GDPR
and data preparation:

Ready to do business?

In association with

experian™

Key 🏠 **Click** or **tap** this icon to return to this page | **Click** or **tap** the page arrows to move page or simply scroll or swipe

Contents

In association with

experian™

Sponsor's comment

Rebecca Hennessy, director of market strategy, Experian Data Quality

At Experian, we firmly believe the General Data Protection Regulation (GDPR) presents a positive opportunity to transform the way you organise and process your data - increasing the value you derive from it and reinforcing customer-centric business practices that are essential in our data-driven age.

We have once again sponsored Data IQ's GDPR Data Preparation report as we believe it delivers the industry benchmark for insight into how UK organisations are approaching the new legislation and the progress they have achieved in becoming compliant.

This latest instalment offers a fascinating understanding of progress and I believe shows that GDPR has become "real" for many organisations. Levels of awareness are now nearly wholesale and preparedness has moved forward again. Significant numbers of organisations have identified third parties with whom they share data, performed company-wide data audits, and have classified and documented data types. These are activities that were lacking even just 12 months ago.

Further evidence of this awakening can be seen in the recognition across industries that the GDPR will impact on the business operating model. Many organisations understand they will need to adapt systems and processes in order to maximise the benefits of the new legislation.

But it's not easy. Organisations have called out that interpreting the new regulation is the single biggest challenge to its implementation, ranking it far above sourcing and training appropriate staff, auditing data suppliers and gaining budget.

Although daunting, the GDPR should be seen as a chance to transform a business for all the right reasons. Its provisions promise to enforce responsible data practices that can only improve relationships with customers.

At Experian, we support a wide range of organisations with their regulatory data preparations and I would encourage businesses of all shapes and sizes to take the opportunity that this moment brings. Now is the time to create a truly consumer-centric approach to data governance and strategy, and to secure your customers' place at the heart of your data-powered future.

Key findings

- Three-quarters of organisations are very aware of GDPR, with one in five somewhat conscious, leaving barely a handful who claim no knowledge. Yet 12.6 per cent are not very or not at all prepared, nearly equal to the 15.3 per cent who are very prepared.

- The most widely-undertaken preparations are identifying third parties that personal data is shared with (48.3 per cent) and company-wide data audits (43.3 per cent). However, 7.3 per cent have not identifed third-party data sources or sharers, while 16.3 per cent have not documented their personal data sources.

- Seven out of ten organisations are either currently reviewing their privacy policies (59.0 per cent) or have already done so (12.9 per cent), ensuring the front line of data collection should be ready for the new era.

7 out of 10

organisations are either currently reviewing their privacy policies or have already done so

- GDPR allows for data to be collected under legitimate interest or by consent - one third of organisations (36.5 per cent) will decide based on the circumstances, but one quarter (25.8 per cent) have yet to decide, perhaps because they are still waiting for formal guidance to be issued.

One third of companies already enable Subject Access Requests and withdrawal of consent

- Many of the new consumer rights granted by GDPR already exist under the Data Protection Act, meaning one third of companies already enable Subject Access Requests and withdrawal of consent. This falls to just 20.8 per cent for the new right of data deletion and only 11.8 per cent for data portability. Even so, half (47.3 per cent) say they will only react when receiving a Subject Access Request.

- Data Protection Impact Assessments have already been carried out on existing processes by half of organisations (51.1 per cent), while nearly the same number (46.1 per cent) will conduct DPIAs on new processes.

- Data Protection Officers gain significant new status under GDPR - four in ten organisations (43.6 per cent) will enhance the role of their existing DPO. But 15.7 per cent are not planning to have one, even though there are few exceptions to this requirement.

- Dealing with international data transfers may prove to be the hardest new set of requirements to meet, not least because of Brexit, with 45 per cent of organisatiosn saying the don't know whether they will use Binding Corporate Rules, Privacy Shield or rely on an adequacy ruling.

Two thirds of organisations have carried out a data audit

- With GDPR-mandated reporting of serious data breaches within 72 hours, two thirds of organisations have carried out a data audit and know where sensitive data sits, while 44 per cent have analysed their vulnerability to attack. But under four in ten have practiced their data breach response and 26 per cent have no policies or resources in place.

- The biggest challenge facing organisations is agreeing on how to interpret GDPR - 42.9 per cent rank this number one, three times the level who place technology fixes in first place. Although not ranked first by many organisations, training staff is the third most-named challenge.

- Even among companies who are very or somewhat prepared, GDPR is expected to have an impact on their business model - 32.9 per cent of all organisations expect this effect to be high, with 46.4 per cent expecting some impact.

- Data preparation is the responsibility of a wide range of functions, led by marketing (62.0 per cent), data management (58.9 per cent) and CRM/customer management (53.5 per cent). But it is the board which leads in providing finance according to 31 per cent.

- With the breadth of functions involved in data preparation, 23.8 per cent of organisations measure data quality at departmental level. Only 18.3 per cent have company-wide KPIs, but 27.9 per cent only measure data quality at the point it is used - usually, this is too late to remediate any problems.

- Six out of ten organisation do not currently use any of the major methods for keeping data clean, up-to-date and accurate, although just over four in ten (41.1 per cent) do have point-of-use data cleansing.

- Perhaps as a consequence, between two-thirds and three-quarters of firms name five major functions as suffering from some or significant impact from data quality - sales (63.5 per cent), insight and analytics (66.7 per cent), CRM and customer management (71.4 per cent), data management (72.1 per cent) and marketing (75.2 per cent).

Section 1: Planning for the General Data Protection Regulation

1.1 - Awareness and preparedness for GDPR

0.9

2.2

20.3

75.7

- Very
- Somewhat
- Neutral
- Not very
- Not at all

0.9

15.3

16.7

55.4

9.5

3.1

Aware of GDPR (%)

Prepared for GDPR (%)
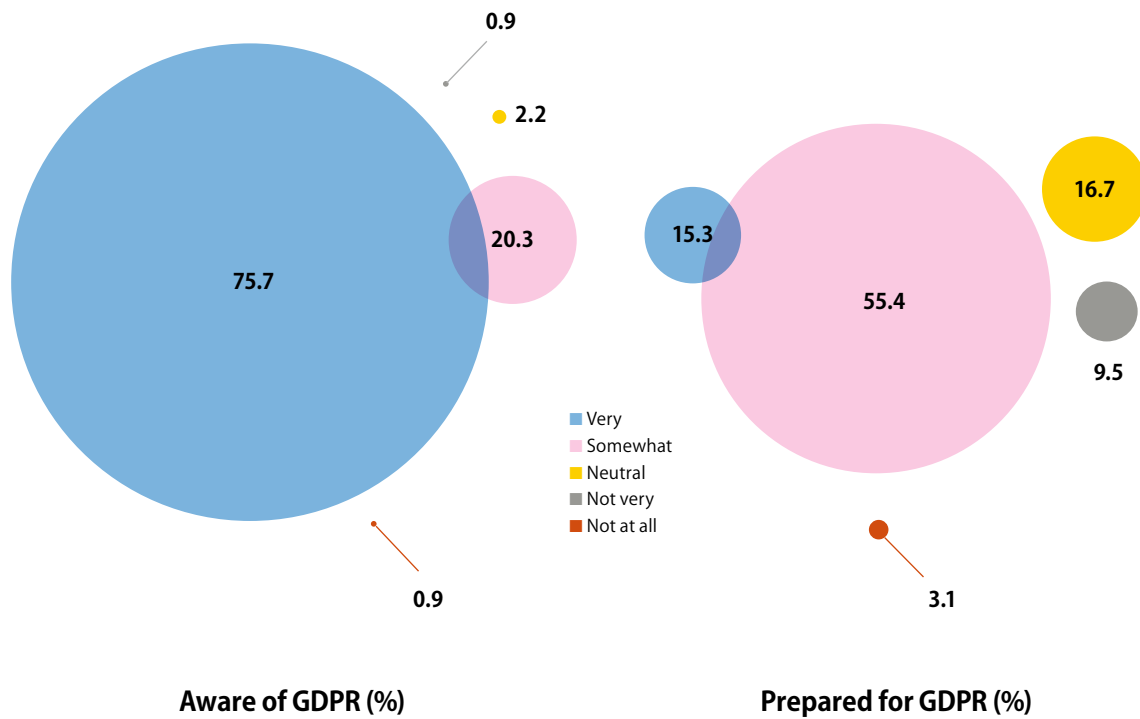
The General Data Protection Regulation (GDPR) was first officially published in January 2012 and passed into UK law in May 2016. Enforcement is due to begin on 25th May 2018. That means organisations involved in controlling or processing personal data have already had over five years to consider how it will impact on their business. So it is unsurprising that three-quarters say they are very aware of GDPR, with one in five somewhat aware. Only a handful claim to have no awareness at all.

