

GDPR Impacts

SEV GDPR Workshop – Athens

Giles Watkins, UK Country Leader

Wednesday 7th February, 2018



500+ corporate members



27,000+ members in
90+ countries



8 annual events worldwide



20% average growth
in the last **3** years



14,000 certified pros

Agenda

- What is the ‘Privacy Opportunity’?
- What is different under GDPR?
- Where organisations are focusing?
- What can you do in the next 100 days?



WHAT IS THE ‘PRIVACY OPPORTUNITY’?

The Data Economy 2.0.....

- Businesses and society are experiencing benefits from massive data generation
- Easy access to personal information results in new customer insights and business growth opportunities
- Companies must balance these benefits against potential privacy risks



The size of the opportunity

- CISCO - 'Internet of Everything' represents \$19Trillion opportunity
 - \$14 Trillion in Privacy sector
 - \$5Trillion in the Public sector
- General Electric - IoT investment to exceed \$60 Trillion
- IHS - 75 Billion connected devices by 2025
- LSE - Economic benefit of personal data over € 1 Trillion by 2020 in Europe alone
- Data driven company valuations have soared.....

But there are risks.....

5 Biggest Data Breaches of 2017

Dunn & Bradstreet - 33.7million unique records

Republican National Committee - 198 million Americans

Verizon - 14 million subscribers

Uber - 57 million rider and driver accounts

Equifax - estimated 143 million customers

- And of all time....

Anthem - 80 million records

FriendFinder network - 413 million records

Aadhar - 1 Billion records

River City Media - 1.37 Billion records

Source: Information Is Beautiful

The impacts can be significant



Financial
Impact



Regulatory
Impact



Reputational
Impact

What are the biggest risks of GDPR non-compliance for your organisation?

