

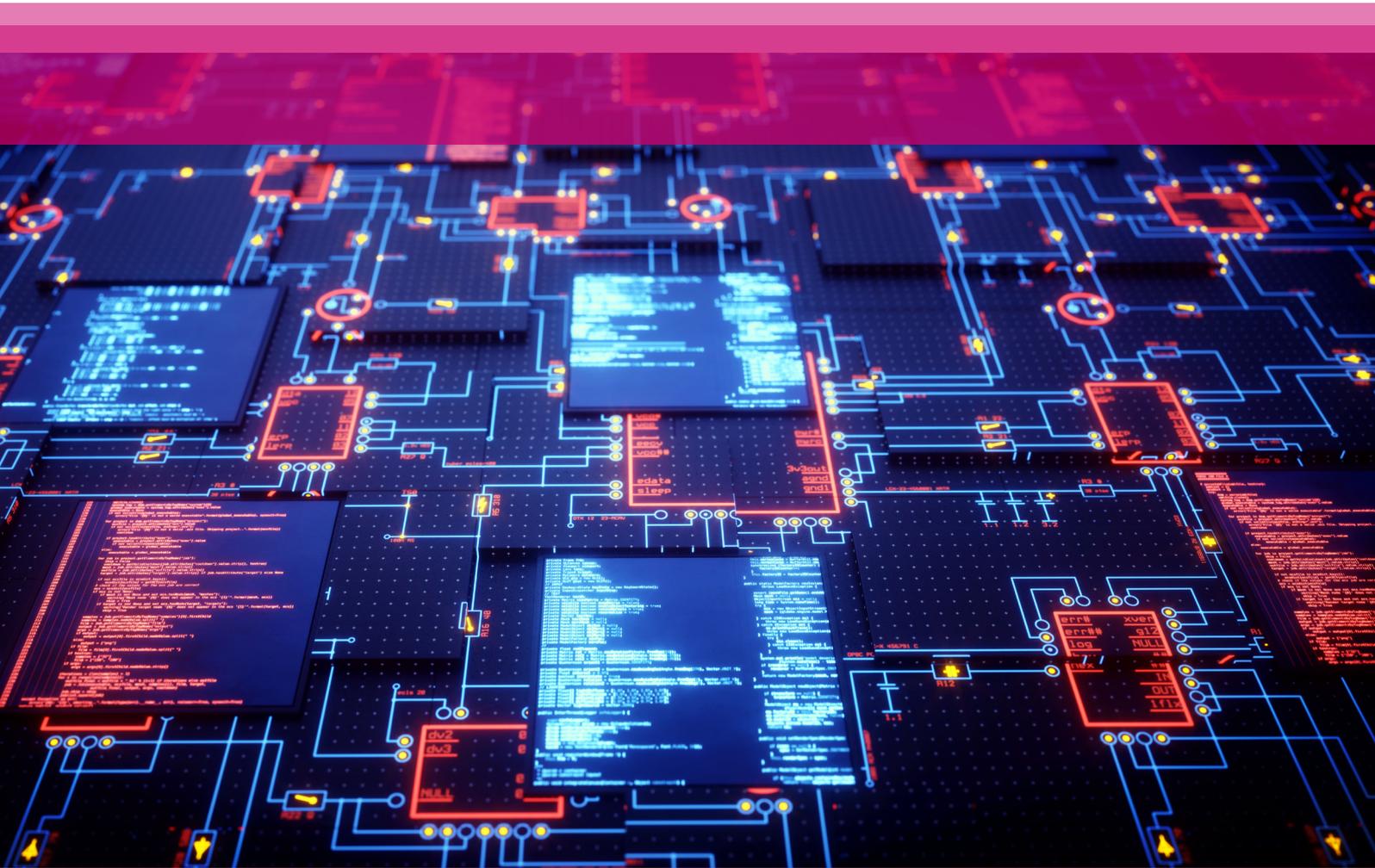
GENERAL DATA PROTECTION REGULATION

A SURVEY OF THE READINESS OF IRISH BUSINESS
TOWARDS GDPR IMPLEMENTATION – PART II

November 2017



McCANN FITZGERALD



About Mazars

Mazars is an integrated and independent professional service firm with more than 18,000 professionals and 1,000 partners across 79 countries. Mazars specialises in assurance, tax and advisory services. In Ireland we have 23 partners and more than 400 staff in our offices in Dublin, Galway and Limerick. Our core purpose is to deliver exceptional value to our clients through technical excellence and quality of service.

About McCann FitzGerald

With almost 600 people, including over 350 lawyers and professional staff, McCann FitzGerald is one of Ireland's premier law firms. We are consistently recognised as being the market leader in many practice areas and our pre-eminence is endorsed by clients and market commentators alike.

Our principal office is located in Dublin and we have overseas offices in London, New York and Brussels. We provide a full range of legal services, primarily to commercial, industrial and financial services companies. Our clients include international corporations, major domestic businesses and emerging Irish companies. We also have many clients in the State and semi-State sector.

About the Research

W5 carried out a quantitative online survey of senior figures with responsibility for the compliance and data protection functions in Irish business during August / September 2017. The representative sample comprised a cross section of businesses by size (measured by number of employees) and business sector and industry.

Total sample size : N=56 Fieldwork dates: 22 August - 13 September 2017. We are very grateful to all the survey participants for their valuable time and insights.



INTRODUCTION

General Data Protection Regulation

A Survey of the Readiness of Irish Business – Phase II Findings

Twelve months after McCann FitzGerald and Mazars first conducted research into the readiness of Irish business for implementation of the General Data Protection Regulation (GDPR) we have gone back to assess the current state of preparedness and to see what variances, if any, should be noted and what lessons can be learned.

In summary, we see a much greater awareness of what is required to meet GDPR compliance requirements with 95% saying that meeting the compliance requirements of the GDPR will be challenging to extremely challenging. To address this, 73% of organisations have, at this point, mobilised a project (versus 16% last year) representing a significant increase.

