Preparing for the EU General Data Protection Regulation

Assessing Awareness, Readiness & Impact of the Proposed Changes in US, UK, France & Germany
Preparing for the EU General Data Protection Regulation

Introduction

The EU’s new data protection framework, known as the GDPR (General Data Protection Regulation), is in its final stages of negotiation and is due to be finalized by the end of this year and come into force at the start of 2018 after a two-year “sunset” period to allow businesses to prepare for its implementation.

Its proposals are sweeping, and place a number of new obligations on any business that handles the data of EU citizens, independent of where the business is located. That means businesses need to get ready for the old patchwork of laws being swept away and replaced across all 28 member states.

This report looks at the state of readiness and awareness of the GDPR, its obligations and its likely impact on businesses in the EU and the US – and reveals a picture of varying knowledge and readiness for the new legislation.

“Despite over four years of high profile negotiations half of companies are still unaware and there is a worrying chasm between those who are actively preparing and those blind to the changes ahead.”

Chris Babel, CEO TRUSTe

Methodology

The research was commissioned by TRUSTe, the leading data privacy management company and carried out via an online survey between September 18 and October 6, 2015 using a representative external sample of 202 professionals with knowledge of data privacy from companies with >250 employees.

The respondents were not aware that TRUSTe was the survey sponsor. They were drawn from four countries:

• US – 103 participants
• Europe - 99 participants (UK – 35; Germany - 34, France - 30)

While the survey reveals a fairly consistent view across all four markets, there were some notable regional variations. These are noted in the discussion of the findings, but caution should be exercised with these where the sample size is small.

About TRUSTe

TRUSTe powers privacy compliance and trust by enabling businesses to use data across their customer, employee and vendor channels. We have nearly 20 years experience and a team of over 150 professionals dedicated to providing data privacy management solutions and services, including assessments, certifications and our SaaS-based Platform.

The Data Privacy Management Platform provides control over all phases of privacy; from conducting assessments and implementing compliance controls to managing ongoing monitoring. Companies worldwide rely on TRUSTe to minimize compliance risk and protect their brand.
Executive Summary

Overall the research revealed the divide between corporations who were unaware of the pending regulation and a smaller more informed group of companies who have already started to prepare and set aside in excess of half a million dollars to address the necessary changes.

Half of the respondents were not aware of the GDPR – a concerning finding given that the GDPR implementation deadline is potentially just two years away. Awareness was the highest amongst financial services companies (58%) and lowest amongst tech companies that are some of the highest users of data (43%). Companies with mature privacy programs (10-25 privacy employees) had the highest awareness. There was surprisingly no significant difference in awareness between the US and the three European countries surveyed.

Of those aware of the GDPR, two thirds (65%) are starting to prepare even before the law is finalized. 83% had already allocated budget with 21% allocating $0.5 million or more to address the changes and 56% placing this currently ‘High’ or ‘Very High’ on their Corporate Risk Register.

Even though this survey was conducted before the European Court of Justice ruling on the validity of the Safe Harbor agreement there is still a high belief that the new legislation has teeth with 77% thinking that it will be actively enforced by EU regulators. 82% think it will be a higher enforcement priority than the EU Cookie Directive and 76% agree they will spend more on compliance than for the EU Cookie Directive.

The top concerns were the new penalties (42%) and tighter consent requirements (37%). Only 6% are not concerned about any of the proposed changes. Many of the respondents said they felt they do not have enough information on the proposed changes to EU data protection law to help them prepare for the change, and would like detailed guidance on the new requirements. Nearly half (43%) are interested in technology solutions to prepare them for compliance.

73% agreed that the GDPR is the most important change to data privacy legislation for 20 years - and the good news is that four out of five companies (82%) felt the changes would have a positive impact on consumer data protection.

I think it’s the most significant change in global data privacy regulation in 20 years

<table>
<thead>
<tr>
<th>Strongly Agree / Agree</th>
<th>Strongly Disagree / Disagree</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>73%</td>
<td>18%</td>
<td></td>
</tr>
</tbody>
</table>
Preparing for the EU General Data Protection Regulation

The current European Data Protection Directive EC 95/46/EC was finalized over twenty years ago when the internet was available only to the few who could navigate unfamiliar technology and who accessed online services via dial-up modems. The cloud and its associated technologies – distributed data centers, encrypted document transfers, cloud-based back ends, software and platforms as services – barely existed and the entrepreneurs behind the businesses that today use those technologies routinely were still in elementary school.

Technology has moved on dramatically since the early days of the internet, when the concept of online privacy barely existed. The focus was on keeping data held on in-house servers protected from external threats. Consumers, employees and suppliers had little or no idea of how their online activities might be tracked and used for commercial purposes, and the kind of wide-scale theft of personal details that are now common, was pretty much unheard of.

