



# The General Data Protection Regulation

The clock is ticking, are you prepared?

## Why is privacy an issue for you?

The digital revolution, together with the proliferation of social media and mobile devices has resulted in a more targeted approach to reach consumers.

Companies are now processing and holding an increasing volume of personal information about their clients and consumers, as well as employees and suppliers. The globalization of systems, processes and supply chains adds to the complexity of ensuring the safety and security of personal information.

Whilst this represents a new way of doing business and a great opportunity, it also presents new challenges. Namely, handling this personal information appropriately and managing the additional Privacy risk it exposes an organization to.

In addition to this, the fast changing regulatory landscape places increased complexity for global organizations in managing personal information in a compliant manner.

## What is the GDPR and why should you care?

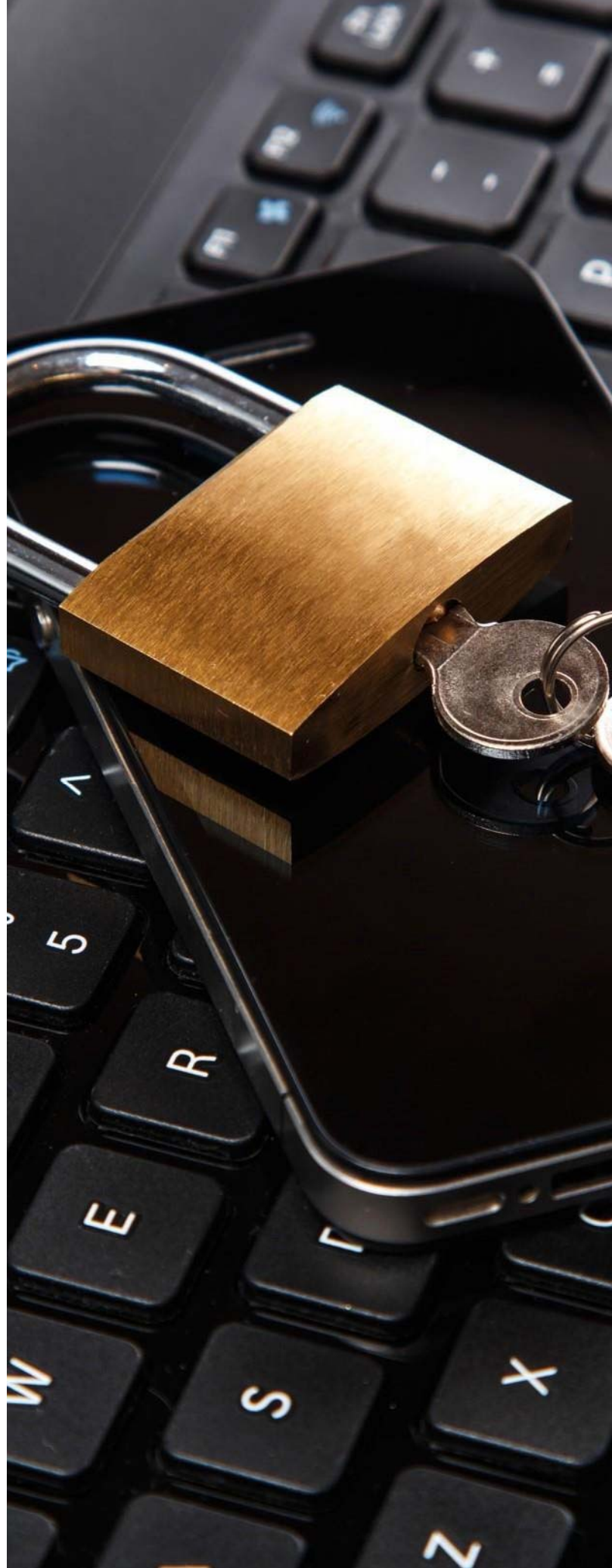
The General Data Protection Regulation (GDPR) is the European's view on what the baseline expectations are for processing personal information of EU citizens as we continue through the digital revolution.

Its ratification after four long arduous years of negotiation by European legislators sends a strong signal across the world that Europe continues to take Privacy extremely seriously.

Without question, the GDPR is a strong piece of legislation and represents a clear shift from the current Privacy regulatory environment in the EU. To use a simple example the current Privacy framework is like a domestic cat – you can largely ignore it so long as you feed it regularly and in the worst case, it will give you a minor scratch. The GDPR is closer to a tiger – pay close attention otherwise it will have your arm off!

The GDPR introduces a raft of onerous and complex new requirements, some of which are explored on the next page. Importantly, for the first time, we will in theory have a single set of Privacy rules across the European member states, and this harmonization goes even broader as the GDPR has cross-territorial implications.

It will be small consolation that organizations will have less than two years to prepare with the GDPR coming into force in May 2018. Most will have a lot of work to do before then.





“With the revised requirements, the expanded EU regulators’ jurisdiction and potential enforcement powers, the GDPR has catapulted privacy up the list of global organizations’ enterprise risks, requiring them to re-evaluate and take action. Privacy needs to be at the heart of your business strategy and not an afterthought!”