This heightened awareness of the challenges posed by GDPR compliance has led to a stark increase in numbers that think significant changes will be required. By way of example, 75% think that current data protection / privacy notices and methods of consent will require significant changes – 42% increase on last year.

Despite these changes, our advice remains the same: Organisations need, as a matter of urgency, to review their internal procedures and controls in light of the impending changes under the GDPR, and consider what amendments to such procedures will be required, and what other measures should be taken, to ensure that they are GDPR ready.

To do otherwise risks serious penalties including fines of up to 4% of global turnover or €20 million (whichever is greater) in the case of a breach.

Summary Findings

Specifically, of those surveyed:

- **95%** think that meeting the compliance requirements of the GDPR will be challenging to extremely challenging (a rise of 13% since 2016);
- **75%** envisage that current data protection / privacy notices and methods of consent will require significant changes to be compliant with GDPR (42% increase since 2016);

- **73%** of organisations have mobilised a project to meet GDPR compliance requirements (compares to only 16% in 2016);
- **89%** think that complying with requirements regarding international transfers will be challenging to extremely challenging (up 6% since 2016);
- Where a third party data processor is engaged **28%** are not very confident or not at all confident that the data processor is knowledgeable of, capable and committed to implementing their data protection obligations (20% increase since 2016);
- **64%** expect implementing the more explicit 'right to be forgotten' will be very or extremely challenging (9% increase since 2016 with all don't knows disappeared);
- **36%** of organisations do not have a Data Protection Officer ("DPO") (6% increase since 2016);
- Of those organisations that have a DPO **33%** feel that the role isn't sufficiently senior and independent to meet the GDPR requirements (up 11% since 2016);
- **52%** envisage that maintaining an inventory of personal data will be very or extremely challenging (up 9% since 2016);
- **84%** currently have a policy to notify the data subjects in the event of a personal data security breach (15% increase since 2016) and **85%** have a policy to notify the local data protection supervisory authority (up 4% since 2016);
- **44%** expect meeting the breach notification of 72 hours to be very or extremely challenging (the same as last year);
- One continued positive trend is that **82%** of organisations surveyed will have executive or CEO level sponsorship of compliance programmes to meet the requirements (up 4% on 2016).