Equally, it is not surprising that the majority claim only to be somewhat prepared for the Regulation. Many of its stipulations need to be clarified through guidelines that have yet to be issued, leaving only one in seven able to say they are very prepared for GDPR. More concerning is the 12.6 per cent of organisations who are not very or not at all prepared - time is starting to run out for them to get started.

1.2 - Maturity in the use of data and analytics
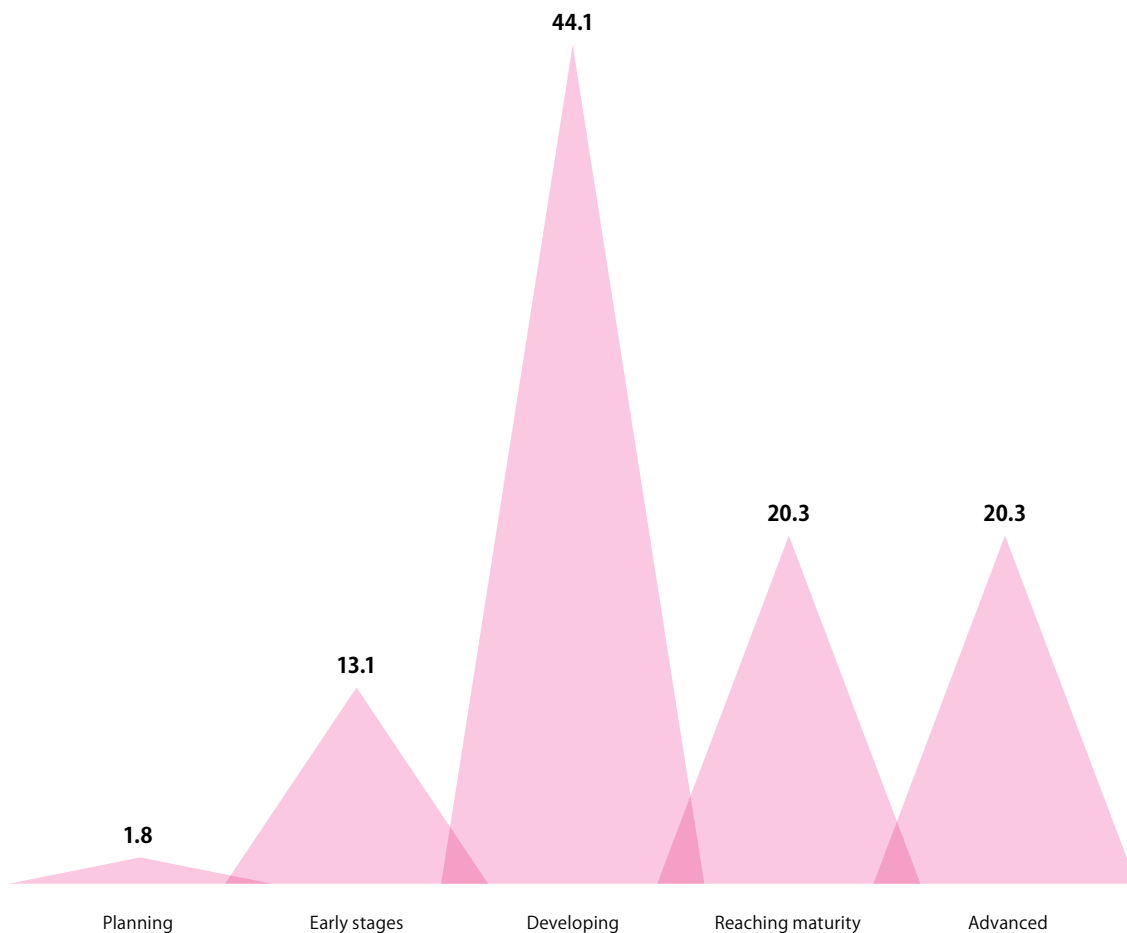
Data and analytics maturity (%)

Planning — 1.8
Early stages — 13.1
Developing — 44.1
Reaching maturity — 20.3
Advanced — 20.3

An important factor in preparing for GDPR is the existing level of maturity around the use of data and analytics within an organisation. The more deeply these have been adopted into business processes, the greater the volume of personal data being used is likely to be and, similarly, the more bound business processes will be to their use. But, equally, at the other end of the spectrum, companies with only limited experience may find it more challenging to adopt the Regulation's requirements as they will have fewer skills to draw on.

The most common level of maturity is Developing - typically, the value of data and analytics will have been recognised and greater focus placed on them. Leaders in this practice who describe themselves as Advanced account for one in five organisations, with a similar number Reaching maturity - a crtical stage where real impact is likely to be seen.

1.3 - Preparedness for GDPR v Maturity
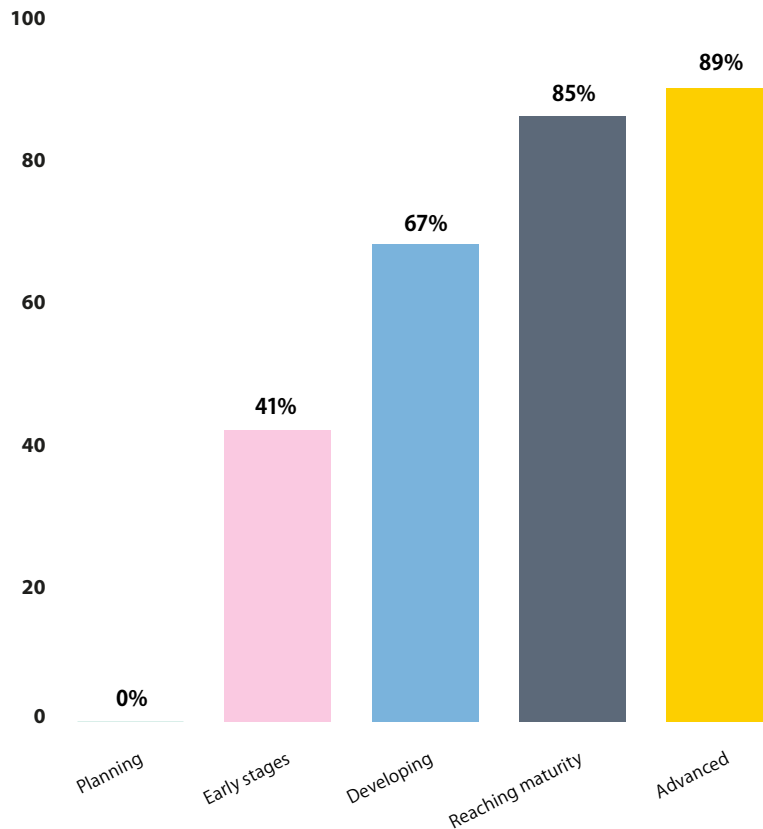
Preparedness for GDPR by level of maturity (%)

Having lengthy notice that legal requirements around data protection are changing should have ensured that organisations started their GDPR projects in plenty of time. This is reflected in the fact that 70.7 per cent describe themselves as very or somewhat prepared.

But the existing level of maturity around data and analytics has made a greater impact than the length of the notice period. From this perspective, nine out of ten organisations who are Advanced and 17 out of 20 who are Reaching maturity saw they are very or somewhat prepared. Their engagement with personal information and the processes and technologies already in place make GDPR projects easier to progress than for those who are less mature.

1.4 - Identifying personal data held by the company

Category	Percentage
Have identified all third parties share data with	48.3%
Already carried out company-wide data audit	43.3%
Have classified data by type and sensitivity	39.9%
Have identified all third-party data sources	39.3%
Have documented all personal data sources	38.8%
Plan company-wide data audit in next 6 months	28.7%
Have created a personal data catalogue	24.2%
Have not documented personal data sources	16.3%
Have not identified third parties source from or share data with	7.3%
Not planning a data audit	4.5%
Unable to classify and catalogue personal data	3.9%
Don't know	13.5%

What GDPR requires organisations to do around the personal data they use is wide-ranging. Steps towards compliance therefore need to cover a lot of territory and each organisation will advance at a different pace depending on its current state. But all will need to identify what data they hold and where it sits, something only just over four in ten have already undertaken, although one quarter are planning for this in the next six months.

