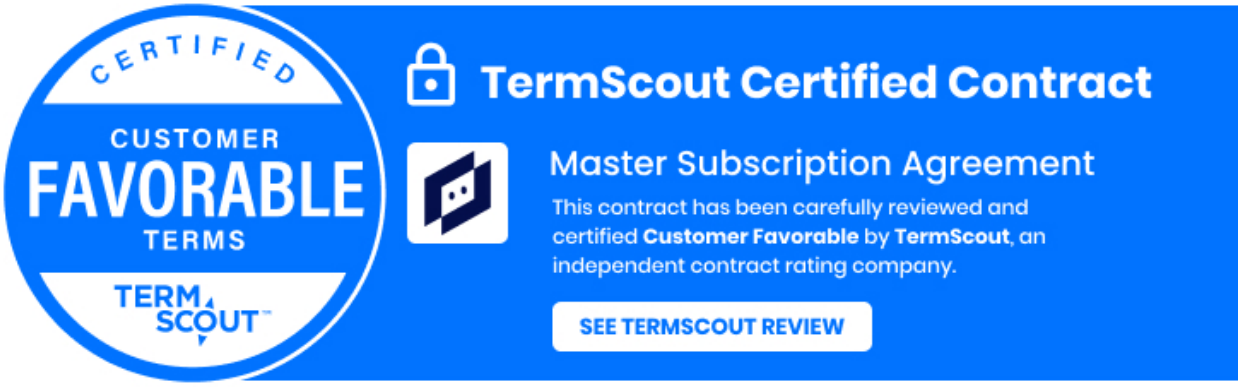
Subscription Agreement Guidelines

LogicMonitor, Inc ("LM", "we" or "us") is pleased that you are interested in subscribing to our cloud-based infrastructure monitoring platform (the "Service"). We are committed to getting you started with the Service as rapidly as possible.

LM provides the Service pursuant to the terms of our Master Subscription Agreement available at **https://www.logicmonitor.com/msa** or such other Terms of Service or End User License Agreement variation as may be set forth on your Order Form or agreed to by the parties (as applicable, the "Terms of Service or "TOS"). Your Order Form sets out the commercial terms (e.g., products and services ordered, volume, fees, subscription term length) and the TOS sets out the legal terms that apply to your subscription. As we begin the contract process, we wish to provide additional context to help you and your team better understand the Service and the TOS pursuant to which we deliver same. We hope that these Subscription Agreement Guidelines (these "Guidelines") will aid your review of the TOS.



LM has worked closely with TermScout, a neutral third-party, to make sure that our contract is not just good for us, but it's good for our customers too. In fact, our terms have been certified 70% customer-favorable, which means that we offer terms that are at market (or better) and that are among the most customer-friendly in the industry. You don't have to take our word for it - click the TermScout certification badge above to see the full Certified Contract Report.

Please note that these Guidelines do not form part of the customer contract and are provided for informational purposes only.

Frequently Asked Questions

1. What is my company purchasing?

The LogicMonitor Service is a fully automated, cloud-based technology infrastructure monitoring platform intended for enterprise IT customers and Managed Service Providers. Through this software-as-a-service ("SaaS") based Service, our customers gain full stack visibility into the health and performance of their networks, cloud, servers, and other technology systems with one unified view. Although LogicMonitor is a cloud-based service, our customers must install LM's data collection software (the "Collector Software") onto its network to benefit from comprehensive observability.

2. Can LM accommodate a customer's form of TOS or SaaS Agreement?

As a SaaS provider, LM provides this Service at scale to thousands of customers. Accordingly, as a practical matter, we need to keep our terms of service as standardized as possible and are not able to work off of individual customers' forms of SaaS Agreement. Our TOS has been carefully tailored to our particular Service and is updated on a regular basis to best meet the needs of our customer base.

Our engagement model seeks to get you up and running as expeditiously as possible. We have found that customer paper does not fit our particular Service and invariably requires extensive changes in order to use as a starting point, significantly increasing the complexity (and cost) of negotiations for both parties. For enterprise customers with annual contract value exceeding $50,000, LM's legal team is happy to review and consider reasonable edits to the TOS that the customer may propose via redline.

3. Why can't LM provide a termination for convenience right?

LM's Service is provided on a subscription term-based model, with a minimum subscription period of twelve (12) months. The specific pricing terms offered to the customer are in consideration for this minimum term commitment. We are thus not able to offer a termination for convenience option during the agreed upon subscription term, as that is contrary to LM's business model. In the event of a termination for cause, of course, LM will promptly refund any prepaid fees for the remainder of the then-current term.

