

5 Key General Data Protection Regulation Obligations

The GDPR seeks to create a more harmonized, unified data protection law framework for all EU countries and businesses using any EU citizen data with goals that include: Reinforcing and enhancing the data protection rights of EU data subjects, facilitating the free flow of data by harmonizing data protection laws across the EU and modernizing the law in line with emerging technologies.

1



Rights of EU Data Subjects

The GDPR enhances the data protection rights of EU data subjects' data worldwide. It codifies and clarifies data subjects' ability to request access to and erasure of their information (right to erase/to be forgotten). In addition, organizations need to provide easier access to personal data, with clear and easily understandable information on processing.

2



Security of Personal Data

Organizations will be obligated to report data breaches to regulatory authorities within 72 hours, and in high-risk scenarios, notify the individuals whose data may have been compromised. All data must have appropriate levels of security that correspond to the level of risk that it carries. Organizations have security obligations and can be in breach of the regulation if they don't take proactive steps.

3



Consent

Customer consent now must be explicitly obtained. How and where the data will be used must be disclosed to customers. Customers can withdraw their consent to any of these at any time, these factors will define how to lawfully retain their data if there is an extended need to do so.

4



Accountability of Compliance

Businesses should expect regulators to potentially exercise their powers to access data and premises, and should more generally be able to demonstrate compliance with the GDPR principles relating to personal data. Mechanisms to assist with providing this proof—including carrying out data protection impact assessments, adhering to codes of conduct and proactively seeking certification through approved mechanisms—will be made available.

5



Data Protection by Design and by Default

Data controllers must implement technical and organizational measures demonstrating compliance with GDPR core principles, ensuring the rights of data subjects are met and that only data necessary for the specific purpose is processed.

Learn more about how IBM could help you in your GDPR readiness and compliance initiatives at [ibm.com/gdpr](https://www.ibm.com/gdpr)

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.



© Copyright IBM Corporation 2017. IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.