LABSTATS' COMMITMENT TO COMPLY WITH THE CALIFORNIA CONSUMER PROTECTION ACT (CCPA)

Version: January 10th, 2020 (1.0)

1. Introduction
   - 1.1. The California Consumer Privacy Act (CCPA) provides California consumers with new rights regarding their personal information and imposes data protection responsibilities on certain entities that conduct business in California. The CCPA went into effect on January 1, 2020.
   - 1.2. Assembly Bill No. 1355 (AB 1355)
     - 1.2.1. AB 1355 adds an exemption for business contact information that a business collects during communications or transactions with another business or government agency. Specifically, AB 1355 exempts LabStats from most of the act's provisions on personal information about an employee, owner, director, officer or contractor of a business or government agency collected by a business as part of a transaction with another business or government agency, in the context of due diligence of, or the provision of products or services to, the business or agency.
2. LabStats and the CCPA
   - 2.1. Business Operations
     - 2.1.1. LabStats understands the requirements of the CCPA and recognizes the act's role in the company's business operations. As such, LabStats is committed to adhering to CCPA requirements, provisions and subsequent amendments as they pertain to the company's operations, products and services.
   - 2.2. Product and Services
     - 2.2.1. The LabStats product allows its users to collect limited non-sensitive personal information, which is controlled solely by the user. As a privacy option, LabStats users can also obfuscate unique identifiers within the product. If a data subject requests the deletion of personal information, the user should work with LabStats' Data Protection Officer (DPO) to navigate the deletion process from LabStats. Contact information for LabStats' DPO is available at the end of this document.
   - 2.3. Selling of Data
     - 2.3.1. The CCPA defines selling data as: "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."

2.3.2. LabStats does not sell any data that it collects operationally or data originating from the LabStats product.

3. Data Protection
   3.1. Physical and Digital Security
      3.1.1. For its cloud offering, LabStats utilizes Microsoft Azure data-centers, which employ many measures to protect operations and data from physical or virtual threats or intrusions. The data-centers comply with industry standards (such as ISO 27001) for physical security and availability. Data-centers are hardened and their locations are not published. They have extensive physical security in place, which include perimeter fencing, video cameras, security personnel, secure entrances, real-time communication networks, etc.
   3.2. Service Provider
      3.2.1. LabStats utilizes the Microsoft Azure cloud platform for delivering the LabStats product in the cloud. Microsoft Azure has a multi-decade long history as a software solutions provider. They are recognized as being the leading cloud platform provider, administering world-class security and risk mitigation, and have the most compliance certifications and attestations of any cloud provider.
   3.3. Data in Transit
      3.3.1. Data transmitted to and from the LabStats Portal and the LabStats Client Service (API) is encrypted using a TLS 1.2 SSL certificate with 2048 bit SHA-256 bit encryption. Certificates are kept current such that they will not expire.
   3.4. Data at Rest
      3.4.1. Certain sensitive data is encrypted at rest for an additional layer of security using 256 bit AES encryption with a private password and salt. The encryption is reversible by the LabStats Portal as is required to present data back to authorized Portal Users or to perform authentication against integrated network assets (in the case of Active Directory integration).
   3.5. Data Breach
      3.5.1. No breachs of any kind have previously occurred, and LabStats will notify organizations if there are real or perceived breaches in the future.

Please refer to our company privacy page for more information (https://labstats.com/privacy/). To contact LabStats' Data Protection Officer (DPO), email legal@labstats.com or call 1-208-473-2222.