4. Does LM process personal data of the customer in connection with the Service?

The focus of the Service is on health and performance metrics related to the customer's technology infrastructure. Accordingly, LM's Service is not meant to function as a conduit to transmit personal data or other sensitive data. There is a small volume of incidental personal data that is processed in connection with our Service (for example, user log-on credentials and names and contact information of employees of each party as needed to conduct the Services and business relationship). Such personal data is at all times treated as confidential information and

secured and maintained in full compliance with applicable privacy laws and regulations. LM does not process any sensitive personal data (as categorized under the EU's General Data Protection Regulation (GDPR)).

LogicMonitor's processing of your personal data is governed by LM's Data Processing Addendum set forth at **https://www.logicmonitor.com/legal/data-processing-addendum** (the "DPA"), which relies on the European Commission's Standard Contractual Clauses ("SCCs"). The DPA is referenced by hyperlink in and incorporated into the TOS. More generally, LM processes personal data for the purposes outlined in our privacy policy available at **https://www.logicmonitor.com/privacy/policy**.

5. Does LM offer a Service Level Agreement (SLA)?

Yes, LogicMonitor provides the Service in accordance with the minimum Service Level Terms set forth at **https://www.logicmonitor.com/SLA** (the "SLA"). The SLA is referred to in Section 8(b)(ii) of the TOS and incorporated therein.

Pursuant to the SLA, LM commits to maintain a Service availability level of at least 99.9% throughout the subscription term. In the event of an SLA failure, the customer is eligible to receive service credits and, in the event of repeated or severe breach of the SLA, a termination and refund right. While our internal target for platform uptime is 99.99% (which we regularly exceed), we can commit to providing service credits only if we fall below the 99.9% threshold set forth in the SLA. Since LM has the same operational targets across our entire customer base through our standardized SaaS platform, we are not able to negotiate the SLA terms with individual customers.

6. When is "Planned Maintenance" performed and what effect does this have on the customer's Service?

Planned maintenance windows generally occur late Thursday evening PST. LM strives to minimize downtime for planned maintenance, and historically this averages to approximately 5 minutes per month. Since planned maintenance procedures apply to all of our customers at the same time, please note that we are unable to negotiate these terms with individual customers. While planned maintenance is performed, the Service will continue to monitor the customer's IT network. All monitoring data is cached during the applicable planned maintenance window and immediately made available when the portal is back online, so there are no "gaps".

7. What are "On-Demand Fees"?

LM's business model is structured on a subscription price model based on the number of devices that the customer desires to monitor during the subscription term, as set forth on the customer's Order Form (the "Reserved Commitment"). During the subscription term, the customer pays a fixed subscription fee for the Reserved Commitment which cannot be reduced. Fee rates for the Reserved Commitment may be discounted based on volume commitment (number of devices) or subscription term length (e.g., discounted pricing for multi-year term commitment).

If the customer's actual usage exceeds the Reserved Commitment (as determined on the basis of average daily usage for a calendar month period), the amount of such excess usage will be billed to the customer via invoice at the end of the applicable month at the on-demand pricing rate set forth on the Order Form. In the event that, following any such month, the customer wishes to amend the Order Form to increase the Reserved Commitment moving forward, any on-demand premium for the prior monthly overage may be waived.

8. We are very concerned about liability exposure from any potential data breach. Why don't you offer unlimited liability for data breach?

This, of course, is a very reasonable concern in today's climate and data security is and will remain a top priority for LM. We offer a "special cap" for data breach that is set at a multiple of the associated contract revenue (i.e., the trailing twelve (12) months' Service fees). Ultimately, however, we must limit our potential exposure in proportion to the contract value and are not able to offer unlimited liability. This is the only way that we, as a SaaS vendor, can provide our Service at scale to thousands of customers and still offer competitive pricing. Moreover, such a limitation of liability for data breach is essentially "industry standard" for SaaS offerings.

While no vendor can eliminate all security risk, LM details the security measures we have in place to permit our customers to make an informed decision when electing to subscribe to LM's Service. It is worth noting that LM's Service involves the processing of only a very limited volume of incidental personal data. Further, please note that, since the Collector Software sits in the customer's IT environment, data security is necessarily a joint obligation of LM and the customer.

