GDPR Readiness: Role of the DPO

EDAA Summit 2017 – London

Paul Jordan

Tuesday 28 November, 2017

Overview

- General DPO requirements under the GDPR: legitimacy of the DPO role

- International Research findings in Data Protection

Data Protection Officer

iapp

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

Data Protection Officers
Art. 37–39

Data Protection Officers (Art. 37–39) are to ensure compliance within organisations. They have to be appointed for all public authorities and for companies where the "core activities":

- **regularly and systematically monitor** data subjects on a large scale, or

- **process on a large scale** special categories of data (Art. 9 and 10).

What does 'core activities' and 'large scale' mean?

- **Core Activities:** Key operations necessary to achieve business goals + processing which forms an inextricable part of the business activity.

- **Large Scale:** Recital 91 mentions "processing operations which aim to process considerable amounts of personal data at national, regional or supranational level which could affect a large number of data subjects and which are likely to result in a high risk".

DPD

SECTION IX NOTIFICATION
Article 18 Obligation to notify the supervisory authority

1. **(…)**
2. **Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:**
   - **(…)**
   - **Where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:**
     - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
     - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

Article 20 Prior checking
1. **(…)**
2. **Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.**

GDPR

SECTION 4 DATA PROTECTION OFFICER
Article 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
   a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

   b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

   c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Data Protection Officers

Nature and challenges

- The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. **The skill set required stretches beyond understanding legal compliance with data protection laws and regulations**.
- Monitoring of DPOs will be the responsibility of the Regulator rather than the Board of Directors of the organisation that employs the DPO: **the independence factor**.
- Internally, the DPO will need to create their own support team and will also be responsible for their own continuing professional development as they need to be relatively independent of the organisation that employs them, effectively acting as a '**business enabler**' within organisations.

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Data Protection Officer

The Data Protection Officer (DPO) role is an important GDPR innovation and a cornerstone of the GDPR's accountability-based compliance framework. In addition to supporting an organisation's compliance with the GDPR, DPOs will have an essential role in acting as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

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.'*

- Certifications: **CIPP/E** (EU data protection legislation), **CIPM** (data protection practices, [D]PIAs, Program mgt)
- Further qualifications & continuous education

"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

Data Protection Officer

Responsibilities (Art. 39)

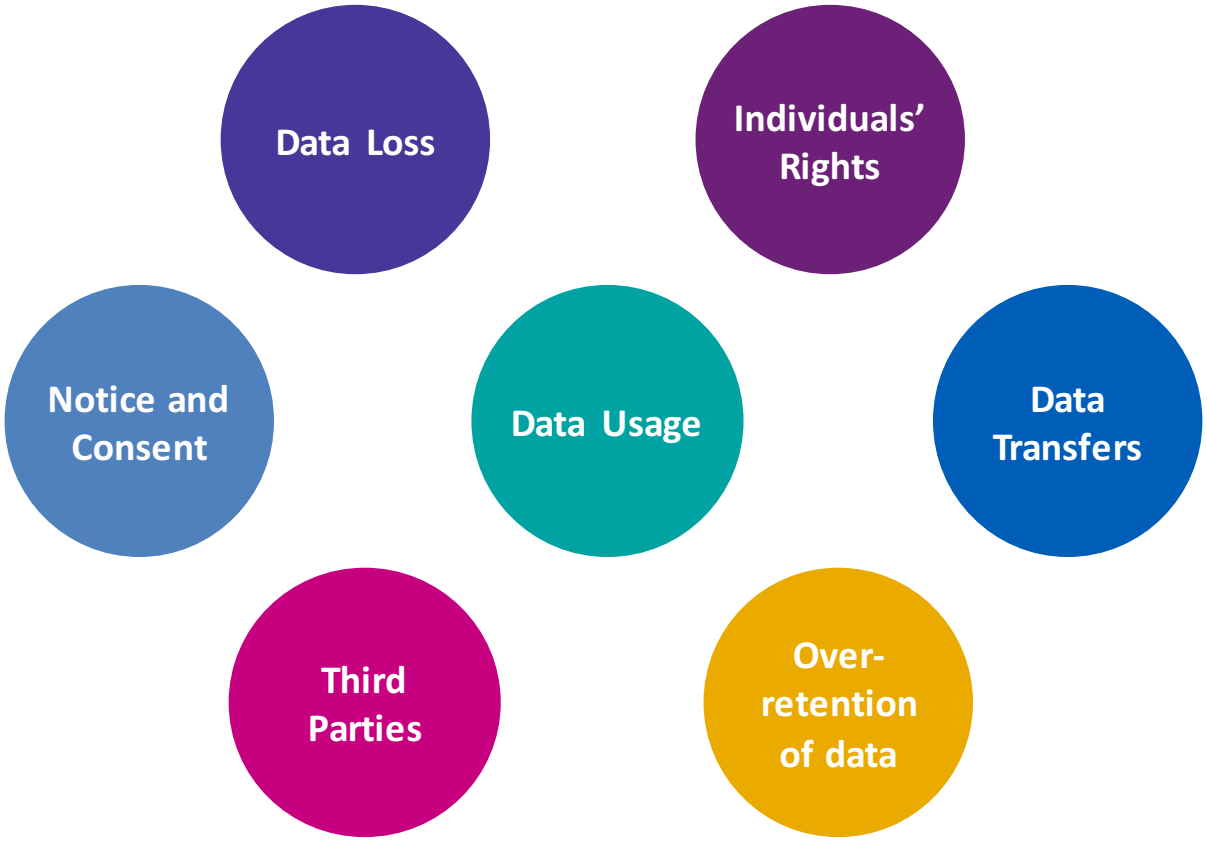
- **Counsel** the entity in regard to applicable data protection laws
- **Monitor** compliance with applicable data protection (GDPR) provisions and alignment with internal policies, including the assignment of responsibilities,
- **Awareness-raising** and **training** of staff involved in the processing operations
- Conduction of data protection **audits** and [D]PIAs
- **Cooperate and communicate** with the responsible regulatory authority