Trust/reputation



Ultimately, its about people

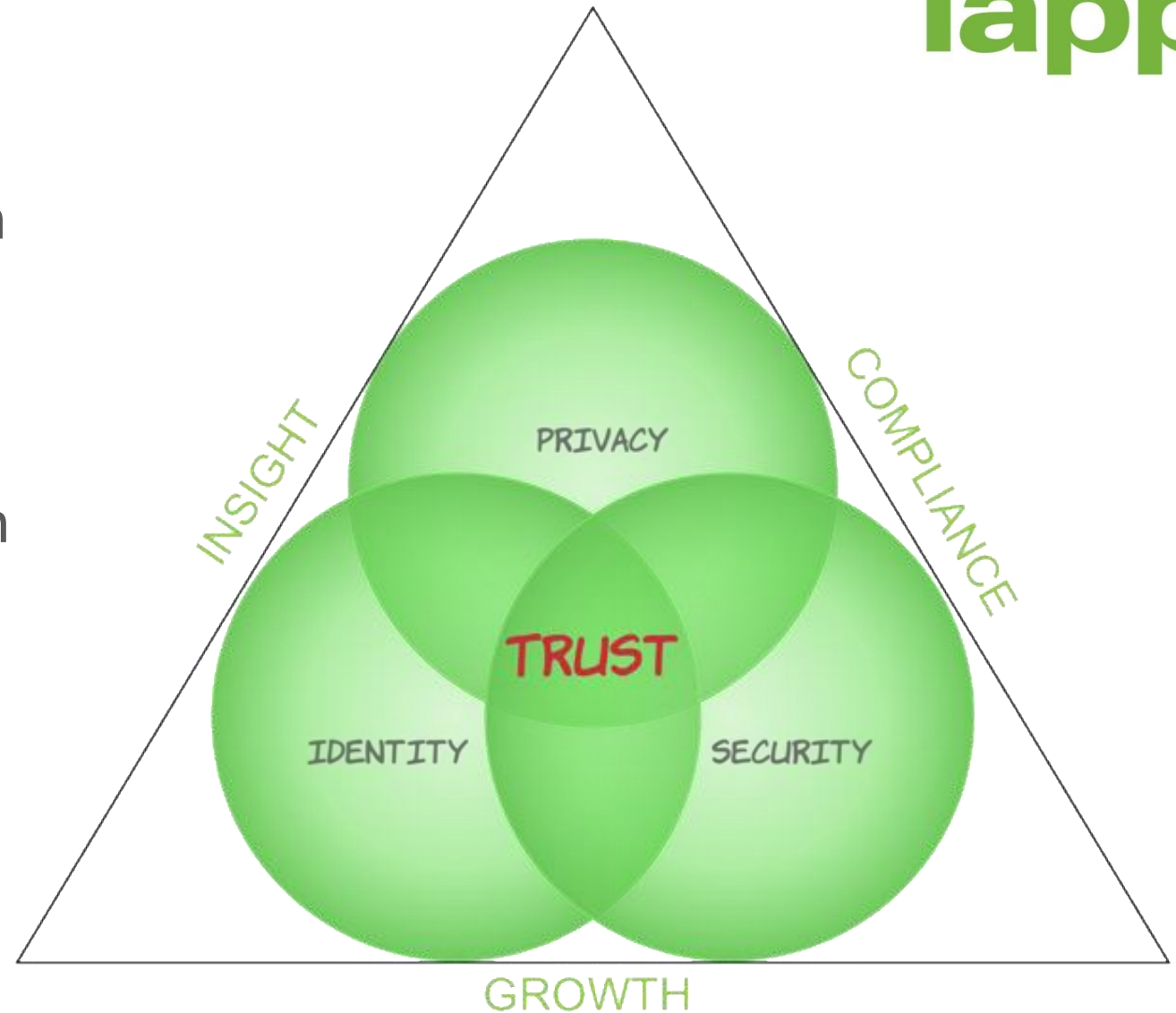


Four types of Privacy ‘harms’

- **Intrusions**
 - “They” come into “your” space and contact you or tell you what to do
- **Information collection**
 - “They” watch what you are doing, more than they should
- **Information processing**
 - “They” have a lot of data, and do things with it
- **Information dissemination**
 - “They” disclose data, perhaps more than “you” think they should

The Digital Trust Payoff

- Businesses need to be confident in the integrity and availability of data and their right to use it
- Citizens will migrate to businesses that work to develop and maintain trust
- Trust (and Brand) are increasingly impacted by core disciplines of Privacy, Security and Identity
- The rise of the Chief Trust Officer..... ?



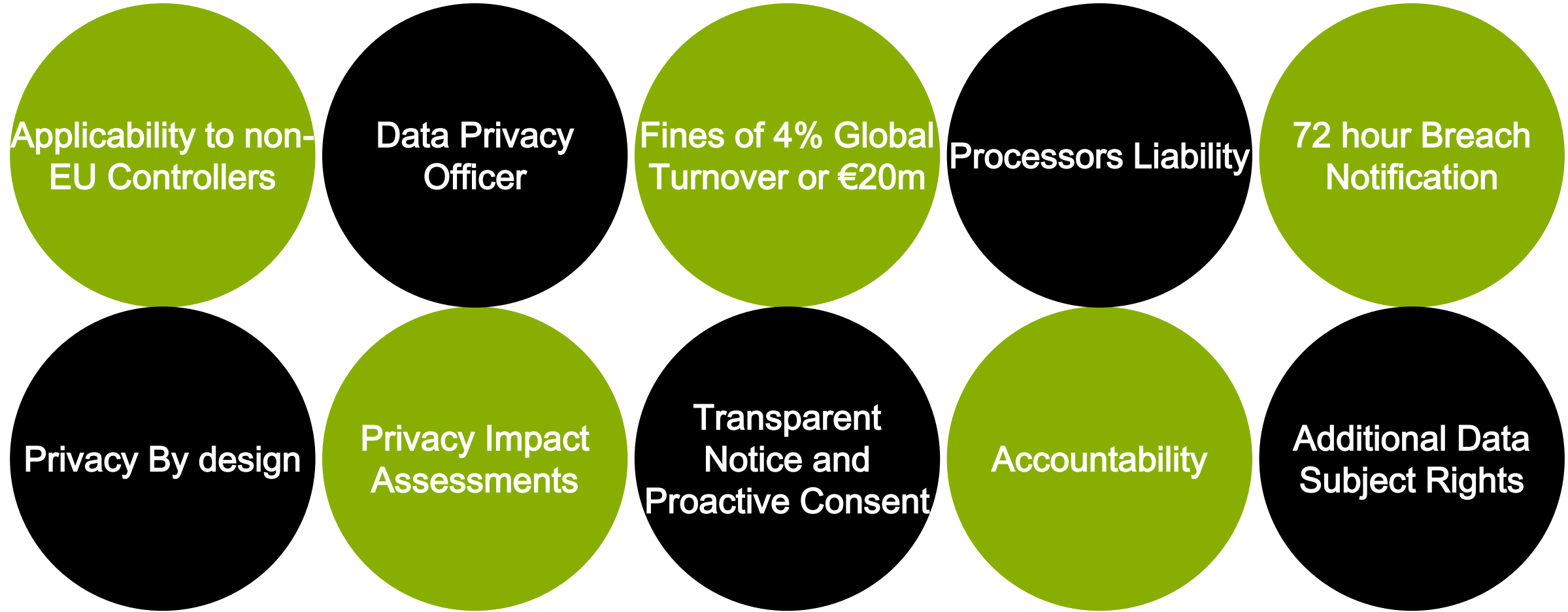
© 2017 Pridium Ltd

www.iapp.org



WHAT IS DIFFERENT UNDER GDPR?

