Understanding the journey towards EU General Data Protection Regulation

A survey report exploring EU awareness of new data protection legislation
Executive summary

New European data legislation is now a reality as every organisation will have to comply with the impending EU General Data Protection Regulation 2014.

The main benefit of the new European Data Protection Regulation is that it is the first attempt to create strong data protection laws for Europe’s 500 million citizens. Or as Vivanne Reding, Vice-president of the European Commission, responsible for justice, fundamental rights and citizenship puts it; “we are creating one regulatory authority - a one stop shop”.

The new legislation is set to ricochet through corporate organisational processes and policies; from HR departments to sales and marketing, this new regulation has the potential to be far reaching. With the UK economic landscape increasingly dominated by globalised or ‘without borders’ virtual businesses or fast growth technology and data-led operations, the cost of failing to protect or play by the new EU rules has massive implications on the growth and shape of our future workplace.

With ratification of the regulation expected later this year, both public and private sector organisations need to start thinking about this now. Failure to comply is simply not an option - if the regulations are broken, fines for organisations could be as high as €100 million or 5% of global revenue. In effect, this has the potential to put a company out of business.

Trend Micro has partnered with Vanson Bourne to explore how aware European organisations are of the new data regulation and whether it’s realistic for them to comply with.

The research has revealed an alarming lack of understanding of the new data regulation, with half of businesses completely unaware of what it is and just one in ten fully understand what steps their organisation needs to take to achieve compliance.

The findings also reveal that more than eight in ten British respondents (85%) believe their organisation faces significant challenges in order to comply with the EU Data Protection Regulation, with a quarter (25%) saying they don’t even think it’s realistic to adhere to. Lack of employee awareness (44%) and restricted resources (31%) were highlighted as the biggest barriers.

This report explores these findings in more detail and provides advice for businesses to help them prepare for the regulation changes.
Introduction

European data laws are changing. The European Parliament voted last month to back the European Commission's proposals to harmonise data protection rules across all the member states - yet UK businesses not only lack awareness of the far-reaching changes that are coming, they are also not ready.

Businesses should be able to look to the government for help with getting ready for the passing into law of the directive, says James Walker, a security adviser at Trend Micro. “The government needs to ensure that our businesses are ready,” he says. “They need to be creating advisory groups to help business understand what the regulation means, and what technology and processes need to be in place.”

This report will look at what the regulations mean for businesses across Europe as well as reveal research into what senior IT decision makers know, or don’t know, about what they need to do to comply.
Protecting privacy

There are three main planks to the regulation, which the European Parliament will move towards implementing. While the ratification date has yet to be set, it could be as early as next year that businesses will have to be compliant.

1. The first key point is, as the European Commission, says: one continent, one law. This means that the regulation will establish a single pan-European law for data protection to replace the inconsistent patchwork of national laws. The European Commission estimates that the benefits will be worth €2.3bn per year.

The implementation of a single pan-European law means that businesses will only have to deal with one supervisory authority rather than different ones in different member states.

2. The single regulation also means that companies based outside the EU as well as those in member states will have to comply with the regulation if they do business with EU companies or look after the data of EU citizens.

The regulation will enshrine the right of EU citizens to be forgotten, which means that unless there is a legitimate reason for preserving it, a company will have to delete your data. It also provides for citizens to have easier access to their data, making it easier for them to transfer it between providers.

3. Businesses will also have to explicitly seek permission to process the data of citizens: consent cannot be assumed and companies will have to notify citizens of any data breaches that could affect them.

Data security becomes an overriding priority under the regulation, with safeguards having to be built in to products and services from the earliest stages of development. The European Commission stresses that “privacy-friendly default settings should be the norm”.

The sanctions for breaching the rules are much tougher: the fines could go up to 5% of a non-compliant business’s global turnover, or €100m, whichever is greater.

Smaller businesses of 250 or fewer employees are exempt from some of the tougher requirements, including the requirement to appoint a data protection officer and they won’t be obliged to carry out an impact assessment unless there is a specific risk.

“It’s a lot for businesses to take in - and thus far it seems as though they haven't taken it in. There does seem to be a major lack of understanding”

- James Walker
Awareness of the rules

Awareness of the need to comply with current data protection regulations is reasonably high across Europe - but 15% of businesses surveyed by Trend Micro said they were not aware that they had to comply with any regulations, with 12% of British businesses saying they weren't aware. German businesses scored highest on their general awareness, with 92% aware of the requirements.

