Strengthening Privacy Protection with the European General Data Protection Regulation

Abstract

The exponential growth of digital data has led to a substantial increase in data breaches. To meet the privacy concerns of the digital world and place safeguards around personal data, the EU Parliament adopted the General Data Protection Regulation (GDPR) in April 2016. Enterprises can win customer trust if they comply with the practical measures listed in the GDPR.

Introduction

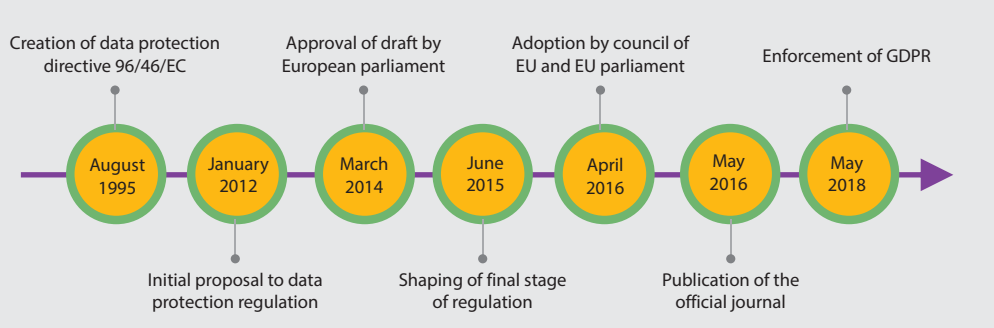
The European Union (EU) parliament adopted the General Data Protection Regulation (GDPR) to address evolving digital privacy challenges, and ensure that organizations collect, process, transfer, store, and dispose of the personal data of EU citizens without infringing upon their individual rights.

The ambit of this regulation includes:

- All EU organizations that process the personal data of EU citizens
- Organizations outside the EU that offer goods and services to EU citizens
- Businesses that process personal data by monitoring the behavior of EU citizens

88% of consumers feel that when choosing a company, safeguarding their personal data is more important than product quality (86%) or customer service (82%).[2]

GDPR Timeline



The GDPR timeline

The Path to Compliance

The GDPR has eight key features with which organizations need to comply.

1. Obtain the consent of data subjects

EU GDPR mandates consent for lawful processing of personal data. Data subjects should give consent freely, either through a statement or a clear affirmative action, and are free to withdraw the same at any time.

GDPR prohibits the processing of 'sensitive' personal data, barring a few exceptions. One of the important exceptions is that of 'explicit consent' provided by data subjects. However, the difference between consent and explicit consent has not been clearly articulated in the legal text. In the case of children, consent can only be given by the person holding parental responsibility for the child.

Organizations should:

- Revisit privacy notices to ensure that they are transparent and provide extensive information on processing personal data.
- Review the grounds for processing sensitive personal data and validate whether explicit consent has been obtained for processing sensitive data through clear, unambiguous, and transparent notices.
- Review existing personal data consent mechanisms for children, and implement appropriate technologies or processes.
- Validate whether legitimacy of processing is in line with GDPR requirements if processing of personal data is not based on consent.

2. Ensure the rights of individuals

The GDPR empowers data subjects by introducing new rights to existing data protection directives, such as:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Organizations should:

- Comply with each right and respond to a customer's request within a month, failing which they will be liable for fines.
- Review current profiling activities to ensure compliance with regulatory requirements.
- Analyze existing request handling mechanisms, and create processes to deal with requests from data subjects.
- Maintain an inventory of personal data flows to deal with new rights related to erasure and data portability.
- Define and implement retention rules for various data categories.

In essence, Organizations should create a privacy culture and implement appropriate measures to ensure that privacy is all pervasive in the overall IT strategy.

3. Demonstrate accountability

The onus of demonstrating GDPR compliance and proving it to supervisory authorities upon request will now be on data controllers.

Organizations should:

- Train employees on GDPR obligations.
- Protect personal data with appropriate safeguards, such as encryption, pseudonymization, Data Leakage Prevention (DLP), Information Rights Management (IRM), and Identity and Access Management (IAM).
- Adhere to approved codes of conduct and certification mechanisms.
- Conduct regular privacy audits of third parties processing personal data.
- Assess and modify the existing international data transfer process.

4.Assess data protection impact

Article 35[3] of the GDPR mandates that organizations should conduct data protection impact assessments that highlight the purpose of processing, data flow analysis, and identified risks and safeguards implemented to protect personal data.

5. Ensure data protection –by design & default

Article 25 of the GDPR highlights the concepts of privacy by design and default.[4]

Data protection by design requires controllers and processors to embed privacy controls throughout the data lifecycle of new projects and systems. Privacy by default requires data controllers and processors to implement measures that ensure that they only collect, process, and store data that fits the intended purpose.

Organizations should, therefore, implement procedures to ensure that, by default, personal data is not made available to an indefinite number of users.

6. Appoint data protection officers (DPOs)

Article 37 of GDPR mandates the appointment of DPOs for public authorities.[5]

DPOs will also need to be appointed for controllers or processors involved in:

- Large scale regular and systematic monitoring of data subjects
- Processing sensitive personal data
- Processing data related to criminal conviction and offenses

Organizations should appoint a data protection officer with expert knowledge of data protection laws and practices.