A similar number have documented all the sources of PII in the organisation, but just one quarter have created a personal data catalogue - an advanced step that will form an important basis for demonstrating accountability to the supervisory data protection authority. One in eight have not done this so far.

Nearly half have identified any third parties with whom they are sharing personal data - a vital step since data sharing will require a separate consent under GDPR from first-party usage - while four in ten know from which third parties they are sourcing personal data. Ensuring that these sources are themselves compliant is a significant challenge.

Although a small number of organisations have not taken these key steps, those least well positioned to meet GDPR's requirements are the 13.5 per cent who do not know what has been done. That is not a message that will meet with favour from the Information Commissioner.

1.5 - Identifying personal data v Maturity and Preparedness

Already carried out a company-wide data audit
- 44.8
- 57.9
- 70.0
- 52.4
- 43.3

Planning a company-wide data audit in next 6 months
- 37.9
- 21.1
- 20.0
- 30.1
- 28.7

Have documented all personal data sources
- 44.8
- 60.5
- 90.0
- 42.7
- 38.8

Have classified personal data by type and sensitivity
- 37.9
- 47.4
- 60.0
- 46.6
- 39.9

Have created a personal data catalogue
- 34.5
- 36.8
- 50.0
- 28.2
- 24.2

Have identified all third-party personal data sources
- 51.7
- 55.3
- 55.0
- 43.7
- 39.3

Have identified all third parties share personal data with
- 62.1
- 65.8
- 85.0
- 60.2
- 48.3

Legend:
- ■ Advanced (%)
- ■ Reaching maturity (%)
- ■ Very prepared for GDPR (%)
- ■ Somewhat prepared for GDPR (%)
- ■ Average (%)

X-axis: 0   30   60   90

Organisations that are very prepared for GDPR are three times more likely than the average to have documented all their personal data sources (90.0 per cent v 38.8 per cent) and nearly twice as likely to have identified all the third parties with whom they share data (85.0 per cent v 48.3 per cent) and to have carried out a company-wide data audit (70 per cent v 43.3 per cent).

Surprisingly, it is those firms who are Reaching maturity, rather than the Advanced, who are ahead of the pack in their preparations. Nearly two thirds have identified third-party data partners (65.8 per cent v 48.3 per cent), six in ten have documented all personal data sources (60.5 per cent v 38.8 per cent) and have carried out a company-wide data audit (57.9 per cent v 43.3 per cent). It may be that the Advanced have been more focused on leading-edge analytics than on core data management and data protection practices, whereas those at the next stage have built in compliance from the outset.

1.6 - Informing customers of new GDPR rights v Maturity

Have reviewed and rewritten privacy notices in line with GDPR
3.4 5.6 3.9

Privacy policies are currently being reviewed and will be rewritten
10.1 14.0 28.1 6.2 0.6

Not yet reviewed privacy notices - plan to in next 6 months
2.2 1.7 12.9 5.1 0.6

No plan to review our privacy notices
0.6 2.2 1.3 1.1

Legend:
■ Advanced (%)
■ Reaching maturity (%)
■ Developing (%)
■ Early stages (%)
■ Planning (%)

0   20   40   60
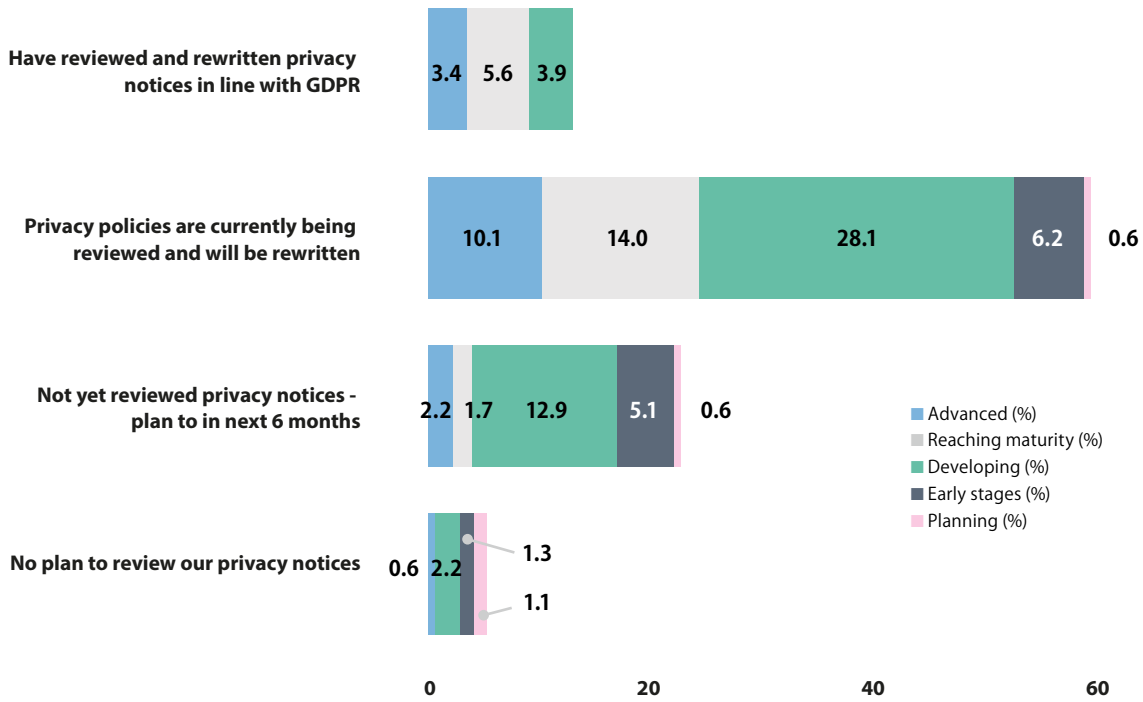
Under the existing Data Protection Act, organisations need to inform their customers about why data is needed, what it will be used for and how they can correct any errors. This means privacy noticies have been in the front line of data collection for several decades. Changing them in line with GDPR is therefore not a major new step, only an extension of an existing process.

As a result, 71.9 per cent of organisations already have the review of their pivacy notices in hand, either because they have already changed them (12.9 per cent) or are currently doing so (59.0 per cent). This is not limited to organisations who already lead on data and analytics - all segments are reviewing their notices, except for those who are only Planning.

A significant minority (22.5 per cent) has yet to start this process, but intends to do so in the next six months. They are taking the risk of running out of time before the most publicly visible aspect of their GDPR project is completed.