What is different under GDPR



Demonstrating Accountability



Demonstrate compliance by implementing appropriate technical and organisational measures



Implementing measures that meet principles of data protection by design and data protection by default



Maintain relevant documentation



Appoint a data protection officer, if appropriate

Data Protection Officer

Positioning in the company (Art. 38)

- 1) Proper and timely involvement in all relevant aspects to be ensured by the controller
- 2) Support by sufficient resources and access to data and systems and allowance of further qualification
- 3) Independence of instructions and protection against sanctioning by controller as employer
- 4) Point of contact for data subjects
- 5) Professional secrecy and interest protection

Data Protection Officer

Qualifications

Art. 37 (5): ‘The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.’

Data Protection Officer

Number of **DPOs** required under GDPR

28,000 ^{in the} **EU**  **75,000 Globally**

GDPR mandates the appointment of a DPO when core activities involve:

1. Regular and systematic monitoring of data subjects on a large scale, or
2. Processing of special categories of data on a large scale.

When in doubt, appoint a DPO

“The most appropriate certification for the DPO is a combination of the IAPP’s Certified Information Privacy Professional credential for EU professionals (CIPP/E) and Certified Information Privacy Manager (CIPM).”

Oxford University’s *International Data Privacy Law* journal



CIPP/E

EU laws and regulations

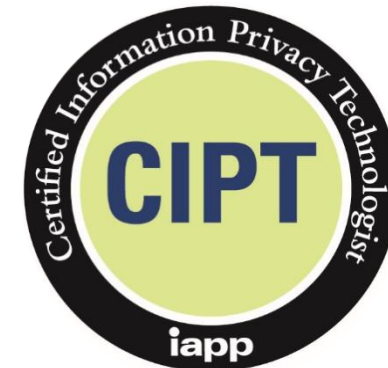
The global standard for the go-to person for privacy laws, regulations and frameworks



CIPM

Operations

The first and only privacy certification for professionals who manage day-to-day operations



CIPT

Technology

The first and only privacy certification for professionals who manage and build privacy requirements and controls in technology



WHAT ARE ORGANISATIONS FOCUSSING ON?

A dark grey rectangular box containing the title of the report in white, bold, sans-serif text.