Data Protection Officer

Data Protection Risk Management

(**Art. 39 (2)**): *'The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.'*

Privacy Risks



Key Risk Impacts

Financial Impact

Regulatory Impact

Reputational Impact

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

Accountability & GDPR

Accountability is a Key Principle

The new accountability principle in Article 5(2) requires the controller to demonstrate compliance with the principles relating to personal data and states explicitly that this is the controllers responsibility

Demonstrating Accountability

Demonstrate compliance by implementing appropriate technical and organisational measures

Maintain relevant documentation

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

Appoint a data protection officer, if appropriate

Outsourcing the DPO?

Shared and external DPOs

(Art. 37 (2)): 'A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.'

(Art. 37 (6)): 'The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.'

CPO vs. DPO

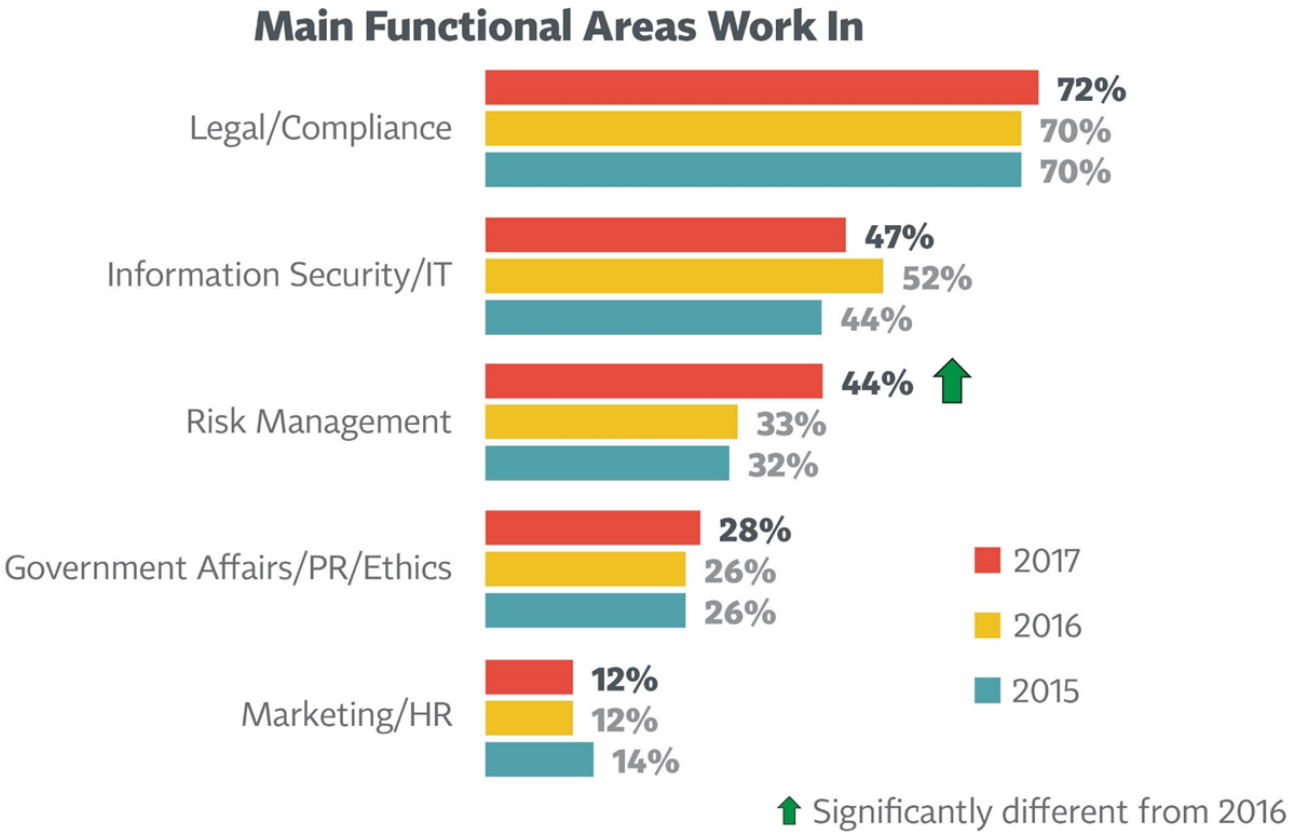
Considerations

- Is this mandatory DPO the lead data protection and privacy voice in the organisation?
- Does the DPO's role in working with the regulator make it difficult for the DPO to engage in high-level strategic conversations?
- Would appointing external counsel as DPO create conflict when working with the lead privacy voice in the organisation?
- Remember Art. 38 (3): *'The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks.'*


iapp
IAPP-EY Annual Privacy Governance Report 2017
iapp
EY

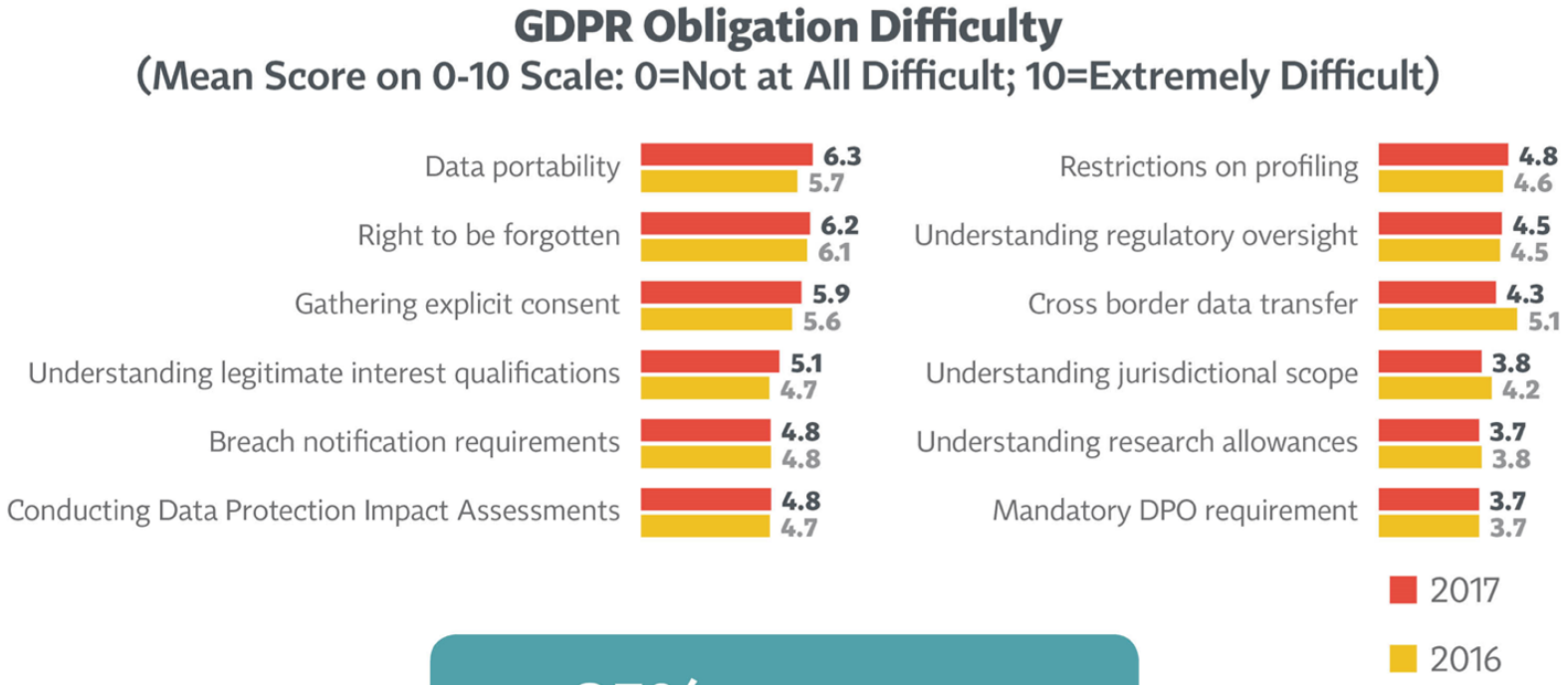
2017 sees an 11-point increase in the percent working in a risk-management function

