query/Detailsq=RGDZ8czL0IwKmqW%2BU2XXfg%3D%3D&isNeviChange=duu6TOm7jzzm1f64DfpShw%3D%3D"
If You have any questions or concerns about this Privacy Notice, please feel free to email us at privacyinfo@42gears.com.

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 data 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 data 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 data 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

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 data for a specific purpose.

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.

Other data

- operate, evaluate, maintain, improve and develop our products and services or our websites (including by monitoring and analysing trends, access to, and use of the website for advertising and marketing);
- customize our websites, products or services to users' needs;

RETENTION OF PERSONAL DATA

We retain Your personal data for as long as required to fulfil the purposes for which it was collected. A summary of our approach to retention is outlined below:

Data Collected from website users

We retain this information for the duration of our relationship with the Customer. Once You have initiated and, where appropriate consented to our communication, You have the right to request us to stop communication (see the 'Rights' tab on this privacy page).

Data collected through the use of our products and services

At the outset of User to unsubscribe or non-renewal or termination of active license the data remains for 6 months on our live system and subsequently the data is retained for further 3 months in the secured AWS(Amazon Web Services) backup system which gets permanently deleted therefore. Apart from AWS we store data in MongoDB, Atlas and Google Cloud Platform(GCP)

In case the User initiates a request for the deletion of the active license, we delete all the data held within two weeks of obtaining the request until and unless to the extent required by any applicable law to retain some or all of the data for a further period. Further, We retain this data for 3 months in the secured and encrypted backup system which gets permanently deleted thereafter. Active license herein includes both the trial and paid licenses.

However, data relating to our commercial arrangement (billing information) will be held as long as necessary for us to fulfil our statutory record-keeping obligations.

OTHER DATA

We store other data for as long as needed to fulfil its purpose. We have a default retention period defined and take what we consider are reasonable measures to remove the data once this has expired.

In some circumstances, we may retain personal data for other periods of time, for instance where we are required to do so in accordance with legal, tax and accounting requirements, or if required to do so by a legal process, legal authority, or other governmental entity having authority to make the request, for so long as required.

In specific circumstances, we may also retain Your personal data for longer periods of time corresponding to a statute of limitation, so that we have an accurate record of Your dealings with us in the event of any complaints or challenges. However, the actual retention periods may vary significantly in context of different products and their underlying purpose.

When we have no on-going legitimate business need to process Your personal data, we will either securely destroy, erase or delete it, or if this is not possible (because Your personal data has been stored in backup archives), then we will securely store Your personal data and isolate it from any further processing until deletion is possible.

If any Personal Data is only required for a temporary period, such as for a specific activity, promotion, or marketing campaign, we will not retain it beyond the necessary duration. In instances where you opt out of receiving marketing communications, we will maintain certain Personal Data on a suppression list indefinitely. This ensures that we refrain from sending you further marketing communications in the future. However, we will not utilize this Personal Data for additional marketing purposes unless you choose to opt back in to receive such communications.

However, 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 Data for these longer periods.

Data Centres

Your data is stored in our secure AWS servers located in the following region:
USA,
UK, and
India

INTERNATIONAL TRANSFERS

We will take reasonable steps to ensure the security of your Personal Data in accordance with applicable data protection laws. We will comply with our legal and regulatory obligations in relation to your Personal Data, including having a lawful basis for transferring Personal Data and putting appropriate safeguards in place to ensure an adequate level of protection for the Personal Data when making any transfers of Personal Data 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 Data 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 may use specific contracts approved by the UK and/or European Authorities which give Personal Data 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 42Gears UEM SureMDM - Software as a Service solutions, You can select whether processing of device specific information takes place in the EU or in the United States when You first register for such service. Your consent to this Privacy Notice followed by Your submission of such information represents Your agreement to that transfer.
We will protect the personal information in accordance with this Privacy Notice. 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.

With respect to Personal Data received or transferred to the United States, 42Gears Mobility

Systems Inc. is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

In certain conditions. We may be required to disclose Personal Data 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.

With respect to Personal Data subject to LGPD's jurisdiction, We will also accomplish LGPD's requirements for transfers of Personal Data to countries which do not have the same data protection laws.

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 now includes Standard Contractual Clauses (SCCs) which You agree and sign at the time of logging in our SureMDM Product.

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 are a European Customer and You are unhappy with our response to a query or You have a further complaint, the Information Commissioner's Office can be contacted at https://ico.org.uk.

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

Our commitment to safeguard your data extends across borders, ensuring that your privacy rights are upheld regardless of your location. We prioritize your privacy no matter where you are in the world. Alongside the principles outlined in our privacy policy, we adhere to a spectrum of data protection laws including GDPR, LGPD, PIPEDA, DPDPA, PDPA, and more. We strive to maintain the utmost levels of data privacy and security by incorporating these regulations into our privacy protocols.
Some of these enactments are:

1. California Consumer Privacy Act (CCPA:

If You are a California resident, You are entitled to certain rights with respect to personal information that We collect about You. Learn more about these rights and how to exercise them in our California Privacy Notice.