9. How does LM protect customer data from cyber threats?

LM was founded by experts in IT security, and we've operated a holistic information security program from the earliest days of our company. Our security practice applies to every facet of our business, from our business technology systems to our software design and development practices and into Service operations. In testament of our comprehensive approach, and to ensure the trust of our customers, our security practices are audited annually against the rigorous AICPA SOC2 and ISO 27000 series standards, and we commit to sharing our third-party auditors' reports upon request. Further, we arrange for third-party penetration testing of our applications on a regular cadence to ensure they remain free of security defects that could impact the confidentiality or integrity of our customers' data.

10. Can we include in the TOS the right to perform our own security audits?

Due to the multi-tenant nature of SaaS, and in order to maintain LM's confidentiality obligations to its customers and to third parties, we can't offer full audit rights or on-site access to our facilities, technology systems, and or the facilities and systems of our subprocessors. Upon a customer's written request, and not more than once per year, LM will respond to the customer's reasonable written requests for information relevant to its security and privacy program.

11. Can we attach our standard security exhibit or DPA to your TOS?

LM's security practices are operated in alignment with the highest industry standards, and we aim to be as transparent as possible about these practices. While we commit to making our third-party audit reports and other security program collateral available to customers upon request to ensure that you are comfortable with the level of protection provided for your data, we cannot attach non-LM security or privacy terms to our TOS, as these are not tailored to LM's Service. Our security measures are operated consistently across all of our customers, and we don't have the ability to support bespoke requirements at the behest of a single customer. Ultimately, LM can consider reasonable redlines to LM's security exhibit (Exhibit A to the TOS) or DPA, but non-LM versions of these documents do not accurately reflect the security measures and practices that we apply across the board and LM is unable to accommodate such requests.

12. Can we change the governing law and forum from California to our home state or country?

The default position in our TOS is that the laws of the State of California apply, with exclusive jurisdiction in the federal and state court in Santa Barbara County, California. Alternatively, LM is willing to change the governing law to the states of Texas, New York, or Delaware or to the laws of Australia or England and Wales. Since the TOS govern intellectual property ownership rights and limitations in LM's Service and technology, we require that the TOS be governed by a body of law that is well developed and with which LM has familiarity.

13. Can we specify a specific data center or region in which LM will agree to store our data? For example, can you commit to store our data in the EU only?

LM operates our SaaS platform out of our "Service Centers," the locations of which are set forth in our Data Handling Supplement available at **https://www.logicmonitor.com/data-handling-supplement**. We can commit that customer data will be primarily stored and processed within a customer's selected Service Center, with the caveat that we rely on a small number of subprocessors located exclusively in the US and Canada (e.g., chat support provider) that handle a limited amount of customer information on our behalf in their support functions.

14. How do we obtain our data upon termination or expiration?

For enterprise customers, LM retains customer data during the subscription term for the prior twenty-four (24) month period at any time; provided, that, customer data is automatically deleted ninety (90) days after termination. Prior to termination or expiration of its subscription, a customer may download whatever historical data it wishes by using the Service UI (to export data in graphical or CSV format) or alternately via LM's API. LM does not place any conditions or limitations (e.g., payment of any fees to LM) for the migration of such historical data. Please refer to our support documentation for further information on obtaining historical data from our API: **https://www.logicmonitor.com/support/rest-api-developersguide/v1/data/get-data**.

15. When a user logs into LM's Service portal, they must consent to LM's Master Subscription Agreement ("MSA") and Privacy Policy. How does this apply if I have a signed agreement with LM setting forth the terms of service?

The "click through" MSA that is referenced in the user log-in portal only applies where the customer does not have an signed license agreement with LogicMonitor setting forth the terms of service. Any signed agreement governing the customer's subscription (whether titled End User License Agreement, Terms of Service, or something similar) will supersede the click-through MSA in the user log-in portal in its entirety.

As a practical matter, the click-through MSA will generally only apply to (a) customers purchasing through a Reseller that have not otherwise entered into a EULA with LM and (b) customers using the product on a free trial basis. The MSA is available at **https://www.logicmonitor.com/msa**.

16. Managed Service Provider ("MSP") customers only: How do we flow down the TOS obligations to our end customers?

As part of our MSP business model, LM does not contract directly with the MSP's end customers. LM and the MSP are parties to the MSP TOS, and the MSP is responsible to LogicMonitor for the access and use of the Service and LM software by its customers and their compliance with the TOS. The MSP is free to contract with its customers using whatever forms(s) of agreement that it wishes; provided, that, the MSP should ensure that its customers are bound by certain minimum protections (e.g., with respect to confidentiality obligations, license restrictions, IP rights, disclaimers and limitations of liability) with respect to LM's service. LM does not "police" the form of agreement that an MSP enters into with its customer and will not be involved in that process. The MSP's standard contract with its customers (not specific to any one licensor) may be sufficient. Upon request, for convenience, LM can provide a form of EULA that may be used by an MSP with its LogicMonitor customers.