Liam McKenna
Partner
Consulting Services
Mazars



Paul Lavery
Partner
Head of Technology & Innovation
McCann FitzGerald



RESPONDENTS

FUNCTION OF RESPONDENT



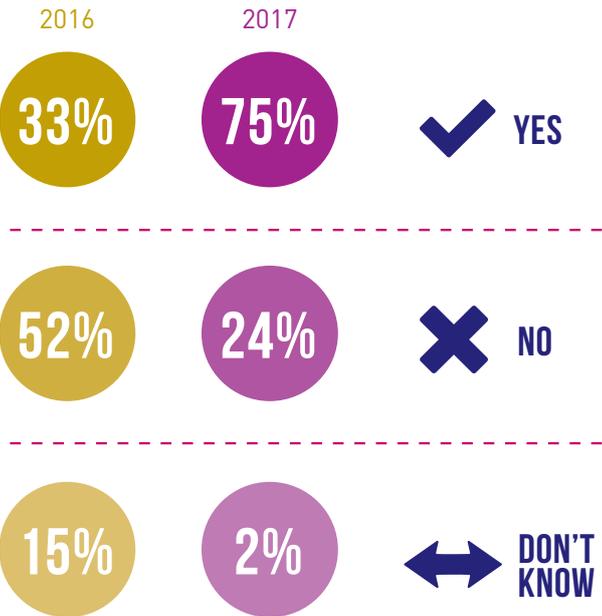


KEY FINDINGS

1. NOTICES & CONSENTS:

The GDPR will require that Data Controllers are able to demonstrate that they have obtained appropriate consent from data subjects to the processing of personal data, where they are relying on consent to legitimise the processing.

DO YOU ENVISAGE THAT YOUR ORGANISATION'S CURRENT DATA PROTECTION/ PRIVACY NOTICES AND METHODS OF CONSENT WILL REQUIRE SIGNIFICANT CHANGES TO BE COMPLIANT WITH THE GDPR?



HOW CHALLENGING WILL IDENTIFYING AND IMPLEMENTING THE NECESSARY CHANGES BE FOR YOUR ORGANISATION?



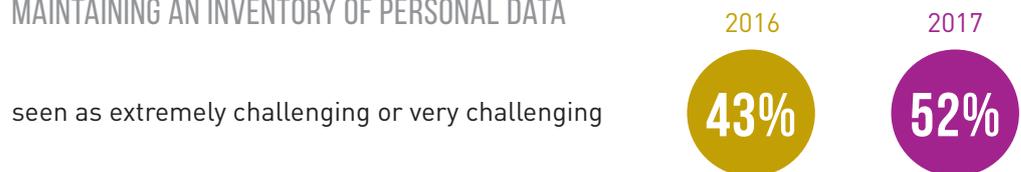


KEY FINDINGS

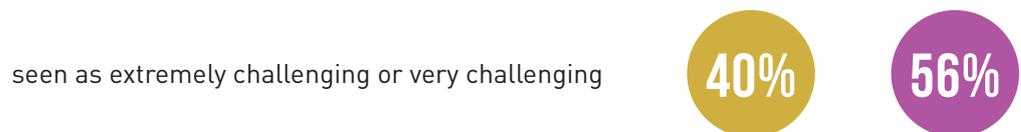
2. COMPLIANCE CHALLENGES:

Data Controllers will need to demonstrate compliance with the GDPR by maintaining an inventory of personal data including its uses and where it is shared.