**Mark Thompson**  
Global Privacy Advisory Lead  
KPMG in the UK



## What are some of the changes introduced by the GDPR?

The GDPR transforms a number of existing requirements and introduces a raft of new ones. These changes are complex and are likely to require significant enhancements in the way organizations process personal information.

	EU Data Protection Directive	GDPR
 <b>Fines</b>	Fines vary by jurisdiction (e.g. UK £500,000)	A tiered fining structure depending on infringement. Level 1 is <b>2% of global turnover</b> or €10m (whichever is higher). Level 2 is <b>4% of global turnover</b> of €20m (whichever is higher)
 <b>Data protection officer (DPO)</b>	Generally no requirement to appoint a DPO	DPO <b>required</b> for 'government bodies' and organizations conducting <b>mass surveillance</b> or <b>mass</b> processing of <b>Special Categories</b> of data
 <b>Supervisory authorities (SA) enforcement powers</b>	SAs' have limited powers under national law	SAs' will be given <b>wide-ranging</b> powers
 <b>Inventory</b>	<b>No requirement</b> to maintain a personal information inventory	Generally organizations will need a personal information inventory
 <b>Breach notification</b>	Generally there are no obligations to report breaches	Requirement to report Privacy breaches to the regulator within <b>72 hours</b> and potentially to the Data Subject
 <b>Security</b>	<b>Vague requirements</b> around security (i.e. 'adequate level')	<b>Explicit requirements</b> around monitoring, encryption and anonymization

"GDPR will require some non-EU businesses that operate in the EU to re-think parts of the activities they carry out in the EU. This makes it much harder to operate certain 'global' services, and will require them to truly put an EU lens on business activities which are undertaken in the EU market."



**Doron Rotman**

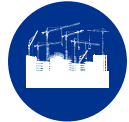
National Privacy Advisory Lead  
KPMG in the US



## What are some of the changes introduced by the GDPR?

### EU Data Protection Directive

### GDPR



#### Privacy Impact Assessments (PIAs)

There is no mandated requirement to perform PIA's

Companies should perform PIAs if the activity is **considered 'high-risk'**



#### Data Subject's Rights

Various rights, including right of access

Rights extended to include **Data Portability** and the **Right to Erasure**



#### Sensitive Personal Data

This includes **religious beliefs, physical/mental health** and **ethnic origin** amongst others

**Similar** but extended to include **biometric and genetic data**



#### Consent

Potential to rely on **'implicit'** consent depending on jurisdiction

Requirement to gain **unambiguous** consent (i.e. explicit)



#### Data Processors (DP)

Processors have limited regulator exposure for processing activities

Processors **are also covered**. Controllers must conduct **due diligence** into processors suitability

"The GDPR sent a strong message to the APAC business community. As result APAC based organizations have woken up to Privacy, they recognise that in order to be successful they need to think about privacy."



#### Dani Michaux

Asia Pacific Cyber Lead  
KPMG in Malaysia



## What do you need to do?

- Understand your current maturity through conducting a GDPR readiness assessment. Not a tick box exercise but a pragmatic focused exercise to really understand the GDPR privacy risk exposures which exist across your operations
- Focus on building pragmatic and realistic GDPR improvement plans, which will help you manage your risk to an appropriate level in line with your overall business strategy. Make sure you have a clear view of what success looks like
- Deliver your programme, focussing on those areas that are of greatest risk and embedding controls as part of day to day business operations. Getting privacy right is about managing risk appropriately and remember getting privacy right will increasingly become a differentiator as customers look to add increasing scrutiny over their personal information



## How KPMG firms can help?

We have deep experience of supporting organizations as they address their privacy challenges. KPMG firms team of experts can adopt a structured and flexible approach to meet the needs of your business. Areas where KPMG firms are frequently engaged:



**Assess** – Provide an independent assessment of current GDPR risk profile and how this compares to desired state

**Implement** – Support the implementation of robust and sustainable GDPR processes, policies and controls to allow you to mitigate your Privacy risk



**Operate** – Provide ongoing support and advice to assist you in operating your GDPR control environment



**Design** – Work with you to design a Privacy Compliance Programme to meet requirements of legislation such as the EU GDPR



**Strategy** – Work with you to develop a pragmatic GDPR Privacy strategy and gain buy-in from Senior Management



**Monitor** – Support you in maintaining your GDPR Privacy control environment

## Why choose KPMG?



### Our people

KPMG's privacy team includes recognised industry leaders and over 200 International Association of Privacy Professionals (IAPP) members. In addition, many KPMG firms have access to KPMG Law Legal Services whose Legal specialists have supported us on a range of privacy/GDPR Programmes



### Our experience

KPMG firms have supported clients on solving specific niche privacy challenges to delivering end-to-end Privacy Compliance Programmes, in complex and highly regulated industries



### Global, Local

KPMG's global reach allows us to work with in a consistent manner with global organizations and its entities across multiple territories at a local level



### Our approach

KPMG's proprietary approach and supporting enablers are tried and tested and help cut through complexity and expedite your GDPR activities



