5 Questions Financial Institutions Should Ask About GDPR Readiness
Many financial institutions already have operations in the European Union or may have plans to expand in the future.

If that is the case for your organisation, the General Data Protection Regulation (GDPR) rules will directly impact your institution’s usage and management of consumer data.
Even if your website simply collects data on EU citizens, you must comply or face significant fines of up to 4% of annual global turnover or €20 million, whichever is greater.

According to Forrester Research:

“One in three firms believes they are GDPR-compliant today — but they may not be.”
Here are 5 questions to consider regarding your GDPR readiness
1. Is there cross-organisational understanding of GDPR?

To ensure compliance with GDPR, you’ll need a strong cross-organisational team. It may include your:

- legal team
- privacy team
- marketing team
- infrastructure architects
- information security officers
- potentially an outside expert with special knowledge of the regulation.
Using multiple channels focused on serving the customer where, when, and how they prefer, financial institutions will be able to provide multiple points of contact with their customers.

This will enable financial institutions to deepen the relationships with customers and become “digital advisors”, guiding the customer in their decision-making throughout their daily financial life.
Most financial institutions have contact centers that are operating 24x7x365.

Delivering that breadth and depth of service requires huge amounts of contact information data across a variety of communication channels.

To comply with GDPR and quickly provide data to your customers, you must first have a handle on where all the data resides.

3. Can you quickly provide data to individuals who ask?
The “right to be forgotten” or the “right to erasure” of GDPR states the specific grounds for the right to request erasure of personal data.

Financial institutions that maintain a comprehensive view of all processes and systems dealing with personal data will be best positioned to respond to requests for “data portability”.

“Data portability” gives consumers the right to request access to, or the removal of, their own personal data from banks without the need for any outside authorisation.
5. How can a digital platform enhance GDPR preparedness?

Financial institutions that have technology built on an underlying end-to-end orchestration layer will have the governance, dynamic processes, and auditability necessary for compliance with GDPR. This approach allows older systems to work with new systems, without requiring retooling.
Learn More

appian.com/finserv

twitter.com/appian

facebook.com/AppianCorporation

linkedin.com/company/appian-corporation

youtube.com/user/appian

instagram.com/appiancorp