**IAPP-EY Annual Privacy
Governance Report 2017**

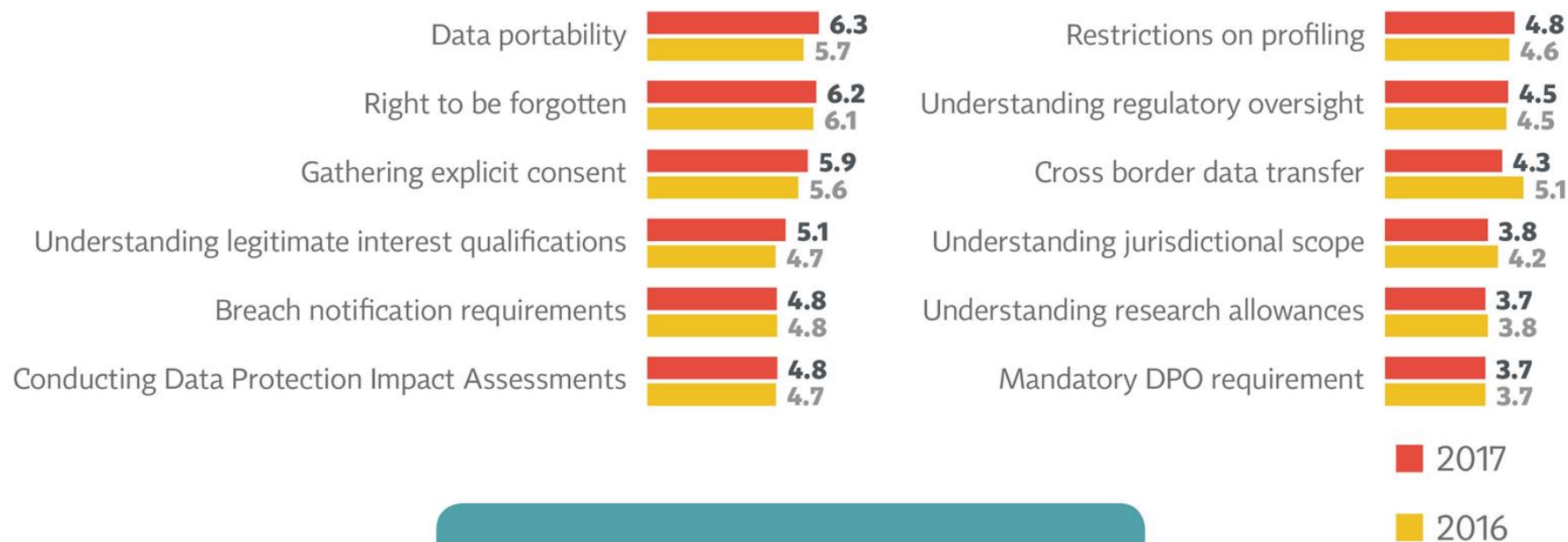


Nearly all firms say they fall under the scope of GDPR

- In addition, two of the top three perceived GDPR difficulties are now seen as even more difficult: data portability and gathering explicit consent

GDPR Obligation Difficulty

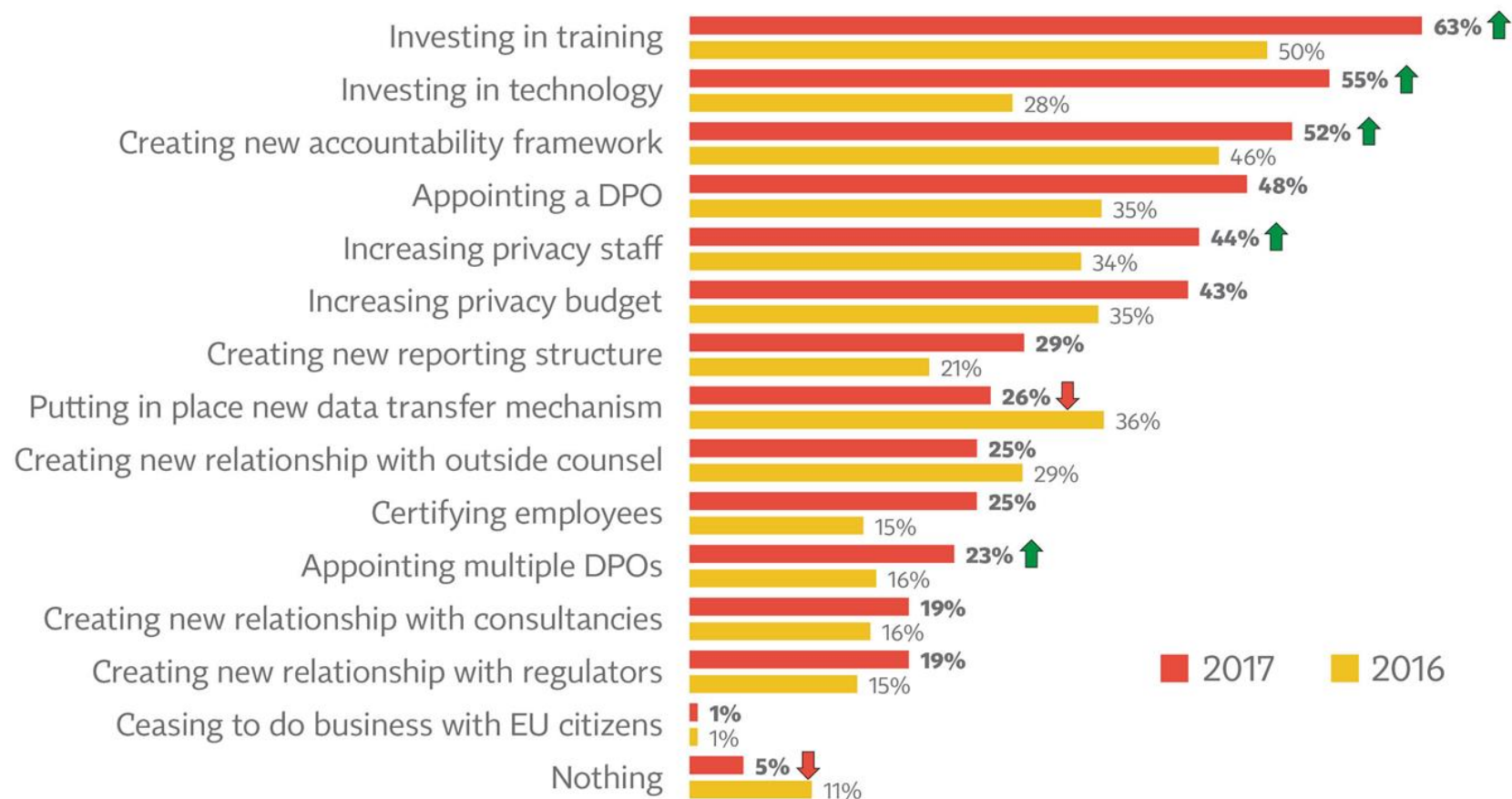
(Mean Score on 0-10 Scale: 0=Not at All Difficult; 10=Extremely Difficult)