Addendum: Processing of Personal Data Under GDPR

17. What legal mechanism does LM rely upon to transfer personal data to the U.S. in compliance with E.U. data protection rules?

LM transfers personal data on the basis of the Standard Contractual Clauses ("SCC"s). LM's DPA incorporates the new SCCs released by the European Commission in June 2021. LM acts as a data processor on behalf of customers in the EU and, accordingly, our DPA relies on the Module 2 SCCs (for controller-to-processor transfers). For certain managed service providers ("MSPs") that are themselves processors on behalf of their customers, our DPA will also incorporate the Module 3 SCCs (for processor-to-processor transfers).

18. What personal data specifically is or may be processed by LM? For what purpose(s)?

As noted in Question 4, the focus of LM's Service is on performance metrics related to the customer's IT infrastructure, and any personal data processed by LM in connection with the Service is incidental. The Service is not intended to function as a conduit to transmit personal data and the volume of such incidental personal data processed by LM is relatively minimal.

Incidental personal data that may be processed by LM generally consists of certain personal data required in order for those designated employees, temporary workers and/or contractors assigned by the customer to use LM's Service (i.e., to log in to the Service portal). These personal data elements may include name, email address, mobile device number (optionally), and workstation IP address. None of the incidental personal data processed by LogicMonitor is sensitive personal data, as categorized under GDPR

The above described incidental personal data are used within the Service solely for purposes of account management, user support, audit logging and delivery of notifications to the customer (email/SMS). These limited use cases are enforced by application code. LM employs specific security controls with respect to personal data, including encryption at rest using AES-256 and encryption in transit using TLS 1.1 or higher with no weak ciphers.

19. Given the small volume of personal data processed by LM, do we need to enter into a DPA?

Yes. Notwithstanding the focus of LM's Service and the small volume of incidental personal data involved, in the event that any such personal data processed by LM on behalf of a customer relates to an individual in the E.U. or European Economic Area (EEA), there must be a valid legal mechanism in place under GDPR to transfer such personal data to the United States. This is not optional and is a requirement for both LM and the customer.

20. What subprocessors may have access to personal data?

Personal data transferred to the United States may be provided personal data to certain of the approved subprocessors listed in LM's Data Handling Supplement, available at

https://www.logicmonitor.com/data-handling-supplement. These subprocessors provide certain ancillary services that support LM's Service, including live support chat and SMS notification. All data provided to such subprocessors is stored in the United States. LM enters into a contract with each subprocessor that contains the same data protection obligations as those set out in the DPA between LM (as processor) and customer (as controller) and, of course, LM is fully liable for each such subprocesor's compliance with its data protection obligations. The procedures for appointing new subprocessors are set forth in Section 6 of the DPA.

21. Can I choose to have all of my customer data stored in the EU and opt out of any processing of personal data in the United States?

LM customers have the option to select the service center region in which their customer data is stored, and this includes the option to select an EU-only data center. Available service centers are listed in LM's Data Handling Supplement, available at **https://www.logicmonitor.com/data-handling-supplement**. Accordingly, a customer can select the option to have all of its monitoring/performance data stored in the EU.

However, even if customer data (including all monitoring/performance data) is stored in an EU data center, the incidental personal data of the type described in Question 17 above may be transferred to the United States for purposes of LM and its approved subprocessors providing support services (e.g., chat support, alert notifications). Additionally, operational logs and other files submitted for analysis by LM's support teams are stored in the United States.

22. Given the reasoning of the CJEU in "Schrems II", what additional due diligence has LogicMonitor undertaken to evaluate and document the risks associated with the transfer of personal data to the US (including intelligence gathering by public authorities)?

LM ensures that all customer data transmitted across public networks is encrypted, which helps to mitigate the risk that the U.S. government could successfully leverage an electronic communication service provider or remote computing service to surveil LogicMonitor's customers' data while in-transit and obtain LogicMonitor U.S. data, such as under Section 702 or pursuant to a national security letter.

With that said, LM has not identified any request for information from U.S. intelligence authorities relating to any LM data in the past, nor does LM process data that could reasonably be expected to be of interest to U.S. government intelligence authorities. A more detailed analysis of the "Schrems II" factors as they relate to LogicMonitor's Service is available at **www.logicmonitor.com/schrems**.