Today businesses have to design and implement privacy and security policies and practices that protect personal data held in the cloud, and probably distributed across a number of servers, possibly in different countries. As well as protecting the personal data of their customers, they also have to manage devices such as cell-phones, tablets and PCs that both access corporate resources and can also contain personal data: the loss or theft of such devices is one of the biggest ways details about third parties are accessed and abused. They have to navigate their way through a myriad of providers and a host of different laws and regulations in the countries they operate in, all the while keeping an eye on the budget and on assessing their risk profile with the threats that emerge every day.

The GDPR – the EU’s General Data Protection Regulation – is a legal framework that will sweep away the existing patchwork of regimes across all 28 member states.

It was first proposed by the European Commission in January 2012 with the aim of boosting online privacy rights and strengthening the digital economy in the European Union. This was in response to how both globalization and technological change have impacted how data is collected, stored, shared and transferred.

The EU hopes that not only will the new legislation improve consumer confidence in the businesses that hold and process their data, it will also reduce costs for businesses who at present have to comply with the different regimes in the countries they either operate in or have customers and suppliers in. The EU estimates that the new legislation will in time save businesses some €2.3bn a year.

The new regulation applies to any business, whether or not it is based in an EU country, that processes the data of EU citizens.

That means businesses from start-ups in Berlin, London and Silicon Valley right up to the multinational giants such as Amazon, Facebook, Google and Microsoft with their operations, customers and suppliers spread around the world, will have to comply with the legislation if they process the data of EU citizens.
Preparing for the EU General Data Protection Regulation

The three institutions involved in the legislative process - the European Commission, the European Parliament and the EU’s Council of Ministers are holding a series of joint meetings, or “trilogues”, to discuss the detail of the proposals. This is the final stage of the process, which began in January 2012. The trilogues themselves began in mid October, and Commissioner Vera Jourová said after the first meeting that “we are on track to adopt the data protection reform in 2015”.

Jan Philipp Albrecht, the European Parliament’s rapporteur, said at the same time that “there are more points we have in common than points that divide us”. In theory, further trilogues in November and December 2015 should finalize all the points and conclude the negotiations, paving the way for finalizing agreement and ushering in the two-year “sunset phase” before the GDPR comes into force.

However, nothing is a given when negotiating and agreeing to complex, detailed European legislation, and there is no time limit set on the trilogues, so if the three parties run into difficulties, the process could spill over into the new year, delaying approval of the GDPR and thus its implementation.

“We are on track to adopt the data protection reform in 2015”
Commissioner Vera Jourová

What is the current legislative state of play?

Key points of the GDPR

The European Data Protection Directive 95/46/EC brought into law the core OECD privacy principles including notice, purpose, consent, security, disclosure, access and accountability.

The GDPR proposals preserve these and build on them with some additional key requirements that will significantly change the landscape of EU privacy and data protection including:

• substantial new penalties of up to €100 million, or 2-5% of annual worldwide turnover, whichever is greater;
• increased territorial scope, impacting more businesses including many outside the EU;
• tighter requirements for obtaining valid consent to the processing of personal data;
• new restrictions on profiling and targeted advertising;
• new data breach reporting obligations;
• direct legal compliance obligations for “data processors;” and
• extended data protection rights for individuals, including the “right to be forgotten”.

Preparing for the EU General Data Protection Regulation

Analyzing the data

The survey covered five key areas for businesses – awareness, attitudes, readiness, top concerns and the overall impact of the GDPR.

1 Awareness

The key finding is that while 89% of businesses think privacy is important, many hadn’t even heard of the GDPR, never mind were aware of its requirements and what they need to do to get ready for compliance: 50% of the 202 companies questioned said they weren’t aware of the proposed changes.

Awareness was the highest amongst financial services companies (58%) and lowest amongst tech companies that are some of the highest users of data (43%).

Size of privacy team was a larger factor than company size. Companies with mature privacy programs (10-25 privacy employees) had the highest awareness. Companies from 1,000 to 4,999 employees had the highest awareness of the coming regulation while those in companies of over 75,000 employees had the least.

There is strikingly little difference in awareness between companies surveyed in the U.S. and those in the UK, France and Germany, with lowest awareness in the UK at 49%.

Analyzing the data

What are your company’s views on privacy?

Very concerned about privacy: 60%
Somewhat concerned about privacy: 29%
Not very concerned about privacy: 10%
Other: 1%

Awareness of new European General Data Protection Regulation (GDPR).

- United States: 50% No, 27% Yes
- France: 50% No, 40% Yes
- Germany: 50% No, 12% Yes
- United Kingdom: 51% No, 12% Yes

Awareness of penalties up to €100 million, or 2-5% of annual worldwide turnover.