Section 2: Preparing the business for GDPR

2.1 - Using legitimate interest and consent v Preparedness
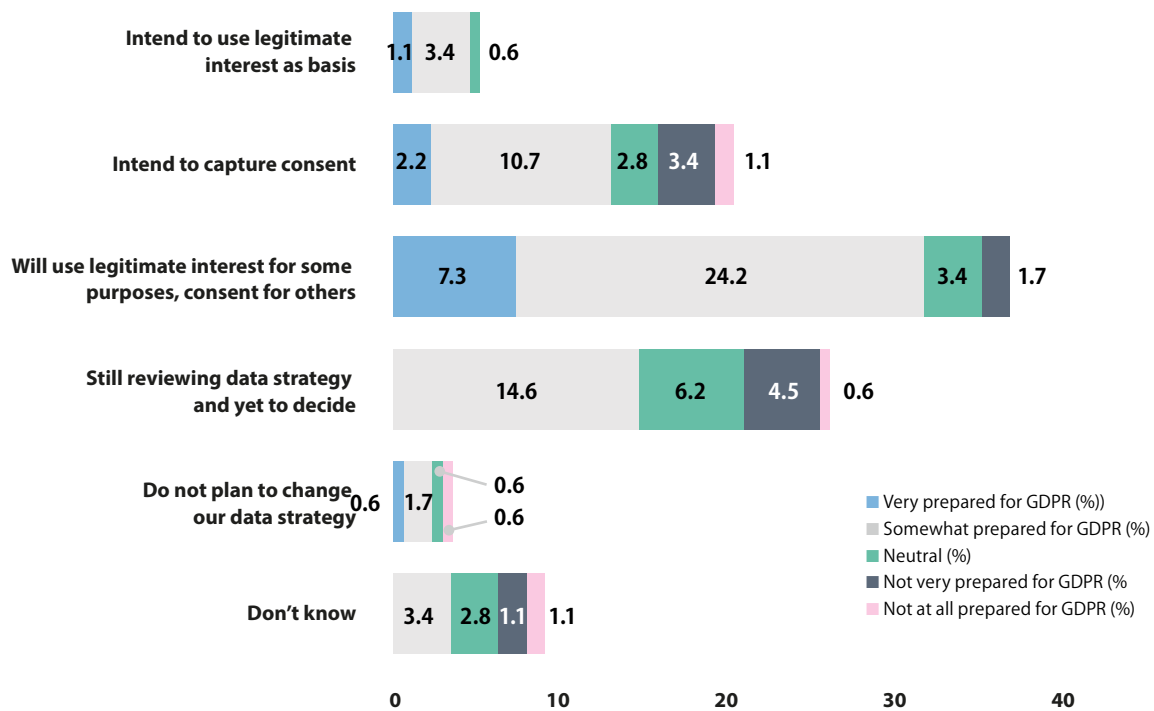
One of the biggest considerations for organisations that rely on personal information is the basis on which they will capture it from individuals. GDPR provides for two approaches - legitimate interest and consent - but guidelines for the circumstances in which either is appropriate have yet to be published. Until they are, firms need to make their own decisions on how to approach this issue. One quarter (25.8 per cent) are still reviewing their data strategy and have yet to make a decision - this might prove to have been sensible if the eventual guidance ends up favouring one approach more strongly than the other.

One third (36.5 per cent) say they will use both approaches, depending on the circumstances. Given the range of purposes for which data is now essential, this is hardly surprising. But one in five (20.2 per cent) plan to capture consent - this will give a very strong legal basis for using personal information, but may also constrain the purposes for which it is used. By contrast, only one in twenty (5.1 per cent) intend to rely on legitimate interest.

2.2 - Enabling new consumer rights

	Already enabled	Enabling in next 3 months	Enabling in next 3 - 6 months	Enabling in 6 - 12 months	Will take more than 12 months	Do not plan to enable	Don't know
Subject Access Requests	36.5	15.7	20.8	7.9	1.1	0.6	17.4
Withdrawal of consent	36.0	12.9	23.6	10.1		1.1	16.3
Data deletion	20.8	16.9	25.3	12.9	2.3	2.3	19.7
Data portability	11.8	14.6	22.5	11.8	2.8	6.2	30.3

Legend:
- Already enabled (%)
- Enabling in next 3 months (%)
- Enabling in next 3 - 6 months (%)
- Enabling in 6 - 12 months (%)
- Will take more than 12 months to enable (%)
- Do not plan to enable (%)
- Don't know (%)

If privacy notices are the frontline of communicating new GDPR rights to consumers, they are only meaningful if the organisation has enabled processes for those rights to be exercised. For an existing right like Subject Access Requests (SARs) it is to be expected that progress will be rapid and 80.9 per cent have either already enabled SARs or will have done so by the time GDPR starts to be enforced.

Withdrawal of consent is significantly enhanced by GDPR since it is intended to be as easy for consumers as their original grant of consent. Eight out of ten organisations (82.6 per cent) have already enabled this or will have done so within a year, perhaps by leveraging the same processes that underpin SARs.

More challenging is the need to delete data if requested or to allow consumers to take a copy of their personal information in a standard, machine readable form. One in five can already delete records, but only just over one in ten already support data portability. Even so, the majority of organisations should be ready in time, although a significant number do not know if they will be able to give their customers the rights to which they are entitled.

2.3 - Business view of enabling consumer rights v Maturity

Only react when receiving a Subject Access Request: 8.5 | 14.0 | 17.1 | 7.0 | 0.8

Are considering a consumer preference centre: 5.4 | 8.5 | 17.1 | 4.7

Will enable deletion if requested: 3.9 | 8.5 | 13.2 | 1.6 | 0.8

Have a consumer preference centre: 2.3 | 5.4 | 7.0 | 0.8

Have enabled customer data access and amendment: 1.6 | 4.7 | 3.1 | 1.6

Don't believe this is what consumers want: 1.6 | 0.8

Waiting to see what other companies do: 1.6 | 4.7 | 3.1 | 1.6

Don't know: 4.7 | 4.7 | 2.3 | 0.8

Legend:
- Advanced (%)
- Reaching maturity (%)
- Developing (%)
- Early stages (%)
- Planning (%)

Until GDPR is enforced, businesses need to meet existing data protection law and also what their customers demand. Nearly half (47.3 per cent) say their support for consumer rights is triggered only when they receive a Subject Access Request, a view that is surprisingly as common among the Advanced and those Reaching Maturity as in other groups.

Consumer preference centres, which offer a very visible willingness to support consumer data rights, have so far only been introduced by 15.5 per cent, although more than twice that number (35.7 per cent) are considering one. This could also prove to be a critical enabling mechanism for data deletion requests if implemented. Remarkably, over a quarter of firms (27.9 per cent) say they already enable this on request, putting them well ahead of GDPR.

Resistance to the idea that consumers do not want these rights is very low, but one in ten (10.1 per cent) say they are waiting to see what other companies do while 12.4 per cent just do not know. Putting off the enablement of rights in this way will make GDPR projects much more pressurised when they do start.

2.4 - Evaluating risks from personal information v Preparedness

Have adopted the principles of Privacy by Design
6.7 | 18.0 | 1.7 / 0.6 / 0.6

Carrying out Data Protection Impact Assessments on existing processes
6.7 | 35.4 | 5.6 | 2.8 | 0.6

Will carry out Data Protection Impact Assessments on new processes
7.3 | 29.8 | 5.1 | 3.4 | 0.6

Have added personal data to Risk Register
4.5 | 24.2 | 2.8 | 1.7 / 0.6

Plan to add personal data to Risk Register
1.1 | 9.0 | 4.5 | 1.7

None of these
1.1 / 1.7 / 0.6

Don't know
0.6 | 5.1 | 5.1 | 3.4 | 2.2

Legend:
- Very prepared for GDPR (%)
- Somewhat prepared for GDPR (%)
- Neutral (%)
- Not very prepared for GDPR (%)
- Not at all prepared for GDPR (%)

0   20   40   60

In order to become accountable for the personal information they hold, organisations have a number of actions that they can take. Just over half (51.1 per cent) are carrying out Data Protection Impact Assessments and nearly the same number (46.1 per cent) plan to carry these out on all new processes.

Including personal data on the firm's risk register has already happened at 33.7 per cent of firms and 16.3 per cent plan to do this, while at a policy level, adopting Privacy by Design is a key step which 27.5 per cent have taken. Each of these actions will not only ensure the organisation is fit for GDPR, but also has policies and procedures in place that reflect a new risk landscape.