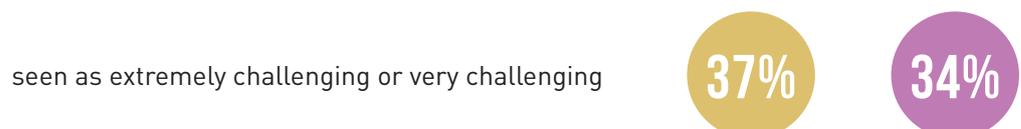
MAINTAINING AN INVENTORY OF PERSONAL DATA



ASSESSING AND DOCUMENTING PRIVACY RISKS



CONSIDERING AND IMPLEMENTING DATA PROTECTION CONTROLS FROM EARLY STAGES IN PROJECTS



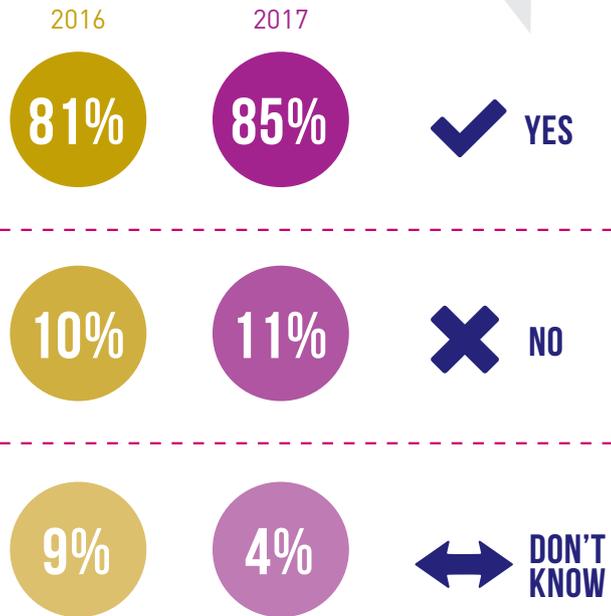


KEY FINDINGS

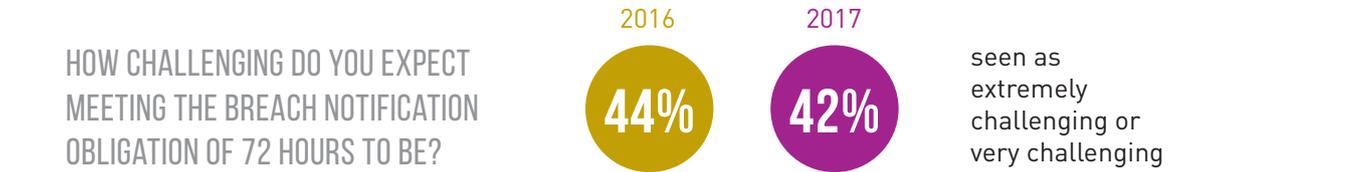
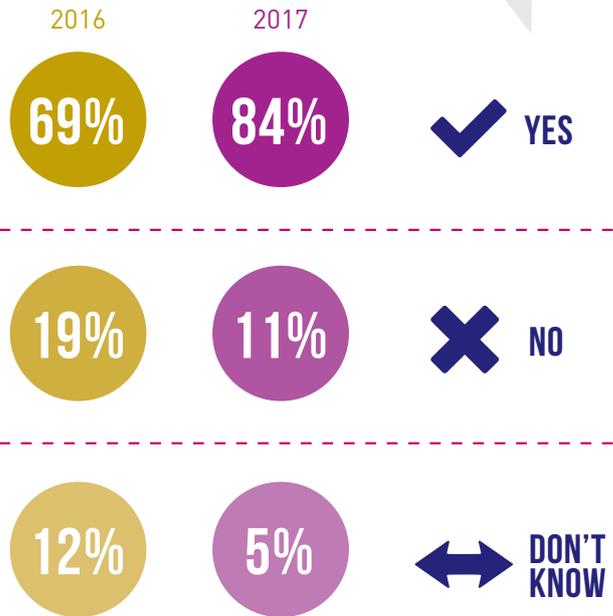
3. BREACH NOTIFICATION:

In the event of a personal data breach, the GDPR requires Data Controllers to notify the local data protection supervisory authority within 72 hours of becoming aware of the breach. Additionally, where there is likely to be a high risk of the rights and freedoms of individuals being impacted, Data Controllers will be required to notify the data subject of the breach.

