Limble Terms FAQs[1]

We're so excited to start our partnership with your team and to welcome you to our community of maintenance heroes! Could you do us a big favor and share these FAQs with the team in charge of reviewing legal and privacy agreements at your company? Context is always important when reviewing agreements, and we find that oftentimes the teams reviewing our agreements are missing critical information around the services being purchased and how they are provided. In our experience, providing this context early in the process is crucial to ensuring the contract review is efficient and enjoyable for both parties. These FAQs will hopefully reduce the amount of time spent discussing boring legal documents and maximize your time as a maintenance pro. We encourage whoever is reviewing our agreements - specifically our Customer Terms of Service (TOS) and our Data Processing Addendum (DPA) - to read these quick FAQs as they will streamline their review. Thank you!

Who is Limble and what services does it provide?

Limble is a software-as-a-service (**SaaS**) vendor providing a modern computerized maintenance management system (**CMMS**) and asset management platform that helps maintenance teams streamline work orders, schedule preventive maintenance, track assets, and manage spare parts inventories. Limble serves maintenance professionals across diverse industries. Limble's mission is to empower maintenance teams to increase uptime, extend asset life, and transform maintenance from a reactive cost center into a strategic advantage through an intuitive, easy-to-use platform. Limble does not provide any hardware or sensors although it can integrate with them. You can learn more about our service-specific functionality in our Product Documentation.

If Limble is helping me manage the maintenance of my machines and assets, does it have access to any personal information from my customers or employees?

Limble does not process any personal information from your customers. Limble only processes certain personal information of the employees and other individuals with log-in access to the Limble platform. We refer to these folks in the TOS as "**Authorized Users.**" You have total control as to who those are. The type of personal information we process from Authorized Users to provide the services is generally limited to first and last name, work email address, work phone number, work location and username. For your admins of our platform, we'll also have access to the IP addresses they use to log-in, admin activity in the platform (e.g., last sign in), help desk tickets submitted, and responses to survey questions (e.g., a response to a question like "please rate your experience").

By the way, we don't process any sensitive information such as payment card information or protected health information so no need, for example, to enter into BAAs or add PCI DSS language :). We refer to that information as **Sensitive Personal Data** in our TOS and we specifically request our customers not to upload any of it to our platform.

Since Limble processes some personal information, how does Limble comply with CCPA and GDPR?

Privacy and security are very important to us! You can access our certifications, SOC 2 Type II report, list of subprocessors, and our security whitepaper in our Trust Center. To access some of the documentation you may need to sign a standard NDA.

Limble processes personal information in accordance with our Data Protection Addendum (DPA). Limble acts primarily as a processor with regard to the personal data in the platform and you are the controller. Please note that Limble acts as a limited controller specifically with regard to your company business contact information (e.g., employee contact information); please see Section 2.4 of our DPA for more information.

We have carefully drafted our **DPA incorporating the GDPR standard contractual clauses and the UK Addendum by reference (see sections 11.2 and 11.3)** to ensure that it includes all the necessary requirements and obligations under GDPR so we both can

[1] *Note that these FAQs are for explanatory purposes only and nothing contained in them forms part of or modifies the TOS or DPA*

comply with GDPR. We also included a section to address CCPA (as amended by the CPRA) in our DPA (see Section 3.1). Rest assured that Limble **does not sell** any **personal information** it receives from its customers through the platform. Please note that we're a multi-tenant SaaS provider and it would be almost technically impossible for Limble to accept a different DPA per customer as it would entail processing data in a slightly different way for each customer. We need to make sure we have standard and consistent security, privacy, and compliance controls among all our customers to ensure equal protection. As a result, and unfortunately, we cannot review your DPA template. Limble updates the DPA from time to time to reflect developments in privacy law and updates to the platform.

How does Limble use the data it collects from customers through its platform?

We use the data to provide services and to prevent or address technical or service problems. We may also use it in an **aggregated and de-identified manner** for things like product analytics and performance, product usage and utilization, setting benchmarks, new product features or services, marketing and related purposes. This data will never identify you or your customers or employees.