2.5 - Introducing the Data Protection Officer

43.6

15.0

15.7

5.0

2.9

14.3

3.6
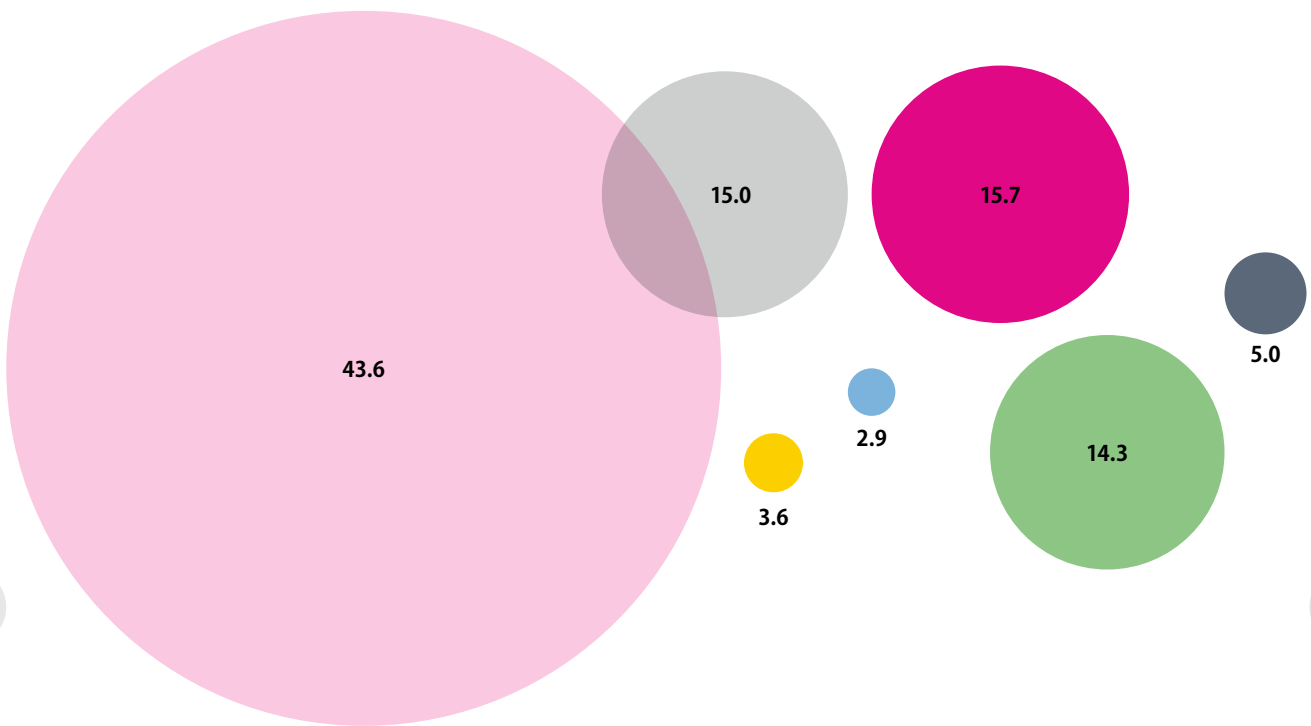
- ◼ Have an existing Data Protection Officer - role will be enhanced (%)
- ◼ Currently creating role of Data Protection Officer - will promote internally (%)
- ◼ Will recruit externally for new role of Data Protection Officer (%)
- ◼ Plan to use third party as Data Protection Officer (%)
- ◼ Do not plan to have a Data Protection Officer (%)
- ◼ Don't know (%)
- ◼ Other (%)

Data Protection Officers (DPOs) are set to play a significant role within organisations holding personal information and are given specific status and rights of their own by GDPR. These exceed what current DPOs can claim, although those already performing this role are most likely to find themselves promoted to an enhanced position. In addition, one in seven

organisations will look to promote their DPO from within.

Surprisingly, one in seven firms say they do not plan to have a DPO. Although this role can be fulfilled by a third party - which a small group of organisations plan to do - there are very few exceptions to the requirement to have an officer in this position.

2.6 - Introducing the Data Protection Officer v Maturity and Preparedness

Have an existing Data Protection Officer - role will be enhanced
- 61.9
- 52.9
- 52.0
- 54.9
- 43.6

Creating role of Data Protection Officer - will promote internally
- 19.1
- 8.8
- 18.8
- 15.9
- 15.0

Will recruit externally for new role of Data Protection Officer
- 5.9
- 3.7
- 3.6

Plan to use a third party as Data Protection Officer
- 4.8
- 2.9
- 6.3
- 3.7
- 2.9

Do not plan to have a Data Protection Officer
- 9.5
- 11.8
- 6.3
- 9.8
- 15.7

Don't know
- 4.8
- 8.8
- 12.5
- 2.4
- 14.3

Legend:
- ■ Advanced (%)
- ■ Reaching maturity (%)
- ■ Developing (%)
- ■ Early stages (%)
- ■ Planning (%)

Axis: 0 10 20 30 40 50 60 70

The existence of a Data Protection Officer who can have their role enhanced for GDPR is 50 per cent higher than average in Advanced users of data and analytics, while plans not to have a DPO are nearly half the average in this group.

But internal promotion into a newly-created DPO role is less likely among those Reaching Maturity - although nearly 10 per cent more than average in this group already have a DPO whose role they will enhance, this would appear to be a gap in their GDPR plans.

Section 3: New business processes and policies

3.1 - Deaing with international data transfers and compliance

■ Already use Binding Corporate Rules for all international data transfers (%)
■ Plan to use Binding Corporate Rules for all international data transfers (%)
■ Already use Privacy Shield for UK-US data transfers (%)
■ Plan to use Privacy Shield for UK-US data transfers (%)
■ Currently rely on EU adequacy rulings for international data transfers (%)
■ Waiting to see how the UK legislates for international data transfers (%)
■ Have identified the lead data protection supervisory authority for each territory (%)
■ None of the above (%)
■ Don't know (%)

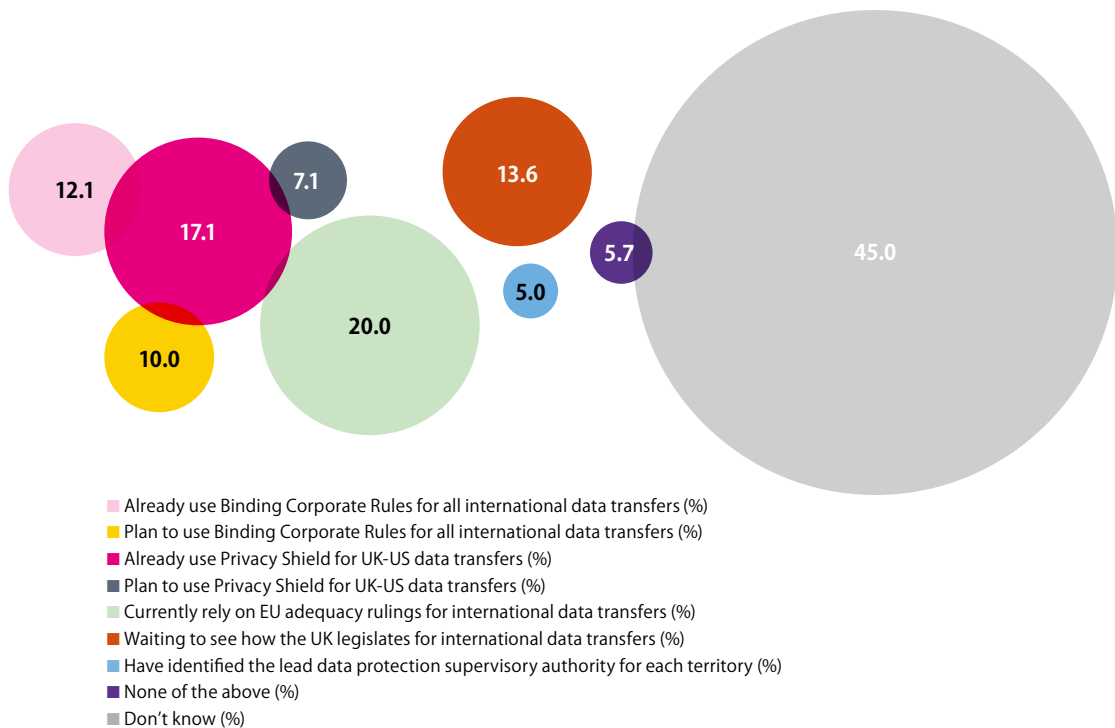International data transfers are almost an inevitability given the global nature of the data-driven digital economy. Rules to ensure that the rights of data subjects are respected during these transfers are therefore important and several key frameworks already exist. One of these is any ruling by the European Union that a destination country has sufficiently robust data protection laws, which one in five organisations say they currently rely on. In the wake of Brexit, one in eight will wait to see how the UK government legislates to enable these transfers.

Almost as important is the Privacy Shield framework agreed between the United States and the EU, which one in six rely on when sending data to or from the US. A recent review has confirmed the robustness of this approach which is reassuring for the 7.1 per cent planning to use Privacy Shield in the future.

Binding Corporate Rules represent the most robust legal approach, but they are complex and expensive to put in place. Nevertheless, BCRs are relied on either currently or in the near future by a significant group of just over one in five.