7. Report data breaches

Organizations must report personal data breaches to a supervisory authority, and in some cases, to affected data subjects, within 72 hours of becoming aware of the breach. Controllers should also provide additional information on the nature and consequence of data breach, categories affected, and measures taken to resolve the issue.

Organizations should:

- Send the data breach report to the supervisory authority.
- Notify affected stakeholders.

8. Avoid sanctions

Organizations should:

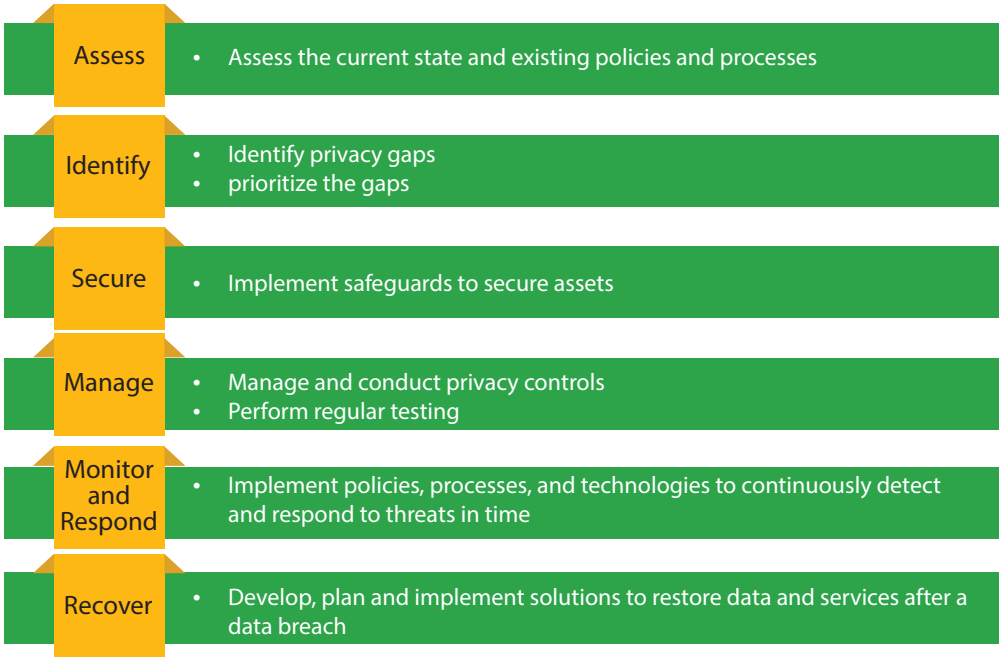
- Analyze and balance data value and data protection to reduce privacy risk.
- Classify data collected into risk categories.
- Create an overall risk score for systems.
- Invest in data protection technologies.
- Conduct privacy impact assessments and privacy control testing to help identify security gaps and bridge them.
- Consider cyber liability insurance to minimize losses.

Organizations found in violation of the new regulation could be charged as much as 4% of their global turnover or 20 million EUR, whichever is higher.

Preparing for the New Privacy Regime: Where to Start

The journey towards GDPR compliance should start with a thorough assessment of the current state, existing policies, and processes, along with implemented security measures to identify gaps with respect to GDPR requirements. Based on these gaps, organizations can prioritize various measures and implement them in a phased manner and thus comply with the regulation when it comes into force.

This is a framework that organizations can use to build a privacy strategy and ensure GDPR compliance.



A framework to ensure GDPR compliance

Conclusion

GDPR is the future of data privacy. It shifts the balance of power from data controllers and processors to data subjects by empowering them with greater control over their personal data. Although the road to compliance is challenging, GDPR presents an excellent opportunity for businesses to create customer trust and delight by demonstrating their renewed commitment to securing personal data.

References

[1] The ITRC Data Breach Report (2015), accessed Sep 2016, http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

[2] Symantec, State of Privacy Report 2015, accessed Aug 2016 https://www.symantec.com/en/uk/about/news/resources/press_kits/detail.jsp?pkid=state-of-privacy

[3] Official Journal of the European Union, May 4, 2016, accessed August 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

[4] Official Journal of the European Union, May 4, 2016, accessed August 2016http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

[5] Official Journal of the European Union, May 4,2016, accessed August 2016http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

TATA CONSULTANCY SERVICES

About The Authors

Swastik Mukherjee

Swastik Mukherjee is a Data Privacy and Protection Consultant in the TCS' Enterprise Security and Risk Management business unit, and helps assess organizational privacy posture across various industries and provides solutions to improve their privacy maturity and compliance.

Siddharth Venkataraman

Siddharth Venkataraman is a Data Privacy and Protection Consultant in the TCS' Enterprise Security and Risk Management business unit, and evaluates organizational privacy positions to enhance privacy maturity and compliance capabilities.

Contact

Visit TCS' Enterprise Security and Risk Management services unit page for more information

Email: Global.esrm@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services | M | 11 | 16