Over **95%** of firms say they fall under the GDPR scope

2017 sees large increases in most of the steps firms say they're taking to prepare for GDPR

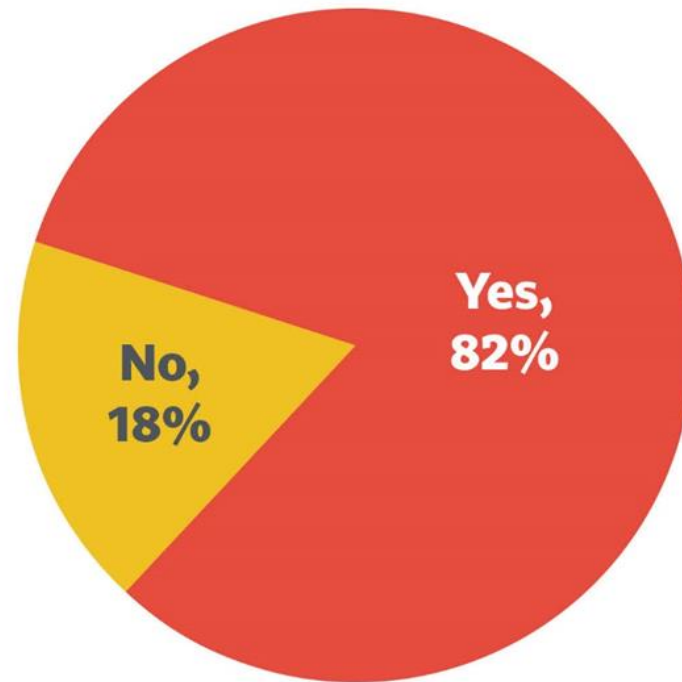
Steps Being Taken to Prep for GDPR (Base: Falls Under GDPR)



↑ ↓ Significantly different from 2016

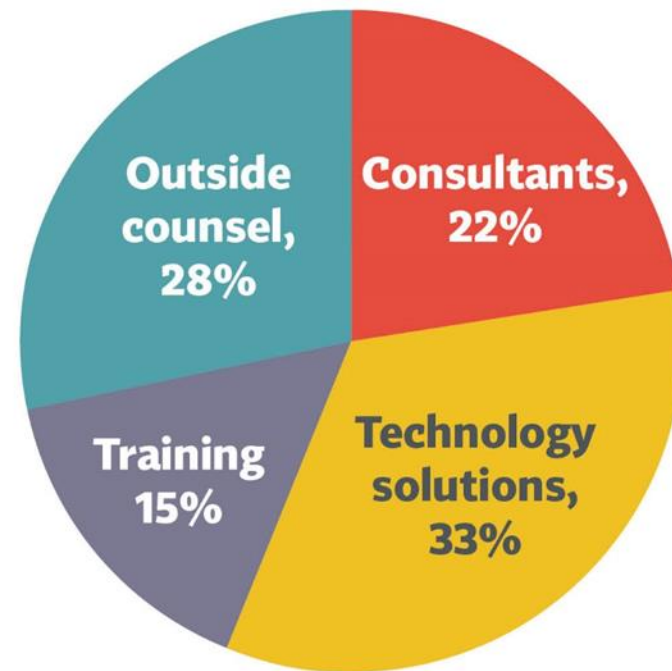
More than 8 in 10 firms falling under the scope of GDPR say they'll need to adapt products to comply

Expect To Adapt Products and Services (Base: Falls Under GDPR)




Among those who will spend more for GDPR, the lion's share will be for tech solutions and outside counsel

Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)