3.2 - Steps taken to deal with a data breach v Maturity

Step	Advanced (%)	Reaching maturity (%)	Developing (%)	Early stages (%)	Planning (%)
Have carried out data audit and know all systems holding sensitive data	10.0	17.1	15.7	4.3	0.7
Have analysed vulnerability to theft of PII or other data assets	7.9	11.4	9.3	2.1	0.7
Have conducted a financial impact assessment of data breach	2.9	7.9	4.3	2.9	
Have a data breach plan and run practice tests	6.4	10.7	7.9	2.1	
Have pre-approved data breach notification communications	2.1	8.6	5.7	1.4	
Have customer-facing web assets, FAQs and dedicated phone lines ready to go live	1.4	0.7	0.7	0.7	
Have appointed a business parter to support us	2.1	1.4	2.9	1.4	
Have credit and identity monitoring services on stand-by			1.4		0.7
Have none of the above in place		2.1	10.0	5.0	1.4
Don't know	0.7	2.9	11.4	2.9	1.4

A significant obligation under GDPR will be to notify the ICO of a data breach within 72 hours. Depending on the severity of the breach and the sensitivity of the data involved, data subjects may also need to be notified. Having processes in place to meet these requirements is therefore essential.

Knowing where sensitive data is held plays a key role, as recognised by the two-thirds of organisations who have carried out a data audit, as well as understanding the vulnerability of these systems to attack, which 44 per cent have analysed.

But pre-planned responses are less common, with under four in ten organisations having run practices of their data breach plans and only one in twenty having credit and identity monitoring services ready to go live. At least these organisations are better prepared than the 26 per cent who have done nothing or the 27 per cent who simply do not know how prepared they are to respond to a data breach.

3.3 - Top three challenges in preparing for GDPR

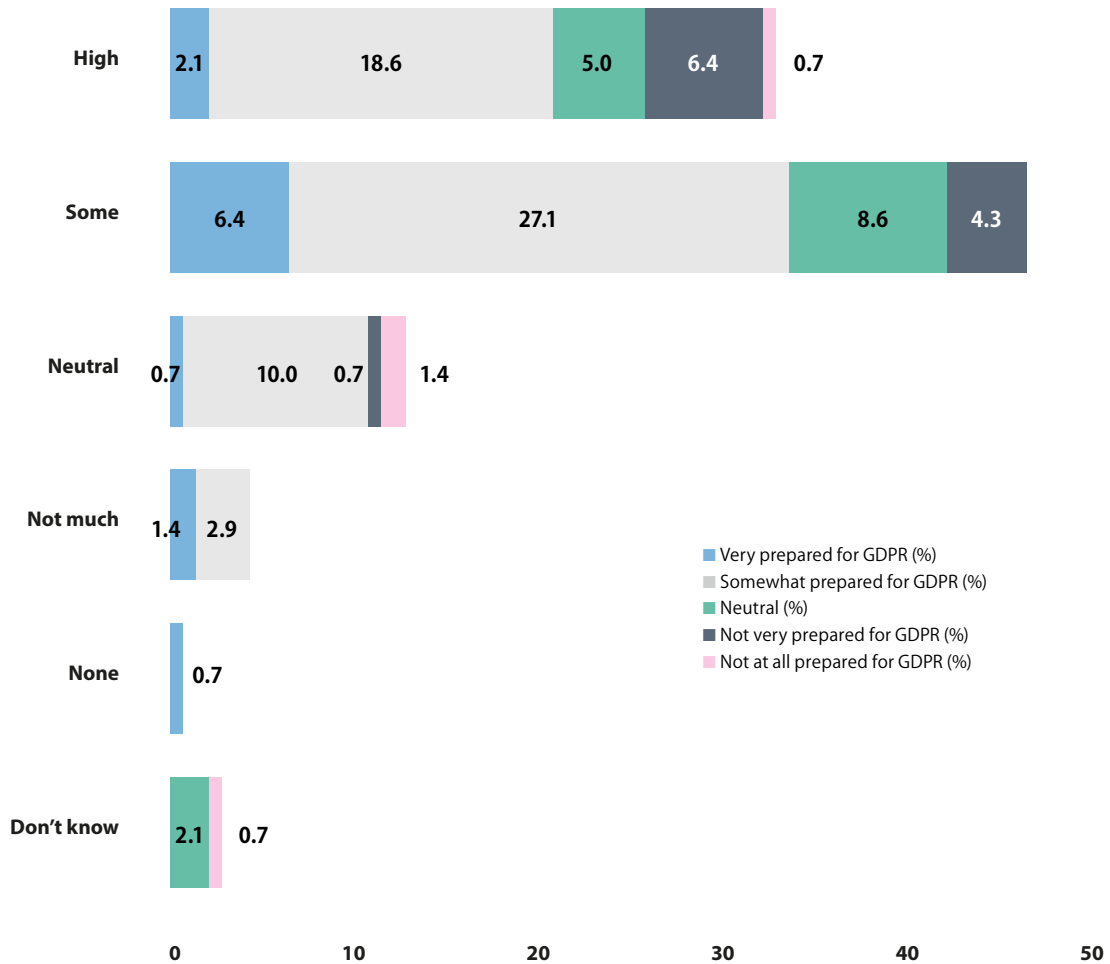| Challenge	Ranked 1 (%)	Ranked 2 (%)	Ranked 3 (%)
Agreeing on interpretation of GDPR	42.9	10.7	9.3
Identifying technology or fixes required	14.3	20.0	10.7
Finding staff with right skills	6.4	7.9	7.9
Agreeing new contracts with all third parties rely on for data and data services	6.4	10.0	17.9
Getting C-level attention and support	5.7	3.6	9.3
Not yet started our GDPR project	5.7	2.1	
Getting budget approval	5.0	7.9	5.0
Getting IT to add GDPR projects to their workflow	5.0	11.4	10.0
Training all staff to understand GDPR	5.0	18.6	17.9
Getting legal and compliance to engage with the business	2.1	5.0	2.9
Finding a Data Protection Officer	2.1	1.4	2.9
Not encountered any challenges	2.1	0.7	2.1

While organisations know the date on which GDPR will be enforced, for four out of ten, the number one challenge to their preparations is the need to agree on how the law should be interpreted. With guidance on key aspects yet to be issued and the need to translate legal obligations into workable business practices, it is not surprising that this issue is three times more challenging than fixing technology.

Although top of the list as a challenge for just one in twenty organisations, training staff to understand GDPR - which is the only way to ensure new processes are followed correctly - attracts the third highest number of mentions in second and third place. This outweighs the number who gave agreeing new contracts with third parties a score of two or three.

3.4 - Expected impact of GDPR on business model v Preparedness

Legend:
- ■ Very prepared for GDPR (%)
- ■ Somewhat prepared for GDPR (%)
- ■ Neutral (%)
- ■ Not very prepared for GDPR (%)
- ■ Not at all prepared for GDPR (%)

High: 2.1 | 18.6 | 5.0 | 6.4 | 0.7
Some: 6.4 | 27.1 | 8.6 | 4.3
Neutral: 0.7 | 10.0 | 0.7 | 1.4
Not much: 1.4 | 2.9
None: 0.7
Don't know: 2.1 | 0.7

A business being prepared for GDPR does not mean it expects the new law to have no impact. Among the 32.9 per cent of organisations who expect their business model to be highly affected, half come from the group who are already somewhat prepared.

