LABSTATS' COMMITMENT TO COMPLY WITH THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR)

Version: November 19th, 2018 (1.0)

1. Introduction

1.1 LabStats is committed to providing all of its customers advanced data protection and security by following the regulations in the GDPR and by entities within and apart from the European Union. Our methods for collecting and processing data have been designed to protect the individual's identity and thus, their human rights. By default, high-level security measures have been implemented to protect data subjects and their personal data.

1.2 The EU General Data Protection Regulation (GDPR) is the most significant piece of European privacy legislation in two decades. It replaces the 1995 EU Data Protection Directive (European Directive 95/46/EC), strengthening the rights that EU individuals have over their data, and creating a uniform data protection law across Europe.

2. LabStats and the GDPR

2.1 LabStats has analyzed the requirements of the GDPR and has enhanced our services, products, documentation, and business practices to support compliance with the GDPR. In addition, LabStats is dedicated to assisting our customers with their GDPR compliance efforts as it relates to LabStas and its products.

2.1.1 One of the GDPR's significant differences from the 1995 EU Data Protection Directive is newfound attention on the data processor (LabStats). As the designated data processor, LabStats works to make sure that it handles and distributes personal data with utmost solidity and responsibility. Under the GDPR, both the data controller (LabStats' customers and partners) and the data processor have additional obligations to protect personal data, and both face liability for any failures to comply with the GDPR requirements.

2.2 Service Provider

2.2.1 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. Our Customers in the EU

3.1 As a current or future customer/partner of LabStats in an EU territory, what steps do I need to take to comply with GDPR?

3.1.1 Start preparing to comply with the GDPR as a data controller. Please consider the following steps to help you understand the GDPR's effect on your organization:

- Learn more about your role as a data controller in relation to LabStats' role as the data processor. See Appendix A for a side-by-side chart of the obligations of the data controller and processor.
- Audit your data and processes. Consider creating an updated and precise inventory of personal information that you control. Review your current controls and processes to ensure that they are adequate, and build a plan to address any gaps. Here are some steps you can take today:
    1. Review your field maps
    2. Review your process documentation
    3. Ensure you have a lawful basis for processing the data
- Stay informed. Get updated regulatory guidance as it becomes available and consider consulting a legal expert to obtain guidance applicable to you. We recommend a regular review of your country's independent data authority's website, which is the country's representative within the EU working group: Article 29.

4. Data Protection

4.1 Physical and Digital Security

4.1.1 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.

4.2 Data in Transit

4.2.1 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.

4.3 Data at Rest

4.3.1 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).

4.4 Data Breach

4.4.1 No breaches 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.

APPENDIX A—OBLIGATIONS CHART

	Controller (LabStats Customers and Partners)	Processor (LabStats)
Definitions	Art. 4(7) Under the GDPR, a controller is the entity that determines how and why personal data is processed.	Art. 4(8) Under the GDPR, a processor is the entity that processes personal data on behalf of a controller.
Data Protection by Design and Default	Art. 25 Starting from the very beginning of the planning stages and all the way throughout the implementation phases of any processing activity, the controller must embed appropriate technical and organizational measures to ensure that the activities are compliant with the GDPR. The controller must also limit the use of the data to its initial intended purpose.	N/A
Joint Controllers	Art. 4(7); Art. 26 A joint controller relationship occurs when two or more controllers determine the purpose and means of processing personal data. Joint controllers must apportion data protection compliance responsibilities among themselves and make this arrangement transparent to the data subject.	N/A

Liability of Joint controllers	Art. 28(1) – (3) A controller may only appoint a processor that can guarantee compliance with the GDPR. Once chosen, the controller must enter into a written agreement with the processor which states that the processor must: (1) Only act within the confines of the controller’s documented instructions; (2) Ensure that anyone who has access to the personal data is bound by confidentiality; (3) Ensure that the data they process is subject to sufficient security measures; (4) Respect the rules regarding appointment of sub-processors; (5) Assist the controller in implementing measures that enable them to comply with the GDPR;	N/A