Sources of information



The Top 10 Operational Impacts of the EU's General Data Protection Regulation

Talk to us.
logicaloperations.com
1-800-456-4677



iapp.org
IAPP - International Association of Privacy Professionals



2017 Privacy Tech Vendor Report
v. 1.1



**WHAT CAN YOU DO IN THE
NEXT 100 DAYS?**

www.iapp.org

GDPR COMPLIANCE PROGRAMS – COMMON FOCUS AREAS



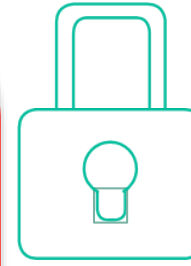
DATA INVENTORY



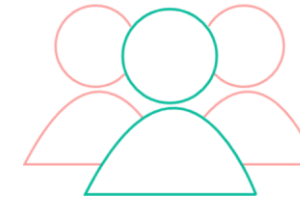
DATA MAPPING



DPIA (DATA PRIVACY IMPACT ASSESSMENT)



SECURITY



BREACH NOTIFICATION



INTERNATIONAL TRANSFERS

100-Day Focus Areas



CONSENT MECHANISM



DATA PROTECTION OFFICER



TRAINING AND AWARENESS



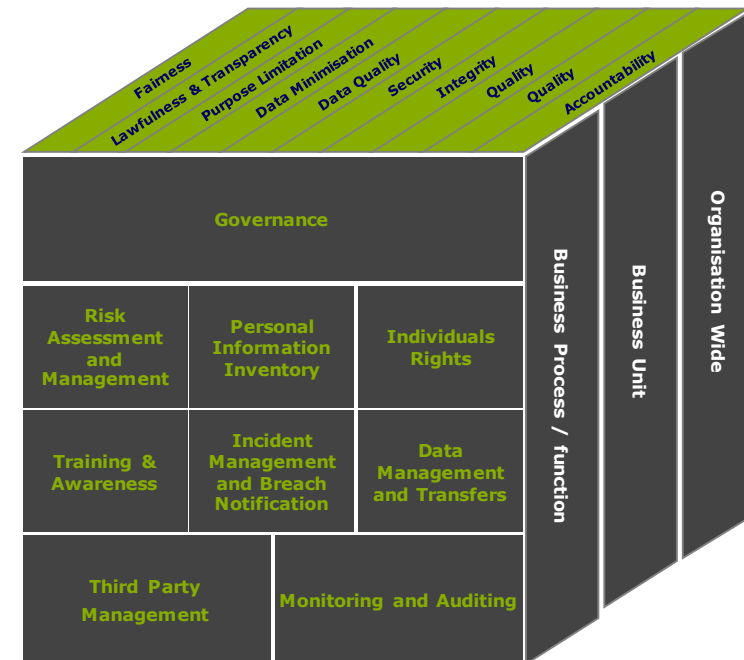
CONTRACT REVIEWS



CITIZENS RIGHTS PROCESSES

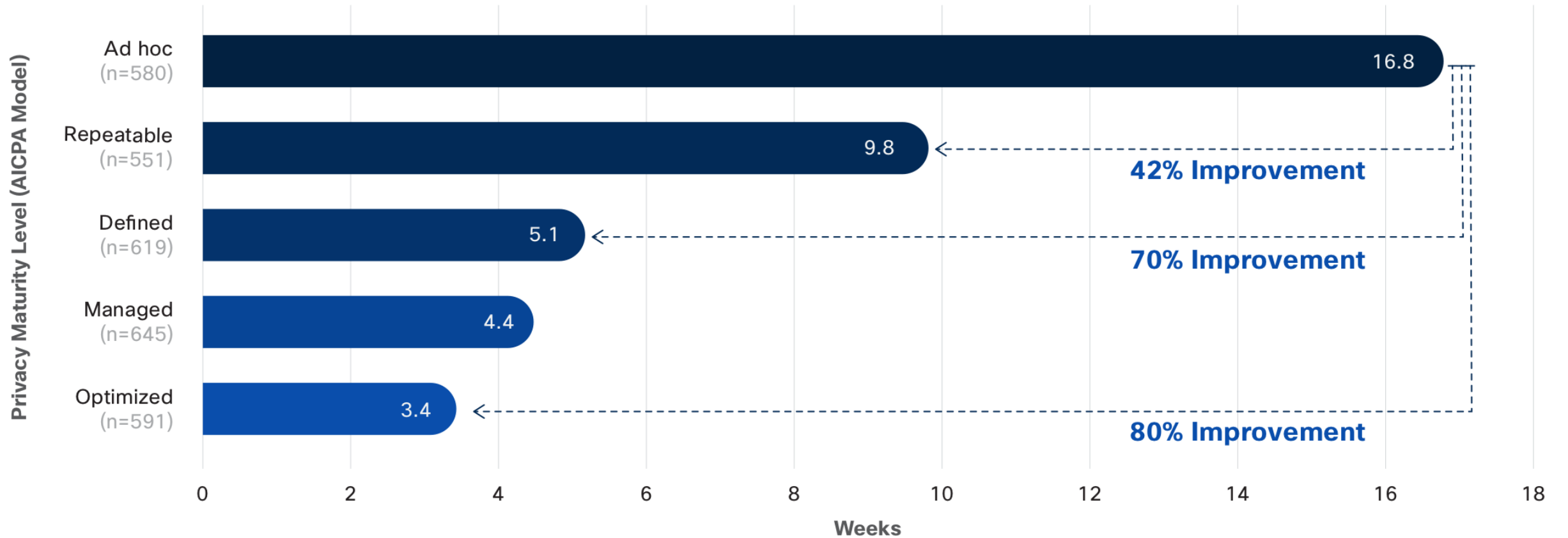
Privacy Management Framework

- Single approach to managing privacy within an organisation
- Achieve consistency of approach and understanding across business functions and geographies
- Facilitates risk analysis
- Allows processes to be defined and maturity levels assessed and managed



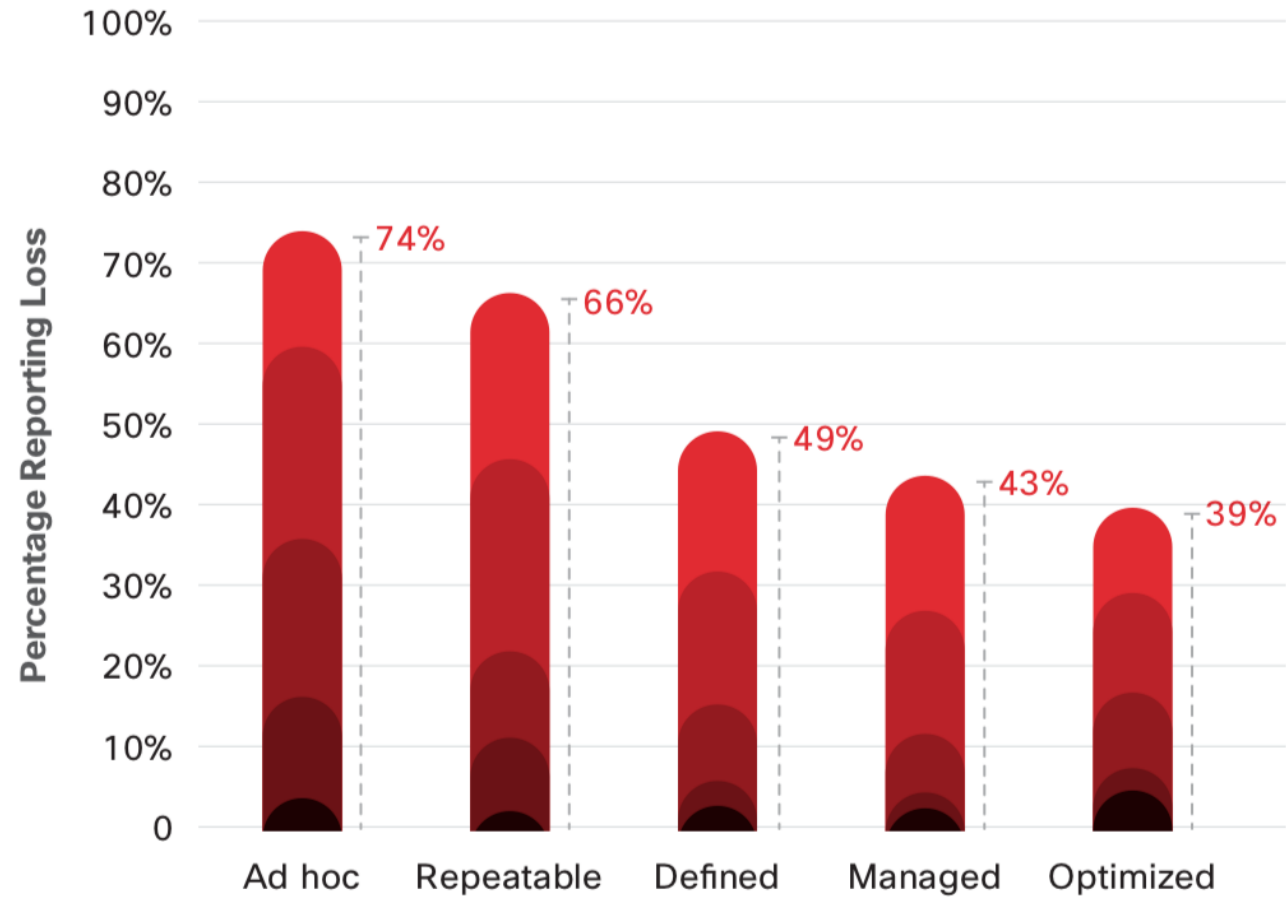
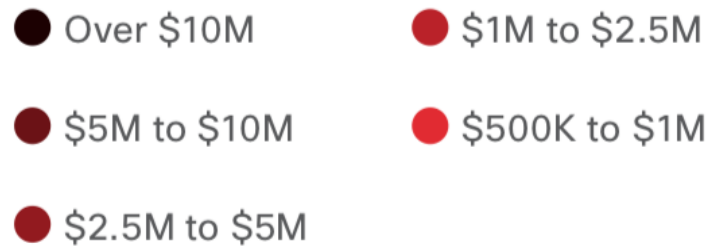
Pridium Privacy Management Framework

