FAQ for Brightly Software's Master Subscription Agreement

This FAQ is designed to provide helpful explanation about our suite of Software-as-a-Service (SaaS) applications, products and services (the "Service") and the applicable Master Subscription Agreement ("MSA", which is drafted to accommodate the unique aspects and functionality of our Service). We hope this FAQ will provide context as you review the MSA. It is for informational purposes only and will not be part of the contract between the parties. Some of the terms in this FAQ are defined in the MSA.

Services- What am I buying?

Brightly Cloud Service: We provide our commercial-off-the-shelf Services to thousands of Subscribers by way of a cloud-based non-exclusive, non-transferable right to access the Service for the Term, as stated on your Order Form and as further described in the MSA. That means that the Service is provided to all of our Subscribers in the same manner –with the same architecture, codebase, infrastructure and security. Because of the off-the-shelf nature of the Service, we can't provide custom service offerings for you and are limited by operational scalability because we must be able to support all Subscribers in the same manner. We offer various geographic hosting locations in the USA, Canada, UK and Australia, depending on the Subscriber's location.

Professional Services: We may provide comparable Professional Services that are mutually agreed upon in a statement of work. Any Professional Services, for example, a facility condition assessment or consultancy services, are governed by our Professional Services Addendum. We have aligned these terms to the nature of the professional services provided and are diligent in making sure that our commitments are standard to our specific Service industry.

Why use the MSA?

Our Service is a "one-for-all" software model. Our MSA was specifically drafted to accommodate and describe the unique features of the Service. We regularly review our MSA to create a fair and balanced agreement based on customer feedback and industry accepted positions. If a Subscriber presents their own terms, we are unable to allow them to govern our Service because it frustrates our ability to provide the features of the Service in their intended manner and threatens our intellectual property rights.

I'm a public entity and I need to make changes to the terms. Can you accept my changes?

We have quite a few public entity Subscribers and have adjusted our MSA terms to be sure they reference the applicable laws that may govern your subscription when you are a public entity. Take note that: 1) Confidential Information is as provided under applicable law and exempted from disclosure, 2) Subscriber's indemnity is only to the extent permitted by law, 3) records requests allows for any public record requests permitted by law, 4) compliance with laws includes reference to any government rules and regulations, and finally 5) governing law in the USA will default to the applicable state law governing a public entity Subscriber. More specifically, the way the governing law section is written, the MSA is already governed by the state laws where a public entity Subscriber is domiciled and if a public entity cannot indemnify Brightly under applicable law, the indemnification shall not apply – no changes are needed.

Explanation of SaaS Terms

Can Brightly increase its liability limits?

A limitation of liability clause serves to limit a party's financial exposure in the event that a claim is made or a lawsuit is filed. For Brightly, we intend to align the responsibility for any such claim or lawsuit to the responsibilities of the parties to the MSA. For example, a construction vendor's claims or lawsuits would be much higher risk than a cloud Services provider. Brightly is entering into a commercial-off-the-shelf cloud Services agreement where Brightly is providing a one-for-all subscription to its software for Subscriber's use; therefore, Brightly must make its liability proportional and fair by limiting it to the value of the annual contract. This is appropriate for any cloud Services provider like Brightly because the Subscriber enters its own data, completes its own inventory management, etc. In situations where a Subscriber's operational or legal practices require a higher liability limit, it is likely due to increased responsibilities of the vendor (for example, a construction vendor) but is not fit for purpose for cloud Services.

What is Brightly's service level obligation?

The service levels are in accordance with our Service Level commitments set forth in Section 2.2, and are the same for all Subscribers. Brightly must be able to provide its cloud Services to all its Subscribers as a one-for-all model, where the Service Levels are the same for everyone. For this reason, we are unable to accept a Subscriber's own service level requirements.

What Third Parties are involved in the MSA?

There are two (2) ways in which Third Parties can be involved: 1) Subscriber may link the Services to a Third Party website, application or service (Section 1.2(f)), and 2) Brightly may use, embed or incorporate Third Party software in its Service (Section 1.3(c)). First, the links to Third Party websites are entirely at the discretion of a Subscriber; for example, you may choose to allow our Services to share data or interact with a procurement system, GIS mapping, etc. For all these interactions, Subscriber will have a licensing or subscription agreement with that Third Party, therefore its use will be outside of Brightly's control. Brightly is not responsible for these Third Party website interactions. Second, if Brightly uses, embeds or incorporates a Third Party software in our Services, it is entirely Brightly's responsibility. Brightly agrees that the use of these "Third Party Tools" is subject to our license terms with that Third Party Tool's provider, that it is sub-licensable and nonexclusive, but Subscriber is made aware of these commitments because any Subscriber breach of Brightly's Service's proprietary rights may also mean a breach of Third Party Tools' proprietary rights.