DO YOU CURRENTLY HAVE A POLICY TO NOTIFY YOUR LOCAL DATA PROTECTION SUPERVISORY AUTHORITY IN THE EVENT OF A PERSONAL DATA SECURITY BREACH?



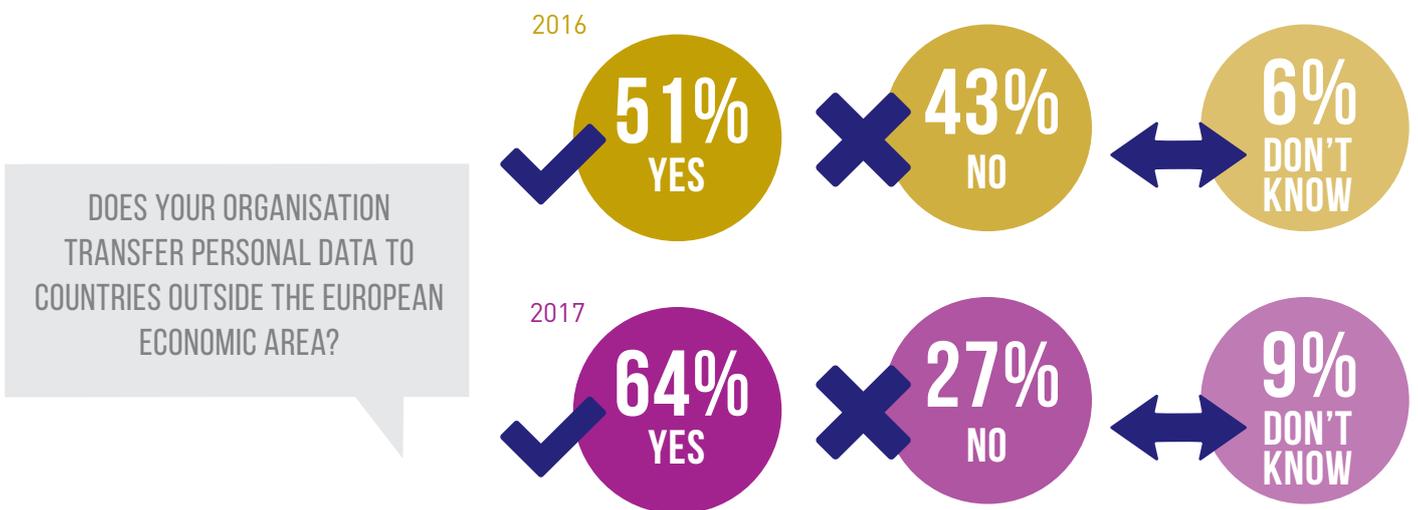
DO YOU CURRENTLY HAVE A POLICY TO NOTIFY THE DATA SUBJECTS IN THE EVENT OF A PERSONAL DATA SECURITY BREACH?





KEY FINDINGS

4. INTERNATIONAL TRANSFERS:



DO YOU THINK COMPLYING WITH REQUIREMENTS REGARDING INTERNATIONAL TRANSFERS WILL BE LESS OR MORE CHALLENGING WHEN THE GDPR COMES FULLY INTO FORCE?