- United States: 73% No, 27% Yes
- France: 60% No, 40% Yes
- Germany: 88% No, 12% Yes
- United Kingdom: 88% No, 12% Yes
83% of companies aware of the GDPR had already allocated budget with 31% allocating between $100K-$500K and a further 21% allocating $0.5 million or more to address the changes.

18% of the respondents said that they either had no budget at all earmarked for the changes or had only earmarked $10,000 or less. For those with little or no budget set aside to prepare for and implement the GDPR this leaves the privacy and compliance team in a difficult position: there is a great deal of work to do to prepare for the GDPR, never mind the costs of identifying, sourcing and implementing compliance solutions.

40% of the respondents said that budget would only be allocated once the GDPR is finally agreed, which leaves only two years to prepare. For smaller businesses, two years should be enough time, but larger businesses adopting this policy might struggle to carry out an audit of existing practices, identify changes that need to be made, make sure all the data they currently hold are compliant, research, source and implement technology solutions and find and train staff.

A further 20% of respondents said that funds would only be allocated once the changes come into effect – which means they risk not being compliant with the GDPR when it replaces the national laws and thus face fines.

83% of companies aware of the GDPR had already allocated budget with 31% allocating between $100K-$500K and a further 21% allocating $0.5 million or more to address the changes.

18% of the respondents said that they either had no budget at all earmarked for the changes or had only earmarked $10,000 or less. For those with little or no budget set aside to prepare for and implement the GDPR this leaves the privacy and compliance team in a difficult position: there is a great deal of work to do to prepare for the GDPR, never mind the costs of identifying, sourcing and implementing compliance solutions.

40% of the respondents said that budget would only be allocated once the GDPR is finally agreed, which leaves only two years to prepare. For smaller businesses, two years should be enough time, but larger businesses adopting this policy might struggle to carry out an audit of existing practices, identify changes that need to be made, make sure all the data they currently hold are compliant, research, source and implement technology solutions and find and train staff.

A further 20% of respondents said that funds would only be allocated once the changes come into effect – which means they risk not being compliant with the GDPR when it replaces the national laws and thus face fines.

---

Annual budget allocated to address these changes in regulatory requirements:

- **$10,001 to $100,000**: 21%
- **$100,001 to $250,000**: 15%
- **$250,001 to $500,000**: 16%
- **$500,001 to $1m**: 11%
- **$1m**: 10%
- **$10,000**: 11%
- **Don’t know**: 10%
- **Not earmarked budget for the changes**: 7%

When are the budget decisions made reagrding this kind of regulatory change?

- **As soon as potential regulatory changes are known**: 24%
- **Yearly during annual budget process**: 16%
- **Once regulatory changes take effect**: 20%
- **Once new regulatory changes have passed, but before they go into effect**: 40%
- **Once new regulatory changes have taken effect**: 11%
Preparing for the EU General Data Protection Regulation

Of those companies who are already preparing for the Regulation, encouragingly, more than a third (35%) have already reviewed their IT and security systems, and 32% have briefed the C-suite. Just under a third (31%) have done initial research such as attend a webinar or read relevant articles about the GDPR, while a quarter (25%) have engaged external experts for advice.

German businesses are the ones most likely to have started preparations: 82% of the German companies who were aware of the GDPR were taking active steps to prepare for it, followed by 71% of UK business. French and U.S. businesses are also taking steps, with 60% of companies who were aware saying they are actively preparing.

And many of those preparing for the GDPR say they need help in the form of detailed guidance on the requirements (55 per cent), more information on the proposed changes (53 per cent) and with technology solutions to help them be compliant with the GDPR (43 per cent).

One point to note about the C-suite is that GDPR compliance is a key area that requires expert strategy and leadership. Compliance and protecting the privacy of users is a risk-management exercise as well as touching all other areas of the business from HR to IT, and as such demands leadership and coherent strategy from the C-suite.
Preparing for the EU General Data Protection Regulation

With such far-reaching changes on the horizon, there are a number of areas of concern for businesses. Top of the list, unsurprisingly, is the size of fines, with the Parliament draft of the regulation calling for fines of €100m or 2-5% of global turnover, whichever is the greater.

In the UK, the maximum fine under the current Data Protection Act for example is £500,000, a figure that larger companies could reasonably be prepared to write off as a risk-management cost; however, a serious breach could cost a US company such as Facebook, which reported annual sales of nearly $12.5bn in January last year, a fine of at least 2% = $250M! In the survey, 42% said that the size of the potential fine was their biggest concern.

Other areas of concern for the companies in the research included the tighter requirements for obtaining valid consent (37%), the increased territorial scope of the regulation (34%) and the new breach reporting regulations (29%). Only 6% were not concerned about any of the potential changes in the Regulation. 56% placed the Regulation ‘High’ or ‘Very High’ on their Corporate Risk Register.