2. Lei Geral de Proteção de Dados (LGPD:

LGPD is a new Brazilian data protection law that will come into effect on 15th August 2020 echoing the new principles similar to GDPR and CCPA provisions.
This new data privacy legislation having an extraterritorial scope will apply to all the global businesses dealing with personal data of Brazil citizens regardless where the organisations are located.
This new Brazilian law requires the organisations to be more responsible and accountable while collecting and processing all or any personal data of Brazilian citizens.
LGPD requirements are significant and we confidently meet these upcoming compliance standards having robust privacy and security protections embedded in our products and services offerings.

3. The Personal Information Protection and Electronic Documents Act (PIPEDA):

PIPEDA is a Canadian Federal Privacy law that regulates how private sector organizations handle personal information related to Canadian citizens when engaging “commercial activity”.
This law has expanded its scope to include the organisations which have a real and substantial connection with the citizens of Canada.
PIPEDA provisions allow individuals the right to know why their personal data is being collected, how it will be used, and to whom it will be disclosed and all the rights ranging from access to the deletion.
All our instituted policies and security measures mentioned in our Privacy Notice are in compliance with PIPEDA legislation.

4. Personal Data Protection Act (PDPA) Thailand:

The Personal Data Protection Act, B.E. 2562 (2019) ('PDPA') which is Thailand's first consolidated data protection law, was published in the Thai Government Gazette on 27 May 2019 and will take effect on 27 May 2020.

The legislation aims to guarantee protection for individuals and their personal data with imposing similar obligations on businesses when collecting, using, and disclosing personal data.

Further, once the data protection authority i.e. the Personal Data Protection Committee ('PDPC') is established, further sub-regulations and guidance on the PDPA will be issued and updated by us accordingly.

In addition, the PDPA mirrors the GDPR's extraterritorial applicability and applies to data controllers and data processors outside of Thailand if they process personal data of data subjects in Thailand and offer goods and services to, or monitor behavior of the data subjects.

In this regard, we ensure to provide Thailand residents with several privacy rights, including the right to erasure, the right to be informed, the right to object, the right to data portability, and the right to access etc as outlined in our Privacy Notice and other similar provisions in order to comply with this landmark legislation.

Protecting our customers' information and their users' privacy is extremely important to us.

We continually monitor compliance and controls to ensure ongoing data security as per the applicable laws in relation to the collection, use, disclosure, and protection of personal information.

For more details regarding what, why and how we collect and process your data, please refer to our **PRIVACY NOTICE**.

Please be assured that all the commitments and principles embodied in our Privacy Notice with respect to the transparency and the data subject legally ascribed rights applies to Brazil, Canada and Thailand citizens in its entirety.

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 data with these third parties to render services for which they have been engaged by us to perform on our behalf, subject to appropriate contractual restrictions 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 illegal 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 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 are transferred to systems controlled by these service providers to complete the payment. The payment gateways render the payment services as a 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 Policy. 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 Policy can be viewed at https://stripe.com/us/privacy
- PayPal: https://www.paypal.com/en/webapps/mpp/ua/privacy-full

We do not share, sell, rent, or trade any of Your personal information to third parties, other than as necessary to deliver the services we provide You or to administer our business. These third parties don't have any independent right to 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

42Gears has developed a functionality that allows its customers to connect their Gmail mailbox using Oauth with our products. Connecting your Gmail mailbox to your 42Gears account allows us to associate your account with your personal information on Google, to see your personal information, including any personal information you have made available, to view your email address and access your emails in order to create them as a ticket in our products. The connection will further allow you to respond to your emails directly from our product and to delete them once they are fetched into our product.

42Gears's use of information received from Google APIs will adhere to Google API Services User Data Policy's App's, including the Limited Use requirement.

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 data, depending on the reason for processing this data:

Right To Be Informed

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

Right of Access

You have the right to access Your personal data 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 data that we hold about you if:

- access may adversely affect the rights and freedoms of others.
- would likely reveal personal data 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 data from unauthorized access, we may ask that you provide sufficient information to identify yourself prior to providing access to your personal data.
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.

Right of Rectification

You have the right to update or rectify inaccurate personal data (including the right to have incomplete personal data 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.

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 data 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 data;
- It is no longer necessary to Process your personal data
- you object to the Processing and no overriding legitimate grounds exist for us to Process your personal data;
- the personal data 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.

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;

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 data by us. You also have the right to object at any time to any processing of Your personal data for direct marketing purposes, including profiling for marketing purposes.

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.

Automated Decision Making

We do not employ solely automated decision making, as a matter of course, that results in automated decisions being taken (including profiling) that legally affect You or similarly significantly affect You. Automated decisions mean that a decision concerning You is made automatically on the basis of a computer determination (using software algorithms), without

our human review. If You are to be subjected to automated decision making, We will make it clear at that time and You have the right to contest the decision, to express Your point of view, and to require a human review of the decision.

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 in the event that an objection request raised by you with respect to your Rights as elaborated here and through the DSAR form, that have not been resolved satisfactorily within a reasonable time period provided by us. 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 Osano as our privacy representative and your point of contact.

Osano International Compliance Service Limited
ATTN: 8T2B
25/28 North Wall Quay
Dublin 1, D01 H104
Ireland

To Exercise your data subject rights or privacy related rights, please fill the subject access request form.

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

Last Updated: 24-05-2024
Version: 4.0