Appointment of Processor	Art. 28(1) – (3) A controller may only appoint a processor that can guarantee compliance with the GDPR. Once chosen, the controller must enter into a written agreement with the processor which states that the processor must: (1) Only act within the confines of the controller's documented instructions; (2) Ensure that anyone who has access to the personal data is bound by confidentiality; (3) Ensure that the data they process is subject to sufficient security measures; (4) Respect the rules regarding appointment of sub-processors; (5) Assist the controller in implementing measures that enable them to comply with the GDPR; (6) Help the controller obtain DPA approval when needed; (7) Upon instruction from the controller, either return or destroy the personal data at the end of the controller-processor arrangement (unless EU or Member State law require storage of that data); and (8) Allow the controller access to all the information necessary to demonstrate that the processor is GDPR compliant.	Art. 28(1) – (3) A controller may only appoint a processor that can guarantee compliance with the GDPR. Once chosen, the controller must enter into a written agreement with the processor which states that the processor must: (1) Only act within the confines of the controller's documented instructions; (2) Ensure that anyone who has access to the personal data is bound by confidentiality; (3) Ensure that the data they process is subject to sufficient security measures; (4) Respect the rules regarding appointment of sub-processors; (5) Assist the controller in implementing measures that enable them to comply with the GDPR; (6) Help the controller obtain DPA approval when needed; (7) Upon instruction from the controller, either return or destroy the personal data at the end of the controller-processor arrangement (unless EU or Member State law require storage of that data); and (8) Allow the controller access to all the information necessary to demonstrate that the processor is GDPR compliant.
Compliance with Controller's Instructions	N/A	Art. 29 A processor is forbidden from processing personal data, unless the controller has given them documented instruction to do so, or EU or Member State law requires it.

Conflict with Controller’s Instructions and EU Law	N/A	Art. 28(3)(h) If a processor believes that the controller’s instructions are at odds with the GDPR or another EU or Member State law, the processor is required to immediately inform the controller.
Failure to Comply with Controller’s Instructions	N/A	Art. 28(10) When a processor breaches the controller’s instructions and begins to determine the purpose and means of processing, they will be considered a controller with respect to that processing activity.
Sub-Processors	N/A	Art. 28(2)-(4) A processor is forbidden from appointing a sub-processor without the prior written consent of the controller. A controller may provide processor with a general authorization to use sub- processors. If appointed, a sub-processor must be held to the same terms and standards that are set out in the initial contract between the controller and processor.
Confidentiality	Art. 25 A controller is required to implement appropriate technical and organizational measures to ensure that personal data is not accessible to any unauthorized entities.	Art. 28(3)(b); Art. 29 The processor is required to take certain measures to ensure that any personal data they process is kept confidential. This requirement must be disclosed in the contract between the controller and processor and must further specify that any person authorized to process the data is under an obligation of confidentiality.

Right to Erasure	Art. 17(1)-(3) A data subject has the right to require the controller to erase personal data concerning the data subject without undue delay in certain cases, including: (1) The personal data are no longer necessary for the purposes collected or processed; (2) The data subject withdraws consent; (3) The data subject objects to the processing on certain grounds; (4) The personal data has been unlawfully processed; or (5) The personal data must be erased for compliance with a legal obligation. There are exceptions to the erasure obligation, including cases where the processing of the personal data is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest, and for archiving purposes in the public interest.	Art. 28(3)(e) A processor must assist the controller to fulfill the controller's obligation to respond to requests for exercising the data subject's rights, including the right to erasure.

Records of Processing Activities	Art. 30 A controller must maintain records of their processing activities, including: (1) The controller's contact information, as well as any joint controllers, the controller's representative, and the data protection officer; (2) The purpose(s) of the processing; (3) The categories of data subjects and personal data processed; (4) The categories of recipients who will have access to the data; (5) Information regarding cross-border data transfers; (6) The expected data retention period; and (7) A general description of the security measures in place to protect the personal data.	Art. 30(2) A processor must keep records of its processing activities, including: (1) The name and contact information of the processor and controller; (2) The categories of all processing performed; (3) Information regarding Cross-Border Data Transfers; and (4) A description of the technical and organizational mechanisms in place to secure the personal data.
Cooperation with DPAs	Art. 31 Controllers must cooperate with the supervisory authorities in the performance of their tasks.	Art. 31 Processors are required to cooperate with any requests from the DPAs relating to the performance of their processing activities.