Where does the Regulation appear on your Corporate Risk Register?

Those that are aware of the GDPR see it as very important, with 73% of companies agreeing the new rules are the most significant changes in privacy legislation for 20 years. Four out of five companies (82%) say the requirements will improve data protection for consumers, while 65% see the significance more in terms of their own business practice, saying it will increase their ability to secure budget for privacy processes. A total of 77% of those who know about the GDPR say that the new legislation will have a positive impact on their company’s data protection policies and procedures – which will of course be of benefit to their customers, staff and suppliers, and perhaps more surprisingly 45% say the GDPR will have a positive impact on their bottom line.

Even though this survey was conducted before the European Court of Justice ruling on the validity of the Safe Harbor agreement there is still a high belief that the new legislation has teeth with 77% thinking that it will be actively enforced by EU regulators. 82% think it will be a higher enforcement priority than the EU Cookie Directive and 76% agree they will spend more on compliance than for the EU Cookie Directive.
Preparing for the EU General Data Protection Regulation

So what should businesses and their leaders take away from the survey? The key message is readiness: the GDPR is coming, and there is work to be done on both awareness of the details of the GDPR and its requirements, and in taking steps ahead of it becoming law.

Many companies are already allocating budget and preparing for the changes. While two years may seem like a lot of time the breadth of changes is quite significant and your ability and speed to comply will depend on the current privacy maturity of your organization. All of the changes that you implement for the GDPR will help to improve your overall privacy program and reduce your company’s corporate risk profile. So don’t wait for enforcement, the sooner you start to take action the sooner your company will benefit.

There are five areas that the UK’s Deputy Information Commissioner, David Smith, has identified as key priorities for businesses:

• Consent and control - Businesses need to assess where they will need consent from customers, workers and suppliers, and make sure that is obtained. Also, businesses will need to be clear that EU citizens know exactly what it is they are consenting to and the implications of that consent – especially if they are children. Your terms and conditions will need to be appropriate for your users, which means that if you handle the data of, say, 12-year-olds, then the language you use will have to be appropriate for them.

• Staffing – Organizations may need to appoint a Data Protection Officer. If you don’t need a DPO, you will nonetheless need people who understand the detailed requirements of the regulation. Make sure you either have in place the training necessary for existing staff or that you are well on the way to appointing the specialists you will need.

• Privacy by design - Data compliance should not be something special, it should be a matter of course. Businesses should be looking at processes to ensure that this will be the case, including making sure that data they already hold are compliant.

• Breach management - There are two types of organizations: those that have had a data breach, and those that haven’t – yet. The GDPR is set to require businesses to disclose any data breach within 72 hours after becoming aware of it, both to the relevant authorities and to the individuals whose data has been exposed – although there are exceptions if the organization has encrypted that data. If your business doesn’t already have robust procedures in place to deal with disclosure, it’s time to focus on those.

Now is the time to take these steps.

Conclusion

www.truste.com                    1 888 878 7830                   +44 203 078 6495
How good is your knowledge of GDPR? Take our quick 8 question quiz and test yourself.

1. If my company is based outside Europe does the GDPR apply?
   a) No, it only applies to EU-based companies
   b) Only if you have EU customers or monitor the behavior of EU citizens
   c) Only if you previously used EU Safe Harbor

2. Will the GDPR include legal requirements or just guidelines?
   a) Yes they are legal requirements
   b) No, they are guidelines for Member States to implement into law
   c) No, they are guidelines for companies to interpret

3. What does Accountability mean in the GDPR?
   a) Companies must provide annual reports on data privacy programs
   b) Companies must be able to show privacy program details on request
   c) Companies must employ accountants in the EU

4. What are Binding Corporate Rules?
   a) A framework for cross-border data transfers set by the EU
   b) A set of non-negotiable rules for companies of more than 250 employees to comply with
   c) A set of non-negotiable rules that only apply to businesses with more than 5,000 employees

5. What is a PIA?
   a) Personal Impact Authority
   b) Privacy Impact Assessment
   c) Private Individual Agreement

6. What is Safe Harbor?
   a) A list of countries where data can be held
   b) A data privacy framework approved by the US Department of Commerce (currently in transition)
   c) The list of countries the GDPR applies to

7. When do companies need to comply by?
   a) As soon as the legislation is in place
   b) One year after legislation agreed
   c) Two years after legislation agreed

8. How big could the penalties be?
   a) Up to 500,000 euros
   b) Up to 1 million euros
   c) Up to 100 million euros

Answers: 1)b  2)a  3)b  4)a  5)b  6)b  7)c  8)c