MORE CHALLENGING

DON'T KNOW

LESS CHALLENGING





KEY FINDINGS

4. INTERNATIONAL TRANSFERS CONT:

Under the GDPR (as is currently the case), a transfer of personal data to a third country or an international organisation outside the EEA will be permitted only if the European Commission has decided that the country or international organisation in question ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards.

DOES YOUR ORGANISATION CURRENTLY USE BINDING CORPORATE RULES AS A MEANS TO TRANSFER PERSONAL DATA WITHIN A CORPORATE GROUP STRUCTURE OUTSIDE OF THE EEA?



DOES YOUR ORGANISATION CURRENTLY USE THE STANDARD CONTRACTUAL CLAUSES APPROVED BY THE EUROPEAN COMMISSION AS A MEANS TO TRANSFER PERSONAL DATA OUTSIDE THE EEA?



DOES YOUR ORGANISATION CURRENTLY RELY ON DATA SUBJECT CONSENT AS A MEANS TO TRANSFER PERSONAL DATA OUTSIDE THE EEA?



DOES YOUR ORGANISATION INTEND TO RELY ON THE EU/US PRIVACY SHEILD AS A MEANS TO TRANSFER PERSONAL DATA TO THE UNITED STATES OF AMERICA?





KEY FINDINGS

5. THE ROLE OF DATA PROTECTION OFFICER:



Under the GDPR there will be an obligation on certain categories of data controllers and data processors to appoint a Data Protection Officer (DPO) in order to monitor compliance with the GDPR. DPOs must have expert knowledge in data protection law and practices, and must be independent and report directly to the highest management level within the organisation.

2016

30%

2017

36%

of organisations do not have a DPO

29%

41%

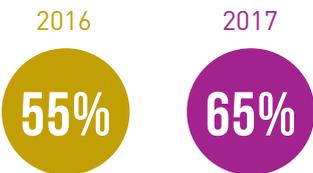
where a DPO exists 41% do not believe their DPO is sufficiently senior to meet the requirements of the GDPR



KEY FINDINGS

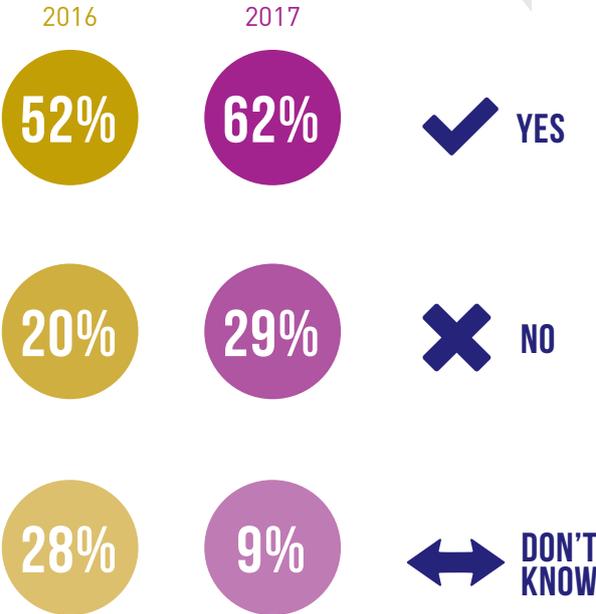
6. DATA SUBJECTS RIGHT TO BE FORGOTTEN AND DATA PORTABILITY:

The GDPR provides for a more explicit 'right to be forgotten' than currently exists under European data protection law.

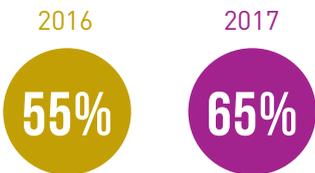


of respondents believe that implementing the more explicit right to be forgotten will be extremely challenging or very challenging.

DO YOU EXPECT THE DATA PORTABILITY RIGHT TO BE APPLICABLE TO YOUR ORGANISATION'S ACTIVITIES AS A DATA CONTROLLER?



