LBS GDPR Compliance Statement

1 Introduction

The EU General Data Protection Regulation ("GDPR") aims to standardize data protection laws and processing across the EU, giving people greater rights to access and control their personal information. The GDPR imposes additional obligations on organizations that process the personal data of EU residents. It came into force on 25 May 2018.

2 Our Commitment

Laurel Bridge Software, Inc. (LBS) is committed to ensuring protection of all personal information that we may hold. Laurel Bridge Software is dedicated to safeguarding the personal information under our control and in maintaining a system that meets our obligations under the applicable regulations. We recognize our obligations in updating and expanding this commitment and our supporting programs to meet the requirements of GDPR and related privacy initiatives. Our practice is summarized in the sections below.

3 LBS Applications: Background Relative to GDPR

Laurel Bridge provides applications and solutions for imaging workflow, archive consolidation, and application development to the medical imaging industry. These applications are sold by Laurel Bridge, but are hosted, controlled, and managed by the application licensees.

LBS does not provide services that receive, collect, or store personal data from the EU or elsewhere. However, LBS products/software/applications may be deployed by licensees within the EU and such products may process personal health information (PHI) at the sites (organizations) where they are deployed; such information is not transmitted to nor managed by LBS. Any PHI processed by LBS software that may be installed at a client organization (client, customer, or OEM) is under the control of and managed by the client organization and is regulated and protected by that organization's policies and practices. LBS's software products primarily facilitate the transfer of medical imaging data between medical devices. Storage of PHI in such products, if any, is typically temporary and transitory in nature and is used to facilitate data transfer communication; because such information is temporary/transitory in nature, it is not generally intended for long-term storage and retrieval purposes, even by the client organization hosting the application.

LBS imaging workflow products/applications (used by OEMs and their customers/clients) support the necessary security features and options to allow them to be deployed by their users in a GDPR-compliant manner. Technically speaking, under GDPR definitions, LBS products are effectively "processors" of data on behalf of the application users, which are the "controllers" of the data. LBS products process (route, transmit, transfer, receive, store, filter) medical data that may contain PHI (i.e., data covered by the GDPR and other privacy regulations) in a transient way to support medical workflows. LBS products do not maintain or store either a designated record set or a legal health record for the data processed.

It is the responsibility of the LBS application users (licensees, end users, or OEM users and their customers/clients) to configure the installation and deployment of LBS's software applications securely, so that the installation and use meets applicable GDPR requirements or other privacy regulations. LBS assists the application users (including OEM users and their customers/clients) in this installation and deployment process. In addition, LBS may provide ongoing remote technical support services to users of LBS applications; such support activities and access may permit LBS personnel to view log files or application screens that may contain or display PHI. Such access, if any, is via secure means, is managed by and under the control of the host organization using the LBS applications, and is subject to applicable privacy agreements between the participants.

4 How We Prepared for GDPR

Laurel Bridge Software already had a consistent level of data protection and security across our Organization, but we have introduced new measures to ensure GDPR compliancy. Most data received or held by LBS relates to direct digital marketing or client relationships.

- Information Audit and Update — We carried out an audit of information previously held and ensured that it was compliant with the new regulations. We updated our consent information and sought consent from all our EU & non-USA contacts; for any contacts who did not provide consent, we deleted their records/information that we held.
- Policies and Procedures — we have revised our data protection policies and procedures to meet the requirements and standards of the GDPR and any other relevant data protection laws, including:
    - Data Protection - our main policy and procedure document for data protection has been revised to meet the standards and requirements of the GDPR and reflect our dedicated focus on privacy and the rights of individuals.
    - Data Retention and Erasure - we have updated our retention policy and schedule to ensure that we meet the "data minimization" and "storage limitation" principles and that personal information is stored, archived, and destroyed in accordance with our obligations. We have procedures in place to meet the new "Right to Erasure" obligation when applicable.
    - Data Breaches - our procedures ensure that we have safeguards in place to identify, assess, investigate, and report any personal data breach as early as possible.
    - International Data Transfers and Third-Party Disclosures - where Laurel Bridge Software stores or transfers personal information outside the EU, we have procedures in place to secure the integrity of the data.
    - Subject Access Request (SAR) - we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge
- Privacy Notice/Policy - we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
  Our Privacy Policy and Cookie Statements may be accessed via our corporate website at: www.laurelbridge.com/company, specifically at: http://www.laurelbridge.com/pdf/Privacy-and-Cookie-Stmts-LBS.pdf .
- Obtaining Consent – As noted above, we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information
- Direct Marketing - we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

5 Data Subject Rights

We provide easy-to-access privacy information via our website and direct marketing messaging. We note an individual's right to access information about any personal information that Laurel Bridge Software processes about them and to request information about:

- what personal data we hold about them
- the purposes of the processing
- the categories of personal data concerned
- the recipients to whom the personal data has/will be disclosed
- how long we intend to store your personal data for
- if we did not collect the data directly from them, information about the source

- the right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- the right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- the right to lodge a complaint or seek judicial remedy and who to contact in such instances.

6 Information Security and Technical and Organizational Measures

Laurel Bridge Software takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure to protect and secure the personal data that we process. We have information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure, or destruction.

7 GDPR Roles and Employees

Laurel Bridge Software has designated the Security Officer, Privacy Officer, and/or Data Protection Officer roles to Fred T. Beam and/or Bronson R. Hokuf and together they act as a data privacy team to develop and implement our roadmap for complying with the current and new data protection regulations and similar privacy initiatives. The team is responsible for promoting awareness of the GDPR within LBS, assessing our GDPR compliance, identifying any gap areas, and implementing the new policies, procedures, and measures that may be required.

Laurel Bridge Software understands that continuous employee awareness and understanding is vital to continued compliance with the GDPR and have involved our employees in our preparation, implementation, and plans.

If you have any questions about our GDPR compliance policies or other privacy issues, please contact us via email at: legal@laurelbridge.com.

--- end of document ---