

# General Data Protection Regulation

## Introduction

On 15th December 2015, following three years of drafting and negotiations, the European Parliament and Council of the European Union reached an informal agreement on the EU General Data Protection Regulation (GDPR). The aims of the GDPR are to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce the administrative burden. The GDPR replaces the 1995 General Data Protection Directive and applies directly to each of the 28 EU Member States.

On 14th April 2016, the Regulation and the Directive were adopted by the European Parliament. The new rules are applicable for two years.

### The Main Changes for Citizens:

- ▶ When an individual no longer wants their data to be processed, the data must be deleted ("right to be forgotten")
- ▶ Individuals have the right to more information on how their data is processed, available in a clear and understandable way
- ▶ A right to data portability will make it easier for individuals to transmit personal data between service providers
- ▶ An individual has the right to know when their data has been breached

### The Main Impacts for Companies and Organizations:

- ▶ Companies and organizations must notify their national supervisory authority of data breaches which put individuals at risk and communicate all high risk breaches as soon as possible to the data subject
- ▶ Data protection safeguards must be built into products and services (Data protection by Design and by Default) from the earliest stage of development. Privacy-friendly default settings will be the norm – for example on social networks or mobile apps
- ▶ For companies who do not comply with EU rules, data protection authorities will be able to issue fines of up to 4% of their global annual turnover
- ▶ As part of the reform, companies based outside of Europe will have to apply the same rules when they offer goods or services within the EU market
- ▶ One pan-European law for data protection replaces the current inconsistent patchwork of national laws, meaning that Companies will now deal with one law, not 28
- ▶ The Regulation, being technologically neutral, enables innovation to continue to thrive under the new rules
- ▶ Companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU

### Journey to Compliance and Competitive advantage

2016

Timeline

2018

Business Case Development

GAP Analysis

Align business

Design

Implement

Monitor

## How can EY help?

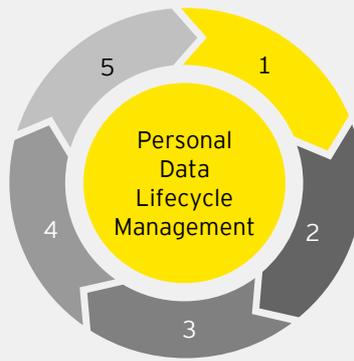
EY has a team of over 200 Certified Information Privacy Professionals (CIPPs) and Privacy Lawyers who help organizations to better understand what risks exist with respect to data privacy and compliance with the GDPR.

We draw on our global privacy team to deliver insights into legislations and regulations across the world.

For over a decade, EY has assisted international organizations in understanding privacy and data protection risks, compliance as well as regulations, thereby helping them effectively manage the use of personal information within their organization.

We can help you to deliver and run privacy improvement programs by leveraging our senior stakeholder management expertise, privacy framework, mature tools, methodologies and flexible resourcing models.

## Personal Data Lifecycle Management



1. Appropriate collection of data
2. Relevant use of data
3. Managed disclosure
4. Appropriate retention and disposal
5. Review of privacy expectations

## Privacy Transformation Program

Understand and manage the impact of the GDPR through your organization by using our privacy transformation program methodology.

We can help you to better understand the privacy, risk and compliance implications of how personal data flows throughout your organization.

## Other Services

EY can deliver a wide range of services:

- ▶ Privacy Impact Assessments (PIA)
- ▶ Personal Information and Inventory Data Flow
- ▶ Vendor Risk Management

One of our biggest credential in India is Support on GDPR implementation for one of the largest global ITES players. We are working with them for the following activities: Development of personal information inventory for client processes, development of methodology conducting Privacy Impact Assessment, review and update the privacy framework to accommodate GDPR requirements and development of content for GDPR awareness.