Appointing a DPO	Art. 37 A controller must appoint a DPO if local laws require it to do so, or if its data processing activities involve: (1) Regularly monitoring data subjects on a large scale; or (2) Processing sensitive personal data on a large scale. Organizations that appoint a DPO must publish the details of the DPO and relay those details to their DPA.	Art. 37 A processor should designate a DPO if local laws require it or where: (1) The processing is done by a public authority; (2) The core activities of the processor consist of processing activities which require systematic monitoring of data subjects on a large scale; or (3) The core activities of the processor consist of processing special categories of data on a large scale. Organizations that appoint a DPO must publish the details of the DPO and relay those details to their DPA.

Data Security	Art. 32 Controllers must implement appropriate technical and organizational measures to ensure that the personal data they are processing is adequately protected. Depending on the nature of the processing, the costs of implementation, and the purpose of the processing, these measures may include: (1) Pseudonymisation and encryption; (2) Systematic reviews of the integrity and confidentiality of the processing systems; (3) A backup system that is resilient and efficient enough to recover personal data in the event of a physical or technical issue; and (4) Regular testing of the technical and organization measures to make sure that they continue to adequately protect personal data.	Art. 28(1); Art. 28(3)(e); Art. 28(4); Art. 32 Processors must implement appropriate technical and organizational measures to ensure that the personal data they are processing is protected from accidental or unlawful destruction, loss, alteration, or disclosure. Depending on the nature of the processing, the costs of implementation, and the purpose of the processing, these measures may include: (1) Pseudonymisation and encryption; (2) Systematic reviews of the integrity and confidentiality of the processing systems; (3) A backup system that is resilient and efficient enough to recover personal data in the event of a physical or technical issue; and (4) Regular testing of the technical and organizational measures to make sure that they continue to adequately protect personal data. Adopting an approved Code of Conduct is one way to legitimize a processor's efforts.

Reporting Data Breaches	Art. 33 When a data breach occurs, a controller must report the event to the supervisory authority without undue delay and no later than 72 hours after becoming aware of it. The notification should: (1) Describe the data breach and include the number and categories of data subjects affected; (2) Include the name and contact information of the DPO; (3) Describe the expected consequences of the breach; and (4) Describe the measures taken to remedy the breach and its adverse effects. If the data breach is unlikely to result in any harm to the data subjects, then it does not need to be reported.	Art. 33(2) Processors are required to notify their controllers without undue delay in the event of a data breach.

Notifying Data Subjects of a Breach	Art. 34 When a data breach is likely to impede on the rights of data subjects, the controller must notify the affected individuals without undue delay. The notification must: (1) Include the name and contact information of the DPO; (2) Describe the expected consequences of the breach; and (3) Describe the measures taken to remedy the data breach and any adverse effects involved. The controller is exempt from this requirement if: (1) The controller has used encryption or another form of security measure to protect the data that was breached; (2) The controller has subsequently taken measures, such as suspending affected accounts, to ensure that data subjects' rights are unharmed; or (3) The notification would require disproportionate effort, in which case the controller must circulate a public communication informing potential data subjects of the breach.	N/A
Cross-Border Transfers	Art. 44 The GDPR forbids Cross-Border Data Transfers unless: (1) It's to an adequate jurisdiction; (2) A lawful transfer mechanism exists; or (3) An exemption applies. The obligation to assert a lawful transfer under the above scenarios applies directly to processors.	Art. 44 The GDPR forbids Cross-Border Data Transfers unless: (1) It's to an adequate jurisdiction; (2) A lawful transfer mechanism exists; or (3) An exemption applies. The obligation to assert a lawful transfer under the above scenarios applies directly to processors.

Liability of Joint controllers	Art. 82 A controller will be liable for any damage caused by its processing activities that infringe GDPR principles, unless the controller can prove that they were not responsible for the damage.	Art. 82(1) – (2) A processor is liable directly to a data subject for any damages caused by their processing activities where it has: (1) Not complied with their specific obligations as a data processor under the GDPR; or (2) Acted contrary to the instructions given by the controller.
Maximum Administrative Fines	Art. 83 The maximum fine that can be imposed for severe violations of the GDPR is the greater of €20 million or four percent (4%) of a company's worldwide annual turnover.	Art. 83 The maximum fine that can be imposed for severe violations of the GDPR is the greater of €20 million or four percent (4%) of a company's worldwide annual turnover.