- There's also been a directional increase for legal/compliance, the most common functional area by far



Nearly all firms say they fall under the scope of GDPR

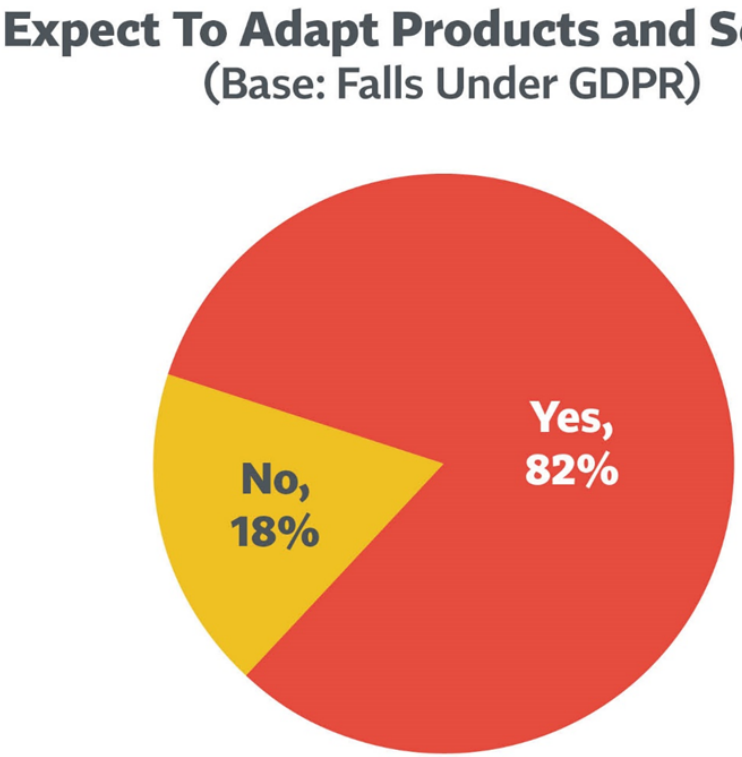
- In addition, two of the top three perceived GDPR difficulties are now seen as even more difficult: data portability and gathering explicit consent



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

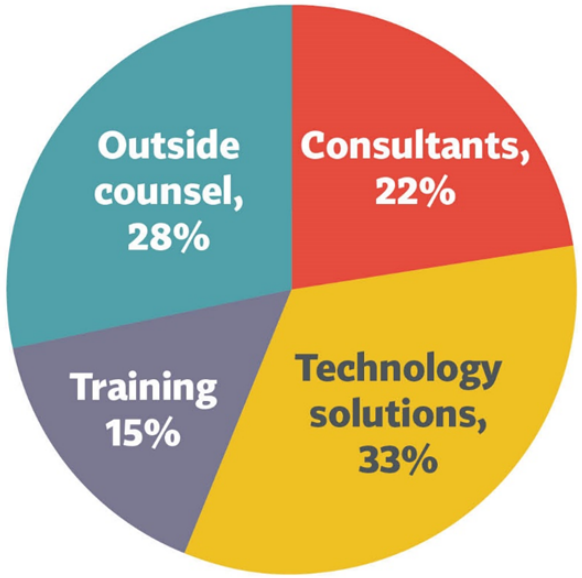
2017 sees large increases in most of the steps firms say they're taking to prepare for GDPR