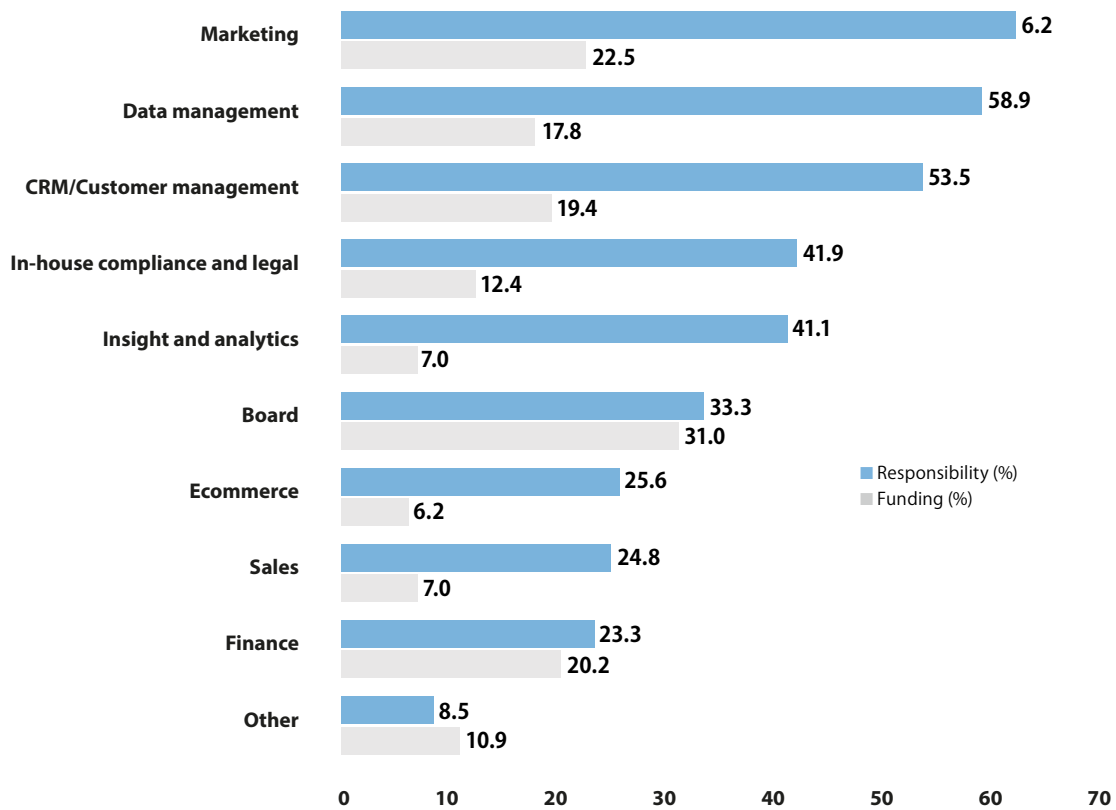The scale of the changes to people, processes and technologies for the use of personal information are simply too great to avoid change. This is clear from the fact that only 5 per cent say GDPR will have little or no impact. Two out of three of the firms who say they are not very prepared anticipate a high level of impact on their business model, even though this fear does not seem to have persuaded them to take action.

Section 4:
Data preparation and the business

4.1 - Functions involved in data preparation

Function	Responsibility (%)	Funding (%)
Marketing	6.2	22.5
Data management	58.9	17.8
CRM/Customer management	53.5	19.4
In-house compliance and legal	41.9	12.4
Insight and analytics	41.1	7.0
Board	33.3	31.0
Ecommerce	25.6	6.2
Sales	24.8	7.0
Finance	23.3	20.2
Other	8.5	10.9

Data is pervasive across organisations and a fundamental resource across multiple functions. This is clear from the range of departments who have responsibility for data preparation activities such as data quality, enhancement and suppression. Customer-facing functions, such as marketing and CRM, take the lead, alongside data management (as might be expected), although ecommerce lags with just one quarter of firms handing responsibility to this department.

It is striking that four in ten organisations (41.9 per cent) have input from in-house compliance and legal, while one third (33.3 per cent) involve the board and one quarter (23.3 per cent) even involve finance. The board takes the lead when it comes to funding data preparation (31 per cent), reflecting the importance of gaining top-level buy-in for any data quality project.

4.2 - Measuring data quality v Maturity
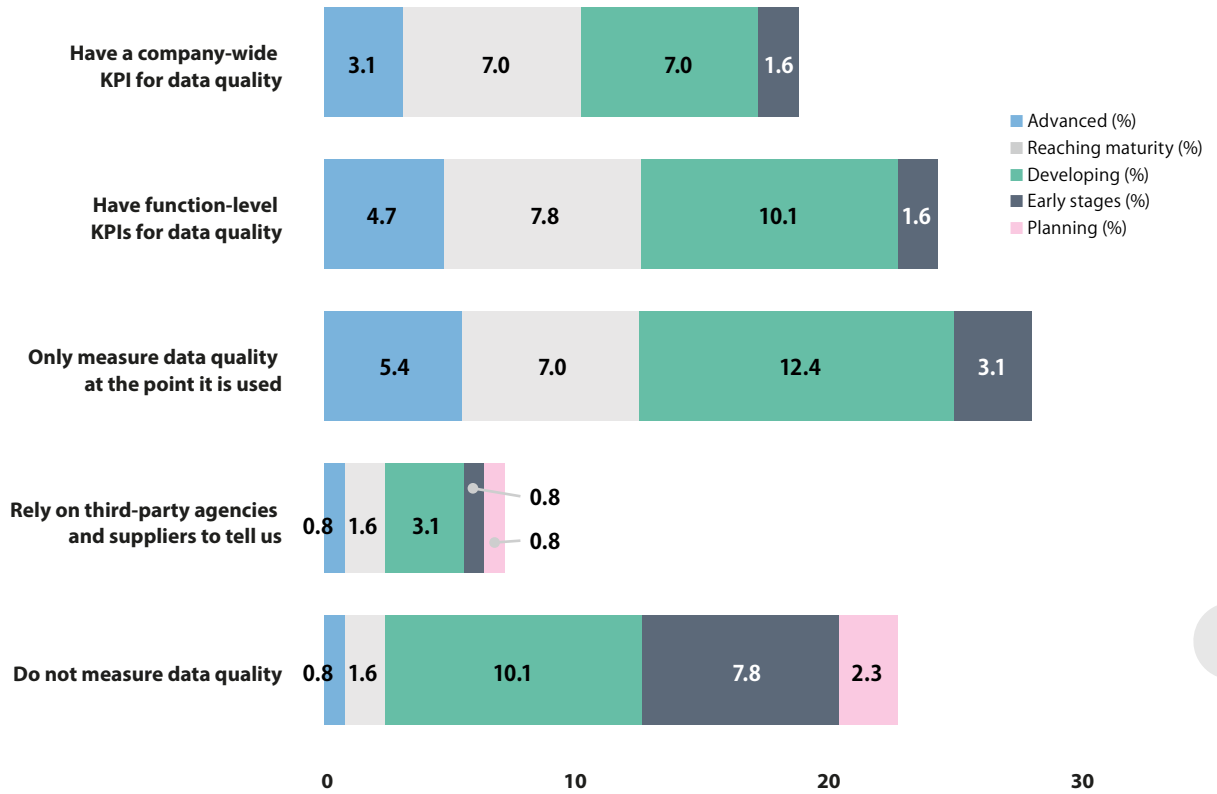
Having metrics for data quality across the organisation should form part of the maturity of data and analytics - as adoption deepens and becomes more sophisticated, so the need to ensure data is accurate, up-to-date and reliable ought to increase. Yet this does not appear to be the case - even the Advanced and those Reaching maturity can be found applying data quality measures only at the point where data is being used. This is the most common approach found in 27.9 per cent of all firms.

By contrast, those still Developing, in Early stages or still Planning are more likely not to measure data quality in any way. With 22.5 per cent of all organisations having no metrics in place, this means the majority of firms are risking a failure in their data-driven process which they may only discover at a critical moment or potentially not at all.

4.3 - Data quality processes used or considering

Process	Currently use (%)	Would consider using (%)	Would not use (%)	Don't know (%)
Point-of-use data cleansing	41.9	30.2	5.4	22.5
Customer data matching and enhancement	41.1	28.7	10.9	19.4
Suppression service	38.0	24.8	11.6	25.6
Data batch preparation service	33.3	26.4	16.3	24.8
Data intelligence service	18.6	28.7	13.2	39.5
Real-time data preparation service	17.8	36.4	13.2	33.3

■ Currently use (%)
■ Would consider using (%)
■ Would not use (%)
■ Don't know (%)

Six out of ten organisation do not currently appear to be using any of the major methods for keeping data clean, up-to-date and accurate. Just over four in ten do have point-of-use data cleansing and it is worth noting that, since only 27.9 per cent say they measure data quality at the point-of-use, a third of those who use data quality tools this way do not know what benefit they are getting. Despite the new reality of in-the-moment digital customer engagement, fewer than one in five firms (17.8 per cent) are using real-time data preparation, leaving more than four in five exposed to data errors at a critical moment of truth.

There is a significant potential adoption curve for all forms of data quality and data preparation services of between one quarter and one third of organisations. The question has to be, however, what has prevented them from facing up to the issue of data quality before now?