The GDPR provides for a new right for data subjects to receive personal data they provided to the data controller in a structured, commonly used and machine-readable format and to transmit it to another data controller in certain circumstances.



of respondents expect that facilitating the data portability right will be extremely challenging or very challenging for their organisation



KEY FINDINGS

7. OUTSOURCED DATA PROCESSORS:



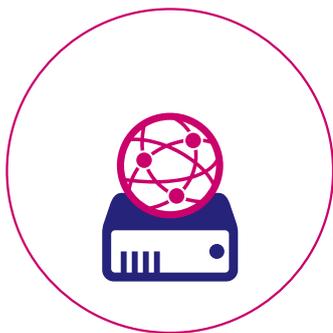
2016

91%

2017

96%

of respondents engage third party data processors for data processing activities (i.e. storage, processing, transmission etc.)



2016

46%

2017

54%

of respondents indicated that their third party data processors are located both within the EEA and outside the EEA.



2016

84%

2017

65%

of respondents indicated that they are very or fairly confident that their data processors are knowledgeable of, capable and committed to implementing their data protection obligations



KEY FINDINGS

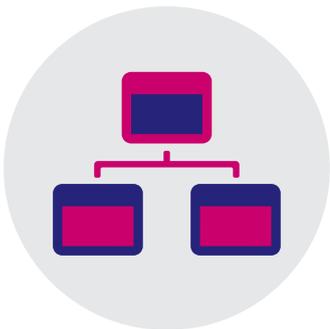
8. APPROACH TO COMPLIANCE DEADLINE:



73% of organisations have now mobilised a project to meet GDPR compliance requirements, versus only 16% last year.



39% of organisations think that maintaining an adequate and complete inventory of personal data will be the most challenging aspect of GDPR, which is the same as last year.



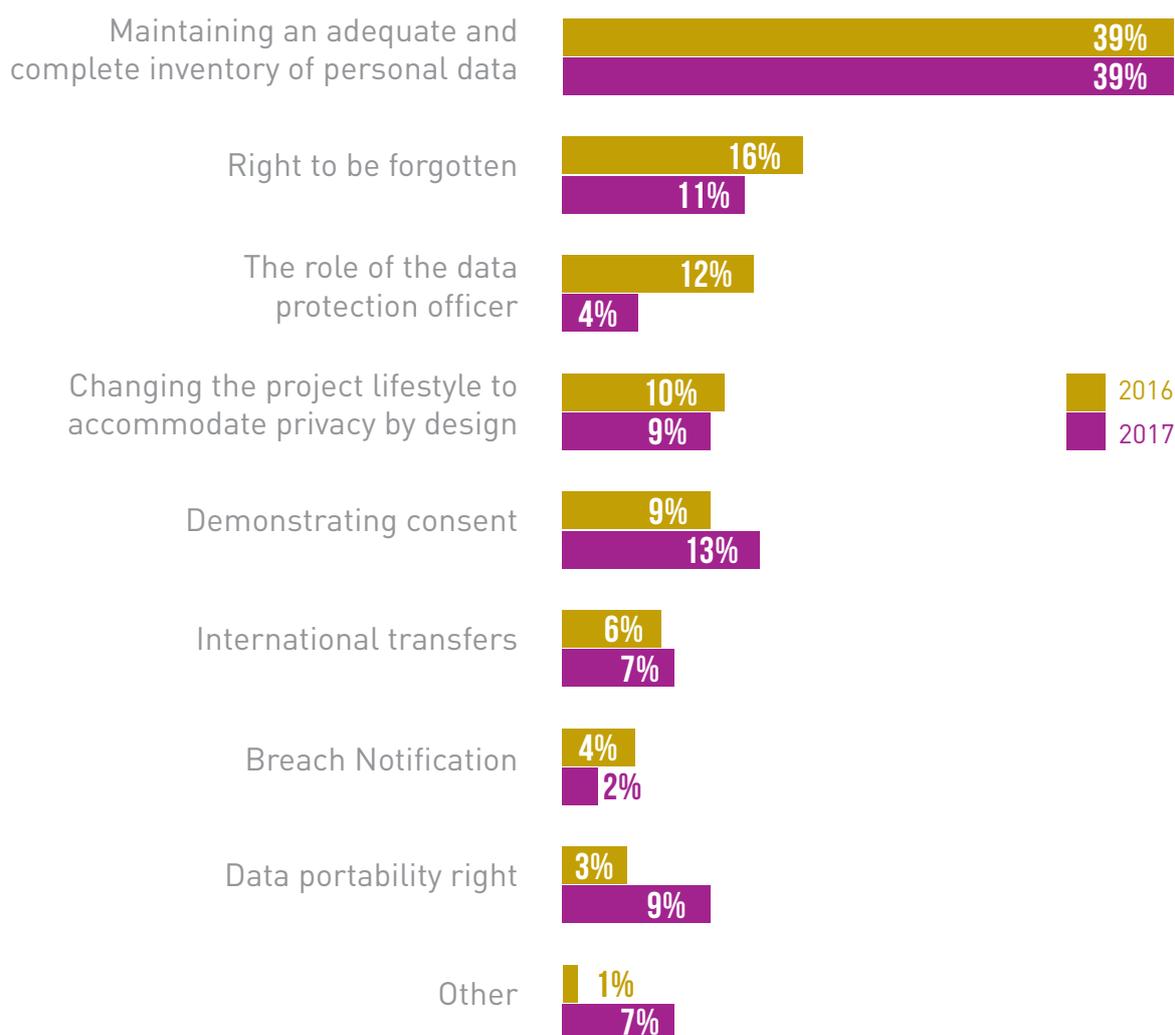
It was good to see that **82%** of organisations have executive or CEO level sponsorship of their compliance programme – up 4% on last year.