#### Mark Thompson

Global Privacy Advisory Lead  
KPMG in the UK  
T: +44 7747 565 630  
E: mark.thompson@kpmg.co.uk



#### Doron Rotman

US Privacy Advisory Lead  
KPMG in the US  
T: +1 4083 677 607  
E: drotman@kpmg.com



#### Dani Michaux

Asia Pacific Cyber Lead  
KPMG in Malaysia  
T: +60 3772 133 88  
E: Danimichaux@kpmg.com.my

# Contact us

**Walter Risi**

**Argentina**

E: wrisi@kpmg.com.ar

**Chris Eaton**

**Bermuda**

E: chriseaton@kpmg.bm

**Jorge Castro**

**Chile**

E: jorgecastro@kpmg.com

**Kasper Carøe**

**Denmark**

E: kcaroe@kpmg.com

**Mayuran Palanisamy**

**India**

E: mpalanisamy@kpmg.com

**Jonathan Brera**

**Italy**

E: jbrera@kpmg.it

**Dani Michaux**

**Malaysia**

E: danimichaux@kpmg.com.my

**Olumide Olayinka**

**Nigeria**

E: Olumide.Olayinka@ng.kpmg.com

**Imelda Corros**

**Philippines**

E: icorros@kpmg.com

**Lyon Poh**

**Singapore**

E: lpoh@kpmg.com.sg

**Johan Bjork**

**Sweden**

E: johan.bjork@kpmg.se

**Hakan Aytekin**

**Turkey**

E: hakanaytekin@Kpmg.com

**Doron M Rotman**

**USA - West**

E: drotman@kpmg.com

**Kelly Henney**

**Australia**

E: khenney@kpmg.com.au

**Leandro Augusto M Antonio**

**Brazil**

E: lantonio@kpmg.com.br

**Henry Shek**

**China**

E: henry.shek@kpmg.com

**Mikko Viemerö**

**Finland**

E: mikko.viemero@kpmg.fi

**Handy**

**Indonesia**

E: Handy@kpmg.co.id

**Hiromi Iwashita**

**Japan**

E: hiromi.iwashita@jp.kpmg.com

**Rommel Garcia**

**Mexico**

E: rommelgarcia@kpmg.com.mx

**Arne Helme**

**Norway**

E: Arne.Helme@kpmg.no

**Krzysztof Radziwon**

**Poland**

E: kradziwon@kpmg.pl

**Peter Borak**

**Slovak Republic**

E: pborak@kpmg.sk

**Matthias Bossardt**

**Switzerland**

E: mbossardt@kpmg.com

**Mark Thompson**

**United Kingdom**

E: mark.thompson@kpmg.co.uk

**David Remick**

**USA - East**

E: jremick@kpmg.com

**Andreas Tomek**

**Austria**

E: atomek@kpmg.at

**Dominic Jaar**

**Canada**

E: djaar@kpmg.ca

**Gloria P Arenas**

**Colombia**

E: gloriaarenas@Kpmg.Com

**Vincent Maret**

**France**

E: vmaret@kpmg.fr

**Michael Daughton**

**Ireland**

E: michael.daughton@kpmg.ie

**Min Soo Kim**

**Korea**

E: mkim9@kr.kpmg.com

**Koos Wolters**

**Netherlands**

E: wolters.koos@kpmg.nl

**Glenn Tjon**

**Panama**

E: gtjon@kpmg.com

**Mihai Gabriel Tanase**

**Romania**

E: mtanase@kpmg.com

**Michelle Snyders**

**South Africa**

E: michelle.snyders@kpmg.co.za

**Jason Y.T. Hsieh**

**Taiwan**

E: jasonhsieh@kpmg.com.tw

**Raman Bharadwaj**

**United Arab Emirates**

E: rbhardwaj@kpmg.com

**Roman Yanez**

**Venezuela**

E: ryanez@kpmg.com

**Benny Bogaerts**

**Belgium**

E: bbogaerts@kpmg.com

**Micho Schumann**

**Cayman Islands**

E: michoschumann@kpmg.ky

**Jan Krob**

**Czech Republic**

E: jkrob@kpmg.cz

**Michael Falk**

**Germany**

E: mfalk@kpmg.com

**Ishai Wertheimer**

**Israel**

E: iwertheimer@kpmg.com

**Michael Hofmann**

**Luxembourg**

E: michael.hofmann@kpmg.lu

**Souella Cumming**

**New Zealand**

E: smcumming@kpmg.co.nz

**Rosario Caldeiron**

**Peru**

E: rccalderon@kpmg.com

**Andrey Lepekhin**

**Russia**

E: ALepekhin@kpmg.ru

**Javier Aznar Garcia**

**Spain**

E: jaznar@kpmg.es

**Peneppa Pookarat**

**Thailand**

E: pennapa@kpmg.co.th

**Rodrigo Ribeiro**

**Uruguay**

E: rribeiro@kpmg.com

**Will Nguyen**

**Vietnam and Cambodia**

E: williamnguyen@kpmg.com.vn



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