Customer Data / Security

Does Brightly have access to data?

You and your designated Account Users have complete administrative control of your Account and data. Brightly's Service requires access to a Subscriber's De-Identified Data to support the reporting, analysis, statistical and benchmarking features of the Service. Depending on the Service subscriptions in your Order Form, the nature of the data collected is focused around

infrastructure, asset and equipment information, work orders, Account User and crew member information, event information, and GIS location information.

How does Brightly protect data?

Brightly Software's Information Security program reduces risks to information resources through implementation of controls designed to safeguard the security, availability, and confidentiality of Subscriber data. Protecting all proprietary information relating to Brightly Software and our Subscribers is vital to our mission to be the global leader in intelligent asset management solutions.

Brightly Software protects the privacy of Subscriber data using a layered defense-in-depth approach to information security. Our cloud platform uses the industry-standard "shared responsibility" model. Built-in security and governance controls prevent unauthorized access to your data from both Brightly employees and any other parties. Subscribers create and manage users, load asset data, create workflows, perform data analysis, and export data using application features. Application Role-Based-Access Controls (RBAC) allow Subscriber administrators to configure appropriate levels of data access for their internal users.

Brightly has adopted security policies and implemented company-wide information security training to protect the privacy of Subscriber data. By policy, Brightly employees are prohibited from disclosing information obtained from Subscribers to any other person or entity except in the performance of services for the Subscriber and when explicitly authorized by the Subscriber. Under the shared responsibility model Brightly Client Services and Technology employees will only access Subscriber data as required to perform implementation and support services, to maintain security, and manage capacity.

All data transmissions over public networks are made using secure, encrypted connections. All Subscriber data is encrypted at rest. Depending on the Service subscriptions in your Order Form, Brightly applications provide for federated identity management using SAML 2.0-based SSO. This allows Subscribers to leverage their existing access control password and Multi-factor Authentication (MFA) policies.

Brightly Software's cloud platform is hosted in multiple secure AWS data centers with sites selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Physical access to data centers is limited to AWS employees and approved third parties. Access requests are only granted with a valid business justification. They are based on the principles of least privilege and are time-bound. Facility access is removed after the requested time expires.

Brightly Software has architected the hosting of our platform and applications over multiple AWS Availability Zones to achieve high availability and business continuity. AWS Availability Zones are built to be independent and geographically separated from one another. Individual data centers within each availability zone have deployed critical resources to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

How does Brightly demonstrate compliance?

Brightly undergoes third party audits, tests and certifications to demonstrate and document the operational and security measures that our customers expect. Depending on our geography and the selected Service, these include ISO certifications, PCI-DSS certification and regular penetration tests. Certain Brightly Services also have SOC 2 type II certifications.

Why can't Brightly use my security terms/requirements?

Brightly does not provide custom service offerings because the Service is commercial-off-the-shelf SaaS and we are unable to apply different security terms to only one specific Subscriber account. Brightly's security terms (against which we are regularly audited) apply to the Service as it's provided to all our customers. Brightly's security measures accurately capture how the Service works and how we provide security for the Service. We are not able to entertain one-off security exhibits that are written with other services or applications in mind, or to generically cover a wide array of services or applications.

How does Brightly enable compliance with GDPR?

Under applicable Data Protection Legislation, Subscriber and Brightly agree that Subscriber is the Data Controller and to the extent that Brightly processes personal data from the UK, Switzerland or the European Economic Area (EEA), the terms of a data processing addendum must be signed by the parties. A copy of our standard data processing addendum is available at www.brightlysoftware.com/terms.

How does Brightly enable compliance with HIPAA?

First, take note that our Service does not require the use of protected health information as defined by HIPAA. If applicable in the USA, and where the Subscriber is a Covered Entity, Brightly may enter into our business associate agreement with those Subscribers using the appropriate senior living Service. Our business associate agreement is designed to leverage the existing terms describing our Service, restrictions on our use and access to your data, and our security measures for our senior living Service.