Levels of compliance with current regulations leaves something to be desired: 30% of all respondents across the EU don’t comply with the existing data protection regulation, with 14% of British businesses not complying with the present Data Protection Act. Across the EU, 11% of businesses said they didn’t know which regulations they had to comply with.

However, when it comes to awareness of the forthcoming EU-wide law, only half of the respondents in the UK are aware of the proposed regulation. Awareness is higher elsewhere in the EU, with 65% of French businesses saying they know about it, while Polish and German businesses have the highest awareness, with 73% and 87% respectively saying they are aware of the proposed regulation.

Unsurprisingly, perhaps, financial services businesses have a high awareness, with 72% in that sector saying they know about the forthcoming rules. Utilities businesses have the highest awareness: 88% say they know about the EU data regulations.

Of those who said they did know about the forthcoming change in the law, 76% across all the EU countries surveyed said they know what it requires, with the highest awareness among German businesses (93%). A total of 70% of UK businesses who knew about the new law said they also know what it would require.

However, nearly half of those responding weren't aware of the level of the fines they could face under the new rules. Only 28% of all of those responding knew that the fine for a data breach could be up to 5% of their annual turnover, and the number was even lower in the UK - just 20% knew the detail of a potential fine.

A total of 38% knew they could face a fine, but didn’t know what the fine could be, while 18% were not even aware that they could be fined for failing to comply. In the UK, a quarter of businesses surveyed didn't know they could be fined, and nearly half (46%) knew they could be fined but didn’t know how big the fines might be.

Given those responses, the finding that only 13% of businesses rated their understanding of the proposed EU General Data Protection regulation as “very good” perhaps does not come as a surprise.

And UK businesses in particular have a lot of catching up to do: just 7% said their understanding of the regulation is “very good”, with 23% saying their understanding is “good”. Worryingly, 23% said their understanding is “poor” - their peers in other EU states fared much better with 20% of French respondents saying they had a “very good” understanding of the regulation.

“Organisations need to start to understand the impact of the regulation,” says James Walker. “They need to start to plan for it from the board down and understand how it would impact their business if they were to have a breach.”
Compliance

“No organisation is exempt”, stresses James Walker

While SMEs are not subject to some of the rules, nonetheless they will have to be compliant, as will any organisation that does business with EU companies or that looks after the data of EU citizens.

However, UK businesses are not ready for the new regulations: only 10% of British companies responding to the survey said they fully understood what steps they need to take to be ready, while 38% say they need more guidance. Only 10% are confident they will have the right data protection processes in place.

And businesses across the EU have some work to do before they’re able to comply with the regulations: more than half (52%) say they need to increase their investment in IT security, with 64% of German businesses saying the same thing, the highest of UK respondents, the highest in the EU. A total of 32% say they need to increase their business insurance to cover a data breach, while 29% will need to hire a data protection officer – a key requirement of the new rules.

Just 11% of all those surveyed said they are confident that they already have sufficient protection in place and don’t need to take any further steps – and 15% of UK businesses say they are already compliant. That’s the highest proportion of respondents: only 8% of French businesses say they are ready, while the Italians have the most work to do – just 1% of businesses in Italy say they need take no further steps.
Realistic requirements

Despite the tough requirements of the new regulations, more than half (51%) think they represent a realistic target for businesses to comply with - although the figure is lower among UK businesses, of which 40% think it’s realistic.

Although the date for ratification is not yet set, European heads of state and government committed to a timely adoption of the new rules at a summit last October, which means that businesses need to prepare for compliance - which could be required within a couple of years.

However, organisations face some challenges in preparing for compliance: 31% say there is a lack of employee awareness, while 30% say they are restricted by legacy IT systems. Just over a quarter of EU-wide respondents (26%) said they didn't have sufficient resources to improve their existing processes, and 24% said that they didn’t have a formal process in place to notify their customers of a data breach.

That lack of readiness is more widespread in British organisations: 28% said a lack of a formal process that they can use to notify customers of a data breach was a challenge in preparing for compliance.

And only 26% of UK organisations already have a formal process in place and always use it to notify customers of a data breach, and 32% do not have a formal process. Across the EU, only 19% of businesses have a process and always use it.

However, European businesses might not be ready to comply: only 39% of those responding thought that between one and two years was enough time to ensure compliance. Of UK businesses responding to the survey, 40% thought that that timeframe would be sufficient, while overall, European businesses thought that 23 months would be a realistic timeframe.

