

# A new compliance journey



**“You have to learn the rules of the game and then you have to play better than anyone else”**

Albert Einstein

**“The [EU Data Protection Directive] remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity.**

**This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market.”**

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

## Previous regulatory regime

Before the introduction of the EU Data Protection Directive in 1995, Data protection across Europe was initially largely unharmonised, leading to businesses facing different obligations across the various Member States. The Directive created a set of laws to be transposed into national legislation across Europe – the general principles were consistent but each Member

State was given leeway in its interpretation, which certainly gave some sense of a unified approach to data protection in the EU, but businesses continued to face conflicting requirements.

## Necessity for change

Given the exponential rise in new technologies and ongoing issues with uncertainty of the interpretation of the Directive across Europe, it was felt that a new regime was necessary to cope with the digital revolution that we find ourselves in.

## Proposed changes

It has been a while in the making, but agreement as to the wording of the General Data Protection Regulation (“GDPR”) has now occurred. Of course, because of its status as a Regulation, the GDPR will be directly applicable in all Member States and will automatically apply without any further input or interpretation from Member States.

While the GDPR was initially discussed in terms of providing a lesser administrative burden and a higher degree of certainty for business, the reality has not reflected that ideal. The GDPR will massively increase the administrative and compliance burden for business. Indeed, because of the potential impact on businesses, there was an unprecedented level of lobbying surrounding the reforms. There had been 4,000 amendments within the 18 months following the proposal of the GDPR, making this the most lobbied regulation in the history of the European Parliament.

The GDPR will benefit EU Citizens by providing a greater control over their personal information, due to new transparency rules, greater rights for them to seek compensation and through a toughening-up of the regulators’ powers. However, this does cause a headache for

entities, which must consider this challenge properly and face up to the task ahead.

## Compliance journey

The GDPR contains a series of new rules that require entities to revisit and refresh their systems and operations for data protection. Collectively, these new rules lay down a new “Compliance Journey” that entities will have to follow to keep on the right side of the law.

There can be little doubt that the GDPR presents a big issue for many entities and particularly those with large stores of personal data or business models based on the commercial exploitation of personal data. The compliance journey involves innumerable challenges and the task is complex. Entities may find that they have difficult choices to make about their priorities moving forward. Ensuring compliance with the GDPR will require considerable resource investments and lots of planning.

The harsh regulatory and litigation risks are considerable and especially so for entities that process sensitive personal data. It appears inevitable that litigation in this sector will follow the example set in the United States, which frequently sees claims being commenced before the courts for compensation after privacy and security breaches.

This comes at a time of a lot of stress in the international transfer environment, following recent, high-profile litigation. Entities will need to ensure that global data sharing and transfer models are capable of proving operational adequacy in the event of challenge.

The GDPR is an important change and one that represents obligations and tensions that must be considered carefully.

# PwC's global privacy practice

## 1. Analyse

What data will you process, how and why?

## 2. Risk Assess

What are the risks and what harms can be caused?

## 3. Consult

Which stakeholders do you need to consult with?

## 4. Design

How will you built in data protection from the beginning of processing?

## 5. Document

How will you prove compliance?

## 6. Engage

What information should you give to the public and what consents do you need?

## 7. Challenge

How will you handle incidents, problems and complaints?

## 8. Supervision

How will you handle the application of legal rights and supervisory powers?

## 9. Sanctions

How will you cope with the most serious regulatory sanction and civil litigation?



# PwC Luxembourg Contacts



**Vincent Villers**  
Partner  
2367  
vincent.villers@lu.pwc.com



**Frédéric Vonner**  
Partner  
4173  
frederic.vonner@lu.pwc.com



**Cédric Nédélec**  
Data Protection Officer  
2186  
cedric.nedelec@lu.pwc.com

Document version 2. This publication has been prepared by PricewaterhouseCoopers Legal LPP (1, Embarkment Place, London, UK, WC2N 6RH) for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Legal LLP (London), its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers Legal LLP (London). All rights reserved. PricewaterhouseCoopers Legal LLP (London) is a member of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.