Privacy impact on sales



Source: Cisco 2018 Privacy Maturity Benchmark Study

Privacy maturity impact on costs of data breaches

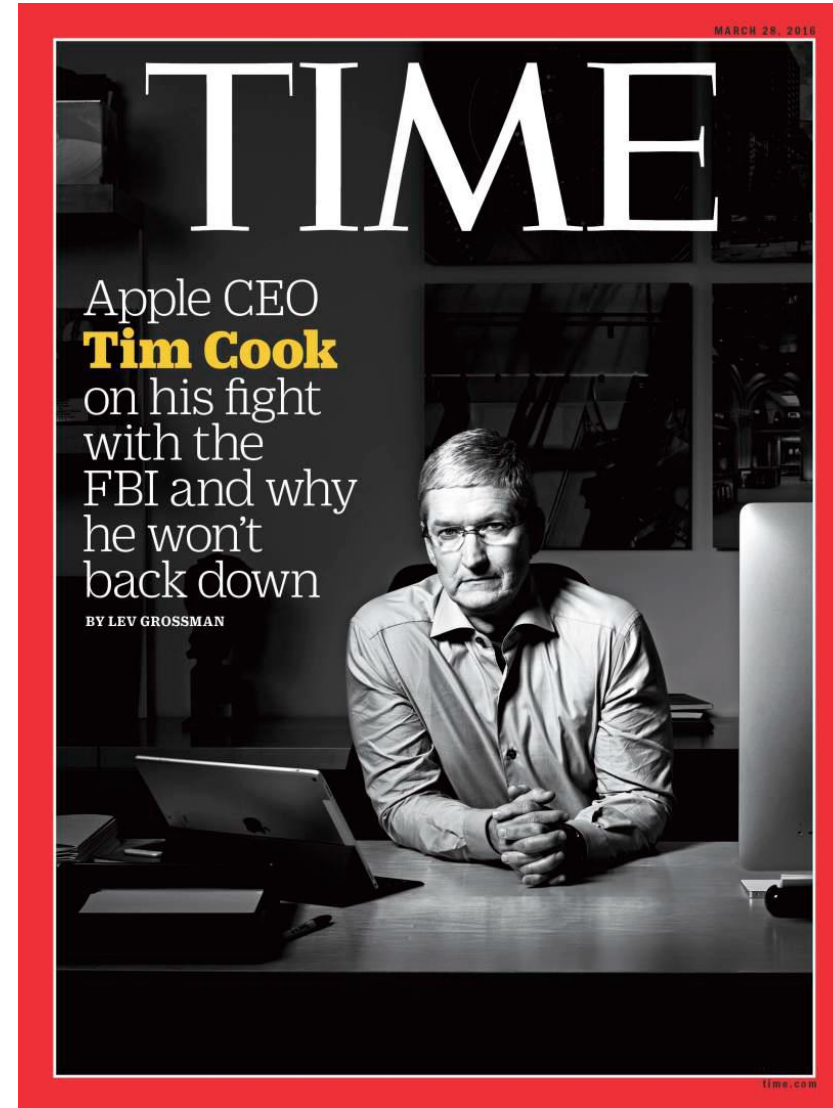


Who would you rather be?

Target CEO steps down after data breach rocks retailer

REUTERS 5th May 2014 12:03 PM

(Reuters) - Target Corp removed Chief Executive Gregg Steinhafel on Monday in the wake of a devastating data breach that hurt the No. 3 U.S. retailer's profits, shook customer confidence in the company and prompted congressional hearings.



**For questions or to request
additional information:**

Giles Watkins

UK Country Leader, IAPP

gwatkins@iapp.org

+44 (0) 7500 072 785

www.iapp.org