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

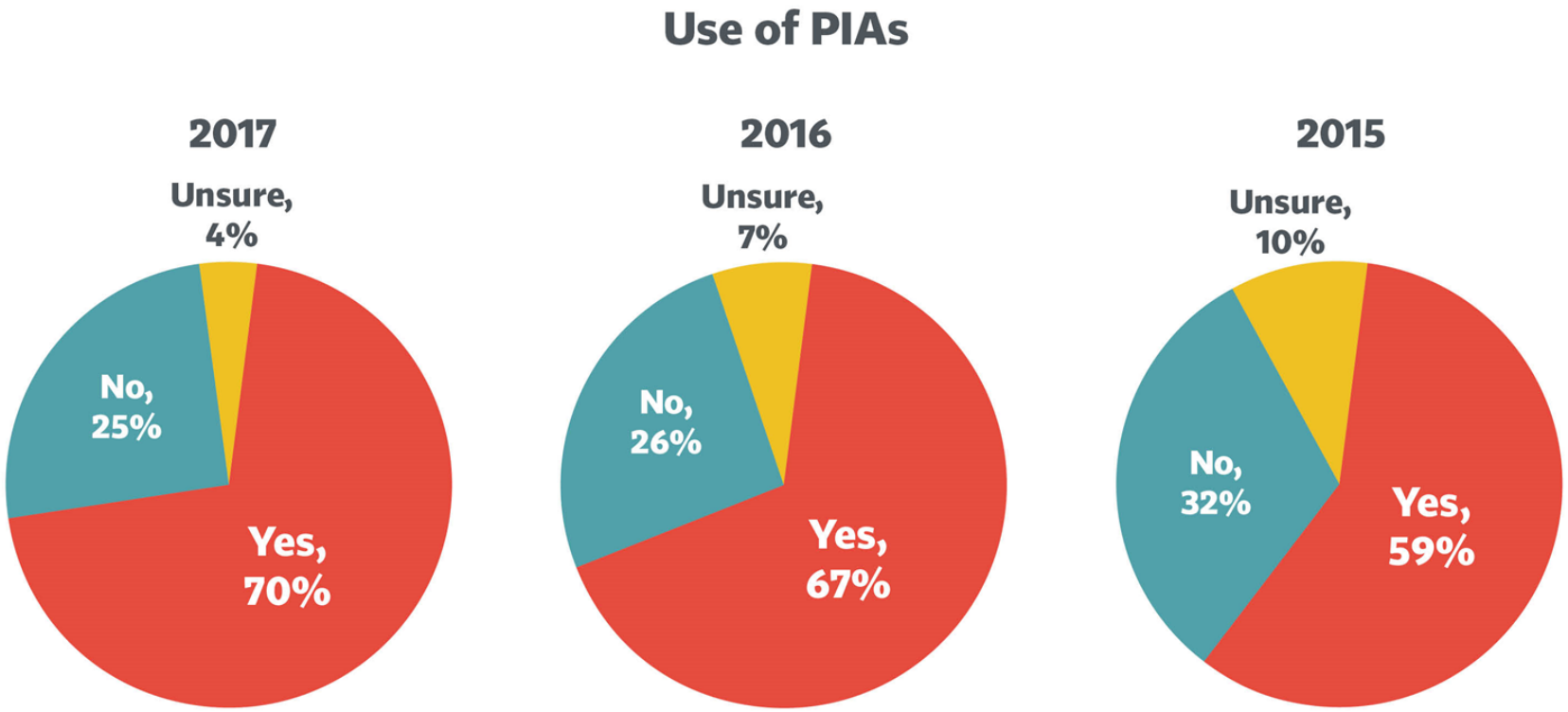


Among those who will spend more for GDPR, the lion's share will be for tech solutions and outside counsel