KEY FINDINGS

9. EXPECTED CHALLENGES:

Which one aspect of the GDPR listed below do you expect to pose the greatest challenge for your organisation?





CONTACT

IF YOU WOULD LIKE FURTHER INFORMATION ON THE
GENERAL DATA PROTECTION REGULATION PLEASE CONTACT:



Liam McKenna

Partner, Consulting Services, Mazars
Phone: +353 1 449 6454
Email: lmckenna@mazars.ie



Conor Hogan

Manager, Data Protection, Privacy & Security, Mazars
Phone: +353 1 449 4481
Email: chogan@mazars.ie



Paul Lavery

Partner, Head of Technology & Innovation,
McCann FitzGerald
Phone: +353 1 607 1330
Email: paul.lavery@mccannfitzgerald.com



Adam Finlay

Partner, Technology & Innovation,
McCann FitzGerald
Phone: +353 1 607 1795
Email: adam.finlay@mccannfitzgerald.com



Annette Hogan

Consultant
Phone: +353 1 607 1207
Email: annette.hogan@mccannfitzgerald.com

This publication is for general guidance only.
It should not be regarded as a substitute for
professional advice. Such advice should always be
taken before acting on any of the matters discussed.

2017 © Mazars and McCann FitzGerald.

All rights reserved.

Mazars Dublin, Block 3, Harcourt Centre, Harcourt Road, Dublin 2, Ireland
Tel: +353-1-449 4400

Mazars Galway, Mazars Place, Salthill, Galway, Ireland
Tel: +353-91-570100

Mazars Limerick, 98 Henry Street, Limerick, Ireland
Tel: +353-61-319955

also in 79 countries in Europe, Africa, the Middle East, Asia Pacific,
North America, Latin America and the Caribbean
www.mazars.ie

McCann FitzGerald, Riverside One, Sir John Rogerson's Quay, Dublin 2, D02 X576
Tel: +353-1-829 0000 | Fax: +353-1-829 0010

also at London, New York and Brussels
www.mccannfitzgerald.com

