

Online Communities and the GDPR

What you need to know about the GDPR, and how it impacts your financial services community.

Worried about GDPR? You're not alone.



60% of enterprises in the EU are concerned about complying with the GDPR¹

32% of banks and insurers have made strong progress in GDPR compliance⁴

59% of UK companies haven't yet received any GDPR-related training²

Preparations are underway, but consequences are looming.

80% of those affected by the GDPR will not comply with the regulation³

74% of consumers would switch banks or insurers after a data breach⁴

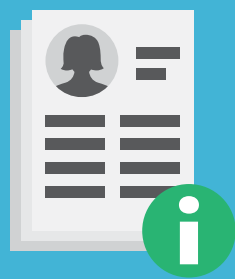
56% of enterprises in the EU think failure to comply will severely impact their brand reputation¹



€20M or 4%
of your revenue, whichever is greater, is the maximum penalty for non compliance

What do you owe your community members under GDPR?⁵

One of the primary imperatives of the GDPR is to protect the rights of individuals, also referred to as 'data subjects'. While there are over half a dozen individual rights outlined in the GDPR, the big ones that will apply to almost every single community include:



The right to be informed

You owe your members transparency. Let them know how you are collecting and using their personal data.

Best practice: review your current privacy policies and terms of service, and make any necessary changes in time for GDPR

Ask your provider: can we update our privacy policy or terms of service directly within the tool?



The right to data access & portability

Members have the right to access—and then edit, delete or export—their personal data in a way that is secure.

Best practice: ensure you and your community provider can handle requests to access, edit or transfer personal data

Ask your provider: can we simplify access with APIs? Can my members access their personal data or will they have to submit requests?



The right to be forgotten

If a member wants their personal data deleted, you must comply in a reasonable timeframe (30 days in most cases).

Best practice: put a plan in place for handling member requests to close their account or permanently remove their personal data

Ask your provider: can my members delete their account themselves? What happens to their content? How does data deletion impact my analytics?

Individual rights are an area where community platforms can—and should—provide functionality to make your path to compliance possible. Some other things to consider as you prepare for the GDPR include:

Consent

If consent is required, you must ensure that consent for processing and storing personal data is "freely given," and requested in "clear and plain language." You might choose to use a site pop-up, registration checkboxes, a notice on the homepage, or a variety of other customized solutions within your community.

Content

There may be personal data lurking in your community forums and threads, undetected . . . until it is. And while a member who is worried about personal data can delete their account, their content may live on forever. Consider setting aside resources to do regular content audits, and to fulfill your obligations to delete the data in the background or better yet—ask your platform provider to help.

Security is about more than just the GDPR

At Lithium, we believe in raising the bar when it comes to security and compliance. To learn more about our complete approach to security and privacy, visit www.lithium.com/security. To read our privacy policy, visit www.lithium.com/privacy. And for questions, contact privacy@lithium.com.



1- <https://senzing.com/wp-content/uploads/2018/02/Senzing-GDPR-Report.pdf>
2- <https://dma.org.uk/research/the-gdpr-and-you-chapter-four>
3- Forrester guide, Predictions 2018: A Year of Reckoning, November 2017
4- <http://www.capgemini-consulting.com/resources/data-privacy-and-cybersecurity-in-banking-and-insurance>
5- <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

Legal disclaimer—no legal advice. The above content is provided for informational purposes only and does not constitute legal advice. You should seek the advice of your legal counsel regarding your GDPR compliance efforts.

The Lithium engagement platform comprises Online Community, Social Media Management and Messaging products for social customer service, social support and social media marketing teams to listen, respond and act on customer conversations – creating deep relationships and fostering brand loyalty and advocacy. With over 15 years of expertise, Lithium has a massive digital footprint with approximately 480 million new digital interactions analyzed daily and 100 million monthly visitors across its Online Communities. The best Fortune 1000 companies in the world trust Lithium to help them build closer, more personalized and trusted relationships with their customers. Learn more at lithium.com, join our community at community.lithium.com, or follow us on Twitter @LithiumTech. Lithium is based in San Francisco.