Does Limble use any subprocessors? How do I know my company can trust those third parties?

Yes. You can see them here. Our relationship with each of them is subject to our third-party security management program to ensure they meet our rigorous security and privacy standards. Each of them has entered into a DPA with us. If we ever add new subprocessors or replace them, we will notify you, and you will have an opportunity to object pursuant to section 6.3 of the DPA.

Will Limble provide our personal information if requested under a US surveillance law?

Please note that we have **never** been requested or subpoenaed to provide any customer data to any law enforcement, intelligence, security or regulatory agency from the US or elsewhere. If this were to happen, and to the extent permitted by law, we would notify you. If prohibited from notifying, we would use reasonable efforts to obtain a waiver of the prohibition.

Does Limble use AI features? If so, will it train AI models with my data?

We offer AI features. We ensure that all our AI Features are clearly designated as such. We also ensure that the AI models only use your data to provide the services and not to train the AI models. If you want more information, feel free to review our AI Risk and Compliance FAQ available at https://trust.limblecmms.com/**.**

Can my affiliates use the platform?

Yes, an affiliate may simply be included in the parent company's Order Form or an affiliate may choose to enter into a separate Order Form with us (see Section 1.3 of the TOS).

Are there any deliverables as part of the services? Do you provide customized services?

We don't provide any work-for-hire or custom services (e.g., customization of SaaS software) for any specific customer as all Limble customers are on the same instance and version of our multi-tenant services.

What are the limitations of liability in the Customer Terms of Service?

We offer a market standard limitation of liability in our TOS. The limitation of liability is mutual, allows both parties to disclaim any consequential and incidental damages, and caps the liability of both parties to an amount that is commensurate with the value of the customer's subscription. Note that in terms of indemnification, we will defend any third party IP infringement claims against a customer as a result of our products and services.

Can I add a termination for convenience right?

We can appreciate the spirit of the request. However, as a SaaS provider we cannot allow a termination for convenience as our pricing and packaging is based on a commitment for the entirety of your subscription term. We rely on these financial commitments

from our customers to constantly scale and improve our services and appropriately staff our award-winning customer support services.

Will Limble review my company's master services form agreement?

We use a multi-tenant cloud structure (i.e., all our customers are hosted together in the same instance in the cloud). Our services are provided to all of our customers through the web on the same operational infrastructure and using the same security and support operations. While there are various plans available, they are all delivered from a common infrastructure with varying levels of functionality and features. Due to this very specific nature of the way our SaaS services are provided, we need to use our TOS and accompanying documents which correctly reflect it. Furthermore, non-Limble TOSs are not accurately tailored to the Limble platform and inevitably require considerable cross-functional resources and customization to review, causing significant delays to the contracting and onboarding process. We regularly review our TOS and believe it is fair and balanced based on customer feedback and industry standard positions.

How does Limble protect the data submitted to the platform?

At Limble we take security very seriously and are constantly looking to not only improve the security of the platform, but also how we conduct business on a daily basis. Limble maintains a demonstrated commitment to security protections for all customers (including compliance with industry best practices and standards). Limble is hosted on AWS, giving us access to the benefits AWS provides such as physical security, redundancy, and scalability. Limble protects data submitted to the platform through layered technical controls designed to ensure confidentiality, integrity, and availability. All customer data is encrypted in transit using HTTPS/TLS and encrypted at rest within its databases. Customer environments are logically isolated to prevent cross-tenant access. Access to systems and data is restricted using least-privilege, role-based controls with formal approval processes, and credentials are stored in a salted SHA256 hashed format. Limble also employs continuous monitoring, secure code reviews, third-party penetration testing, real-time data replication, and encrypted backups stored in geographically separate locations to safeguard against unauthorized access, data loss, and service disruption.

We invite you to visit https://trust.limblecmms.com/ where you can view our security whitepaper and obtain additional security documentation, such as our latest SOC 2 Type II report.

If you have any questions about our agreements, please do not hesitate to reach out to legal@limble.com.