

The EU General Data Protection Regulation (GDPR) – Key Things to Know

At LivePerson, we understand that nothing is more important to our customers than the protection of their data, particularly in light of the EU General Data Protection Regulation (GDPR), which went into effect in May 2018. Below is an outline of the purpose of the GDPR and the steps LivePerson has taken in order to meet GDPR requirements as part of our ongoing commitment to protect consumer data and help our customers comply with the GDPR.

- 1) **GDPR's purpose.** The GDPR substantially enhanced previous privacy laws to give European consumers better control over their personal data in the digital world. The regulation creates a single set of privacy rules that apply uniformly across the EU and are directly enforceable in each EU member state. Notable new requirements under the GDPR include increased security standards, breach notification requirements and, most importantly, rights of consumers to access and correct their data, receive a copy of their data ('data portability'), or have their data deleted ('right to be forgotten').
- 2) **Personal data at LivePerson.** As part of our service to you, LivePerson may collect and store your customers' personal data, such as name, address, etc., from chat/messaging transcripts and other sources. LivePerson implements stringent security measures to ensure that data is protected in our systems. For an overview of those measures, please visit www.liveperson.com/security.
- 3) **LivePerson's GDPR compliance.** LivePerson has operated in Europe for years and actively monitors developments in European Union data privacy law to ensure our continued compliance to serve our EU customers. As such, we have the answers you are looking for when thinking about data privacy. A few highlights:
 - a. At LivePerson, we have robust security measures in place designed to meet and exceed your security requirements. For example, we offer a number of state-of-the-art data protection measures, including tokenization technology on payment card (PCI) forms, automated masking of chat transcripts, and optional AES encryption for data at rest.
 - b. Personal data of EU consumers is generally hosted on our European servers, and any transfers are pursuant to a valid transfer mechanism that protects the data once it leaves the EEA, such as a Data Protection Agreement (DPA) including the standard contractual clauses approved by the European Commission.
 - c. For our SMS feature, we have enabled message body redaction and phone number redaction to ensure that this personal consumer information is not stored outside of LiveEngage.
 - d. We have designed mechanisms and procedures to help you manage requests from data subjects for access to personal data and rectification, portability and deletion of personal data, including our Data Deletion API available at <https://developers.liveperson.com/personal-data-deletion-api-overview.html>, which enables you to request the deletion of personal data stored.
 - e. We regularly update our global privacy policy to address new requirements, available at <https://www.liveperson.com/policies/privacy>.

Please do not hesitate to reach out to your account executive with any questions or concerns.