4.4 - Impact of data quality across the organisation

	Significant impact	Some impact	Not much impact	No impact at all	No way of measuring impact	Don't know
Marketing	41.1	34.1	5.4	7.8	3.1	8.5
Data management	36.4	35.7	9.3	3.1	3.1	12.4
CRM/Customer management	35.7	35.7	9.3	3.9	3.9	11.6
Insight and analytics	29.5	37.2	10.9	5.4	1.6	15.5
Sales	27.1	36.4	12.4	5.4	3.1	15.5
In-house compliance and legal	16.3	34.9	20.9	8.5	4.7	14.7
Ecommerce	12.4	30.2	14.0	12.4	6.2	24.8
Finance	10.1	31.8	27.1	10.1	4.7	16.3
Board	9.3	29.5	26.4	10.1	4.7	20.2

■ Significant impact (%)
■ Some impact (%)
■ Not much impact (%)
■ No impact at all (%)
■ No way of measuring impact (%)
■ Don't know (%)

Given the range of functions which have responsibility for data quality, there are ample opportunities for organisations to notice the impact it has on core processes (and then to act to remediate any negative dimensions). Between two thirds and three quarters of firms name five major functions as suffering from some or significant impact from data quality - sales (63.5 per cent), insight and analytics (66.7 per cent), CRM and customer management (71.4 per cent), data management (72.1 per cent) and marketing (75.2 per cent). In addition, half recognise that compliance and legal also suffer the consequences when personal data is not right.

Functions that are further removed from the customer might be expected to experience a lower level of impact and this can be seen in the fact that finance and the board are only mentioned by 41.9 per cent and 38.8 per cent respectively.
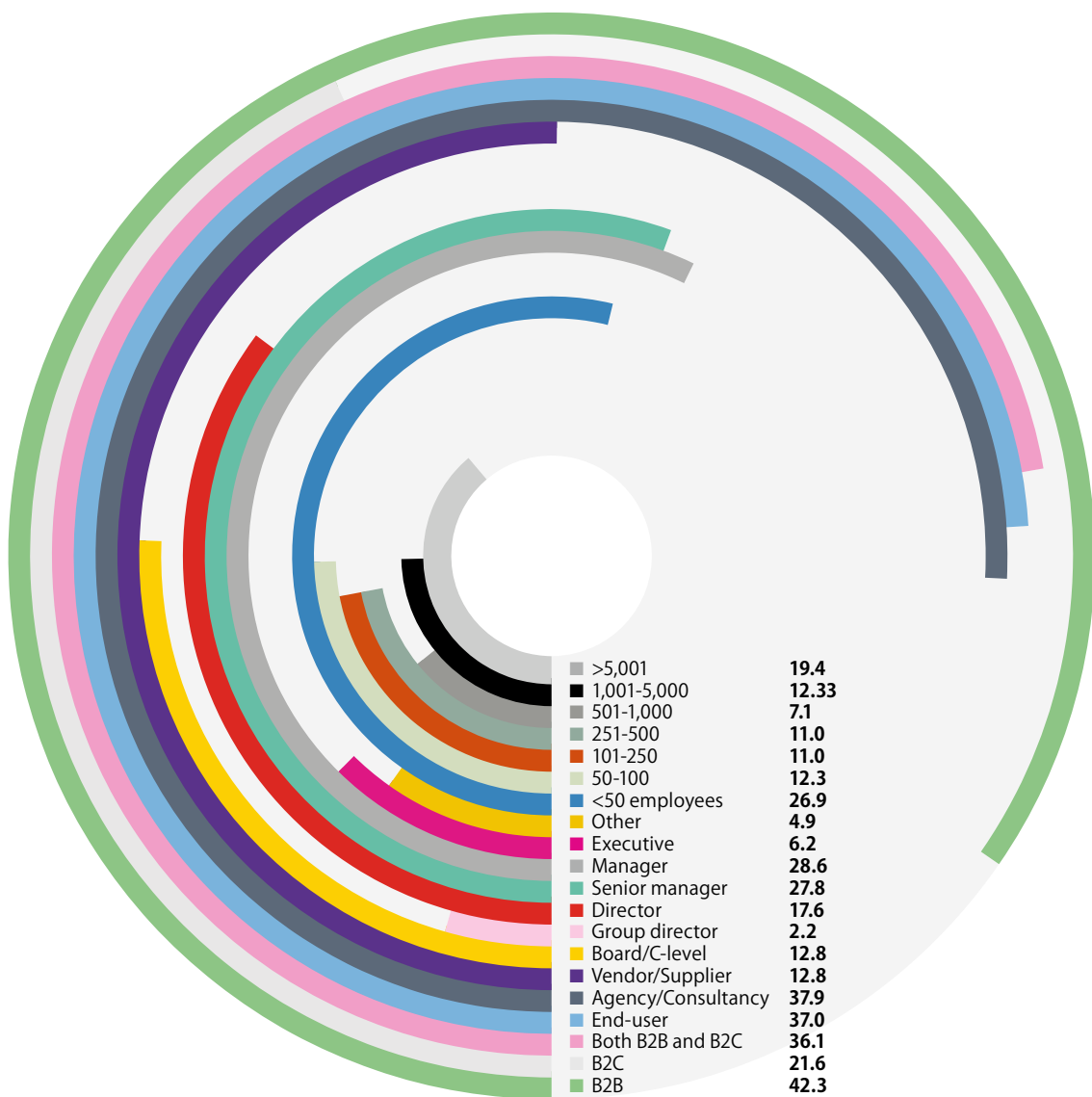
But there is a surprising gap around ecommerce - one quarter of organisations say they do no know whether is is impacted by data quality issues. This rises to three in ten if those who admit they have no way of measuring the impact are included. With digital channels right at the heart of customer engagement for most brands, this lack of insight is worrying.

Methodology

This survey was created as a self-service questionnaire presented online to members of the DataIQ community. Responses were collected during September 2017 and a total of 222 completed surveys were captured.

▮ >5,001	**19.4**
▮ 1,001-5,000	**12.33**
▮ 501-1,000	**7.1**
▮ 251-500	**11.0**
▮ 101-250	**11.0**
▮ 50-100	**12.3**
▮ <50 employees	**26.9**
▮ Other	**4.9**
▮ Executive	**6.2**
▮ Manager	**28.6**
▮ Senior manager	**27.8**
▮ Director	**17.6**
▮ Group director	**2.2**
▮ Board/C-level	**12.8**
▮ Vendor/Supplier	**12.8**
▮ Agency/Consultancy	**37.9**
▮ End-user	**37.0**
▮ Both B2B and B2C	**36.1**
▮ B2C	**21.6**
▮ B2B	**42.3**

GDPR and data preparation: Ready to do business?

About Experian

Experian unlocks the power of data to create opportunities for consumers, businesses and society.

At life's big moments - from buying a home or car, to sending a child to university, to growing your business exponentially by connecting it with new customers - we empower consumers and our clients to manage their data with confidence so they can maximise every opportunity.

We gather, analyse and process data in ways others can't. We help individuals take financial control and access financial services, businesses make smarter decisions and thrive, lenders lend more responsibly, and organisations prevent identity fraud and crime.

For more than 125 years, we've helped consumers and clients prosper, and economies and communities flourish - and we're not done. Our 17,000 people in 37 countries believe the possibilities for you, and our world, are growing.

We're investing in new technologies, talented people and innovation so we can help create a better tomorrow.

Learn more at www.edq.com/uk/gdpr

About DataIQ

DataIQ aims to inspire and help professionals using data and analytics intelligently to drive business performance across their organisation and in every industry sector.

Specifically, DataIQ helps business professionals to understand the benefits of adopting data-driven strategies, develop compelling business cases, implement best practice, ensure they comply with data regulation, and understand how to use the latest tools and technology to deliver sustained business improvement.

DataIQ achieves this by providing essential insight, help and know-how from proprietary research, analysis, best practice and comment from industry leaders and data experts. All made easily available through high-quality events and digital channels.

Our unique community of business decision-makers and influencers - working across functions in FTSE 100, large and mid-market organisations - is growing rapidly as a consequence of this unique focus. Importantly, DataIQ provides the bridge for ambitious vendors, agencies and service providers to ifluence this hard-to-reach and unique community.

DataIQ is committed to championing the value of data-driven business and best practice through focusing on the success stories of data-driven professionals with initiatives including the DataIQ 100 and DataIQ Talent Awards, plus many other events and programmes. We contribute actively to trade and government bodies, including the DMA, IDM, PPA, techUK and UKTI.

For the latest information on how DataIQ can help your organisation go to www.dataiq.co.uk.

For information on how to become a commercial partner to DataIQ, call Adrian Gregory or Adam Candlish on +44 (0)20 3829 1112 or email adrian.gregory@dataiq.co.uk and adam.candlish@dataiq.co.uk