LastPass and the GDPR

On May 25, 2018 the European Commission will require all global organisations conducting business in the European Union, as well as businesses maintaining or processing European Union (EU) personal data, to comply with the General Data Protection Regulation (GDPR). These new rules aim to provide EU citizens with greater control over how their personal data is collected, stored, transferred, and used, while also simplifying the regulatory environment across the EU.

LastPass' Compliance with GDPR

As a global company with customers in nearly every country in the world, protecting the personal data of our customers and their end-users continues to be a priority. GDPR represents an opportunity to continue our commitment in this area. LogMeIn (including LastPass) already participates in the EU-U.S. and Swiss Privacy Shield Frameworks and is compliant with current applicable EU data protection rules. At LogMeIn, our ongoing compliance review and actions build on our existing investments in privacy, security, and the operational processes necessary to meet the applicable requirements of GDPR by May 25, 2018.

To make sure that customers understand LogMeIn's general philosophy towards GDPR, our goals by the date it will be enforced, and how they may be able to use LastPass in a GDPR compliant way, it is important to remember a few points:

- In GDPR terminology, LastPass is a "Data Processor" and you, our customer, are the "Data Controller" for all Customer Content (as defined in the Terms of Service). This means that you are in charge of determining the fate of all data uploaded by you or users on your account. LastPass will comply with your instructions and the terms of any written agreement or contract as to how to deal with data (within the capabilities of the product).
- As Data Controller, you also own the relationship directly with users in your account – these users are considered to be "Data Subjects" under the GDPR. Data Subjects have certain rights under the law and LastPass provides tools for you to assist Data Subjects in their exercise of their rights.
- For your privacy and security, we will delete your vault data (i) at your request, or (ii) if your account is no longer provided under paid subscription and has remained inactive for an extended period of time.
- At any time, you have the right and the necessary tools, to get your sensitive vault data (content) out of LastPass. We make it easy for you to maintain your own local backup copy.

It is very important to remember that by using LastPass you are not necessarily or automatically fully GDPR compliant. We encourage you to verify that you meet all aspects of the regulations, and to get legal advice if needed.

Increasing Your GDPR Compliance with LastPass

As noted above, LogMeIn is well on its way to GDPR compliance and we believe that LastPass may be able to assist our customers in their compliance efforts by leveraging the following functionality:

- **Security:** LastPass is built on AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes to ensure data protection in the cloud. LastPass also operates on a hardened cloud infrastructure and passes many in-depth security reviews each year. This may help customers to address any requirements they may have around utilization of encryption, pseudonymization, and/or anonymization.
- **Data Minimisation:** Enterprise admin controls may be deemed an acceptable data minimization practice. This allows the data controller to specify who has access to sites and accounts, and report on login activity and such functionality. This may help customers limit their data collection to data that is relevant and necessary for the intended use.
- **Data Deletion:** LastPass allows customers to export their data and delete their account, if required. This feature may allow a customer to meet requirements around deletion of personal data after its intended use is complete, consent is withdrawn, or if a legitimate business purpose no longer exists.
- **Privacy-By-Design:** LastPass is built on the principle of zero knowledge. This means by default, only the data subject themselves can access their sensitive data and such functionality may be deemed an acceptable privacy-by-design practice.
- **The bottom line of GDPR?** It's all about ensuring data subjects' privacy and providing for the appropriate handling of personal data. We believe that if our customers are ever called upon to demonstrate their GDPR compliance (perhaps, for example, during an audit), that LastPass features may be able to help. LastPass also offers:
- **User Management:** Apply permissions to users and grant access based on the data and systems they need, and nothing more.
- **Security Policies:** Enforce policies for all employees, such as forced logoff after inactivity, password length and complexity minimums, sharing restrictions, and more.
- **Multi-Factor Authentication:** Require multi-factor authentication to your LastPass account, adding an extra layer of security to non-SSO enabled sites that include company data.
- **Password Strength Measurement:** Use the Security Challenge to identify websites affected by recent security breaches and prompt users to change passwords for those sites.
- **Personal Linked Accounts:** Encourage employees to create personal LastPass accounts, allowing them to store personal sites separate from the Enterprise, and link them for easy, secure access.

Learn more about LogMeIn's GDPR compliance, including product-specific Security and Privacy Operational Controls (SPOCs), at logmeininc.com/gdpr.