



# GENERAL DATA PROTECTION REGULATION

A PRAGMATIC APPROACH  
TO IMPLEMENTATION

---

EXPERTS WITH IMPACT

# General Data Protection Regulation

In 1995, the European Union released the European Directive 95/46/CE which was the first mandated directive in relation to personal data protection.

By 2012, the European Commission put forth a proposal to reform the legislation, as a response to new challenges in the protection of personal data and represent the Digital Age. On the 4th May 2016 the EU officially published the General Data Protection Regulation (GDPR) with a view to implementing harmonised data protection legislation across Europe. The GDPR will be enforced from the 25th May 2018.

- Increase in Territorial Scope
- Elevated Threshold of Consent
- Further Processing Diligence
- Due Diligence on Vendor Processing
- Introduction of PIA's
- Increased Breach Requirements
- Mandatory Data Protection Officers
- Enhanced Privacy Rights

## DID YOU KNOW?

**63%**\*

of data compliance officers have highlighted that their privacy maturity is at early or mid stages of maturity.

**31%**\*

of organisations have a planned increase in employees related to regulatory compliance.

**67%**\*

of executives highlight privacy as the key regulatory and legal compliance initiative.

**90%**\*\*

estimated increase in fines from £1.4bn in 2015, to £122bn in 2018.

### SOURCE:

\* IAPP Annual Privacy Governance Report

\*\* Payment Card Industry Security Standards Council



# What's Changed?

1995

- Limited Accountability and European Reach
- Local Law Divergence
- Exposure to Multiple Data Protection Authorities
- Reactionary Privacy & Control
- No Obligation to Report on Breaches
- Right to be Remembered
- Limited Financial Repercussion

2018

- Global Reach and Verbose Accountability
- Uniform Regulation Across the EU
- Centralised Data Protection Oversight
- Privacy by Design
- Obligation Without Delay
- Extended Data Requirements
- Right to be Forgotten
- Two-Tier System of Enforcement

## WHAT DOES THIS MEAN?

A fine of the greater of **4%** annual turnover or **€20m** for:

- Non-Compliance on Core Principles
- Non-Compliance with a Supervisory Authority Order



A fine of the greater of **2%** annual turnover or **€10m** for:

- Failure to Obtain Parental Consent
- Lack of Data Breach Notification
- No Designated Data Protection Officer



# What do you need to consider when implementing changes for GDPR?

---

## GDPR Readiness



### SYSTEMS

How does personal and sensitive data move within and outside the organisation?

Do you have systems to process the new rights provided to data subjects?



### MODELS

Are the analytical models using personal data legitimately?

Do you use automated decision making models?



### DATA

What personal and sensitive data is processed by the organisation?

Are there legitimate and fair grounds for capturing and using personal data?



### OPERATIONS

Have you appointed a DPO and empowered them?

Do you have an organisation to manage data breaches and other communications?



### CONSENT & COMMS

Do you have consent from data subjects to use the data for existing processes?

Do you need to communicate new privacy policies and/or seek fresh consents?



### PEOPLE

How ready are your HR teams and employees to comply with and apply the changes?

Do you have training plans and modules in place?



### GOVERNANCE

Is your current internal control environment adequate?

Where do additional/replacement controls need to be designed?