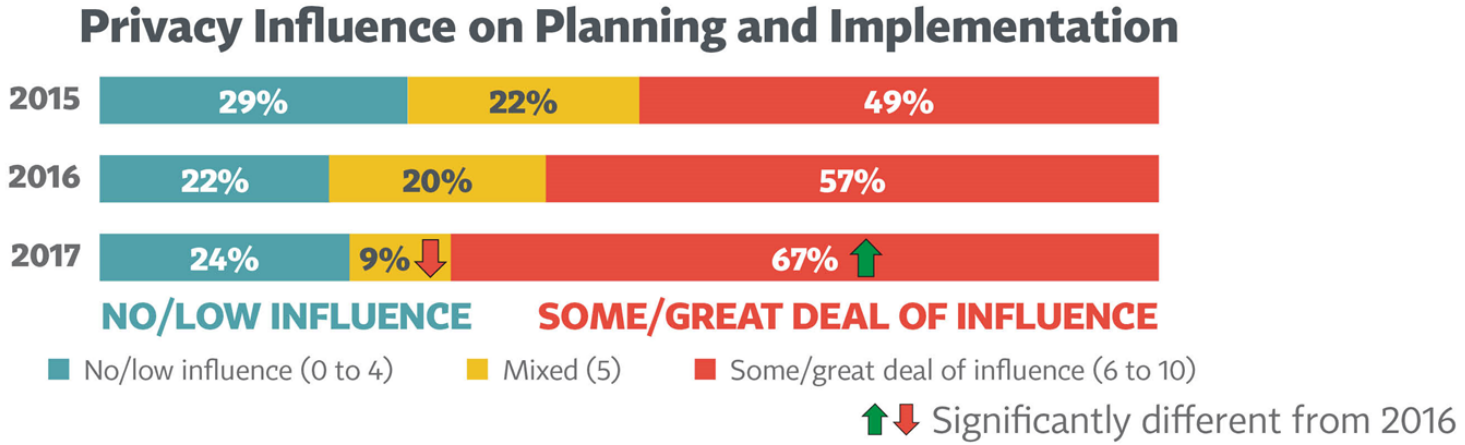
Distribution of Additional GDPR Compliance Budget
(Base: Falls Under GDPR, Will Spend More)

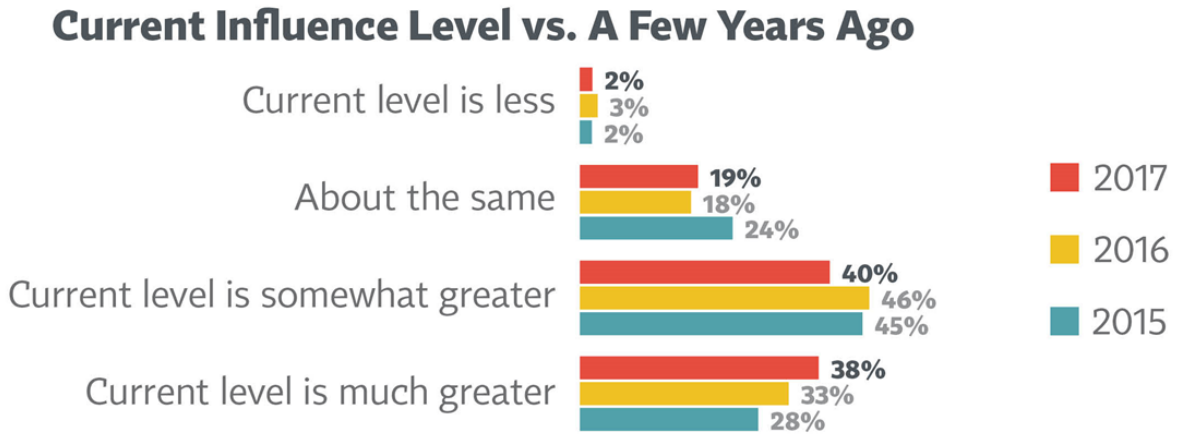


Use of Privacy Impact Assessments is up directionally from 2016, to 70% of respondents



After an 8-point jump, the percent saying privacy has influence on initiative planning is up another 10 points





For questions or to request additional information:

Paul Jordan
Managing Director, Europe, IAPP
pjordan@iapp.org
+32.(0)2.761.66.86
www.iapp.org