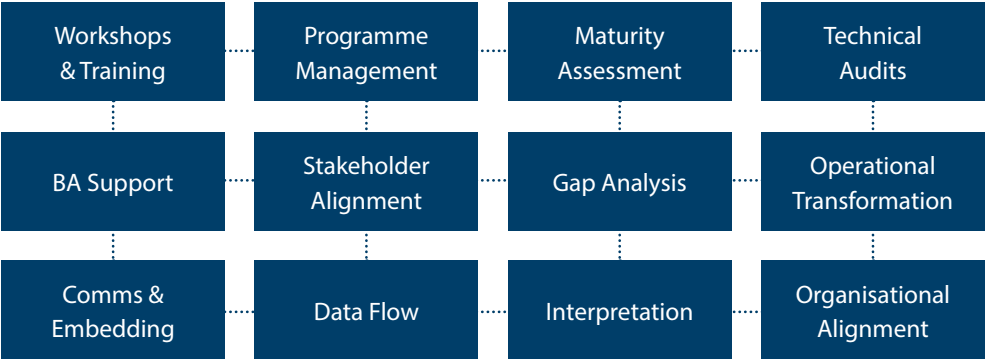


### EMBEDDING CHANGE

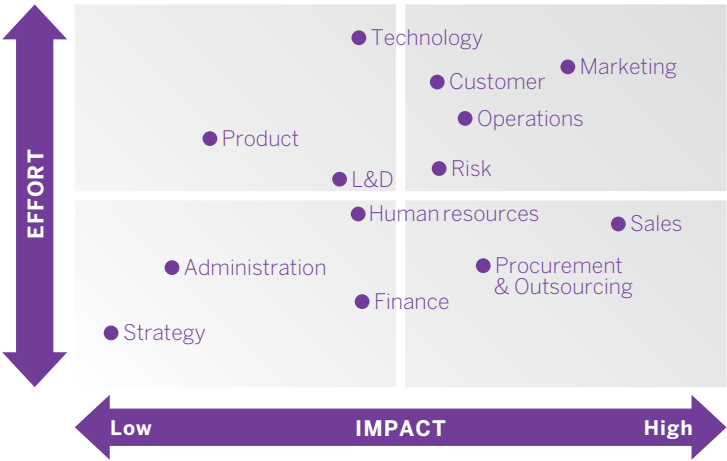
Which people and HR processes need to be updated to ensure the changes are embedded?

How are you communicating the changes internally and externally?

# How can FTI support you?



GDPR requires a diligent level of inter-organisational co-operation, in particular across high risk areas such as customer, marketing, risk and sales.



# Sample Implementation Timeline

## How far have you got to travel?

### DIAGNOSIS

#### Phase 1

##### Objective

Understand the processes at risk due to unavailability of consent, restricted use of data, and inadequate security, among others, and the potential opportunities of enhanced use of data.

##### Duration

4 – 12 Weeks\*

##### Deliverables

- Data map listing all personal and sensitive information
- Identify the supply chain of personal data to track movement of data within and beyond the organisation
- Audit analytical models and dashboards for unlawful use of data
- Maturity model of all systems & processes at-risk

### PROCESS & ALIGNMENT

#### Phase 2

##### Objective

Modify operating model to comply with the regulation. Complement existing data management infrastructure to support the process changes while maintaining appropriate and regular contact with government officials responsible for implementation.

##### Duration

4 – 18 Months\*

##### Deliverables

- Process audits to safeguard lawfulness of data usage
- Process designs for data subjects to exercise new rights introduced in the regulation
- Consent management strategy for deployment of privacy notices and renewal of consent
- Enhanced data enterprise and governance
- Implementation of security provisions including pseudonymisation and encryption where appropriate
- Start to plan internal and external communications

## ORGANISATION ALIGNMENT

### Phase 3

#### Objective

Align your organisation with business imperatives and manage the change in regulatory environment.

#### Duration

1 – 4 Months\*

#### Deliverables

- Audit vendors and internal teams to comply with GDPR
- Develop a programme to leverage GDPR as a catalyst for digitalisation, such as adopting sophisticated techniques for customer master data management
- Data coordinator roles and responsibilities denoted
- Policies and procedures amendments are completed
- Communicate the changes internally and externally
- Plan and deliver the training for HR and employees
- Review your recruitment and on-boarding processes

## CERTIFICATION

### Phase 4

#### Objective

Manage the compliance journey and reduce implementation cost.

#### Duration

1 – 3 Weeks\*

#### Deliverables

- Design of a tailored privacy impact assessment (PIA)
- Monitor and audit proof of compliance
- Develop a project-review dashboard for prioritisation of compliance activities

\* Dependent on organisational complexity



EXPERTS WITH IMPACT

Paul Prior  
Managing Director  
+353 879665296  
paul.prior@fticonsulting.ie

Mark Higgins  
Senior Managing Director  
+353 868343384  
mark.higgins@fticonsulting.ie

Sonia Cheng  
Senior Director  
+44 2037271783  
sonia.cheng@fticonsulting.com

Karen Hulme  
Managing Director  
+44 2033195724  
karen.hulme@fticonsulting.com

#### About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

[www.fticonsulting.com](http://www.fticonsulting.com)

©2017 FTI Consulting, Inc. All rights reserved.