That timeframe was broadly agreed across the respondents: UK and French businesses also agreed that 23 months would be sufficient, while German businesses thought that 21 months would be enough time.
Significant incentives

The potential size of penalties under the new law has made organisations sit up and take notice: 43% of all the organisations responding say that a fine of 5% of their annual turnover would be a significant hit, while 58% of UK businesses said a fine of that size would be significant.

The present regime clearly has not encouraged businesses to beef up their security: at present just 16% of organisations across the EU are very confident that their organisations are as secure as they can be – and that figure drops to 13% for UK organisations.

Not even high-profile data breaches have thus far sparked organisations to rethink their data protection strategy, according to the survey: only 13% said the big breaches from organisations including Adobe, which last year (October 2013) suffered the loss of some 38 million customer records at the hands of a hacker, had made them fully rethink their data protection strategy.

There are a number of steps organisations can take to make it more difficult for hackers to steal information, but worryingly, not much more than half of all the respondents had taken such steps: 58% had worked to increase staff awareness about data security, while 51% have implemented encrypted passwords, and only 29% have rolled out a way to wipe devices remotely if they are lost or stolen.

Encouragingly, UK businesses scored well in this area, with 72% saying they have worked to increase staff awareness and 60% implementing encrypted passwords.

Whose responsibility is it?

James Walker believes that now is the time to communicate. Our government needs to ensure that our businesses are ready.

“\nThe government needs to help create advisory groups to help businesses understand what’s required of them, what technology and process changes there will need to be.\n\nThere needs to be outbound, proactive advice to business.”\n\nEnsuring compliance means understanding the new rules - and most businesses (70%) agree that the responsibility for that lies with the organisation as a whole. Across the EU, 26% believe the responsibility to ensure compliance rests with a data protection officer, while 21% think it’s the government’s responsibility.

Most, however, believe that it’s up to national governments to make businesses aware of the changes in the law, with 32% of EU businesses saying that. In the UK, that figure rises to 42%, with just 10% of UK businesses and 14% of all EU businesses believing that responsibility should lie with industry bodies.
The right regulations

It’s important to handle this well, says James Walker. “Europe is doing the right thing,” he says.

“Whether this is seen as a hindrance or something that our present data protection regime isn’t doing properly is down to politics.”

Presenting the legislation as a burden would play into the hands of isolationist politicians when in fact the new regime not only benefits everyone, from consumers to the biggest businesses, it also has to be complied with whether a country is a member of the EU or not.

“There’s a need for this to happen,” says James Walker. “There is no way back from it. It will become the law in every member state and businesses need to prepare themselves.”
Handling of customer data

How prepared are businesses for the handling of customer data and the security requirements that the new EU framework will demand?

It’s clear from the data that businesses are more aware of the general issues around data security: big security breaches have proven to be a wake-up call for companies - but there is work to do.

Target, the US retailer, suffered an enormous breach at the end of 2013 when hackers stole the details of 40 million credit and debit cards and 70 million customer records that included key data such as names, addresses, email details and phone numbers. In February, the crowdfunding platform Kickstarter suffered a breach, with users’ email and home addresses and phone numbers, as well as passwords, stolen by hackers. In May we also saw online marketplace eBay suffer what has been described as one of the biggest data breaches in history, with some 145 million users having their names, email addresses and other personal data records stolen by hackers.

Those and other high-profile breaches such as the ones suffered by Sony and Adobe prompted 76% of respondents to have a rethink of their data protection strategy - although worryingly, 24% said that they hadn’t reconsidered their data protection strategy in the wake of those attacks.

In the UK, just 8% of respondents said they’d had a full rethink, although 36% said they’d had a partial rethink and nearly a quarter (24%) had had a small rethink, while 32% - the highest proportion of businesses across Europe - said they hadn’t taken another look at their data security policy. UK businesses were the most complacent of the respondents (32%); only the Nordics came close, with 28% of respondents in those countries saying they had not had another look at data security in the wake of those high-profile security breaches.

James Walker says this shows a lack of understanding: “All they see is the top level - that there is potentially a bigger fine. They’re not asking ‘What do I need to change in my business to make the handling of my data more secure?’ This is certainly relevant when we consider the provision within the draft regulation for the right to be forgotten, which actually has already been enacted by the EU Court of Justice in its recent Google decision (based on the existing Data Protection Directive).”

Most British businesses are confident, however, that their organisation is as secure as it can be against a data breach: 69% said they were either very confident (13%) or somewhat confident (56%) that that is the case.
However, confidence about security is higher in other European countries, with 15% of French companies saying they are very confident and 55% saying they are somewhat confident. German businesses are also more confident than those in the UK: 19% are very confident and 54% are somewhat confident.

That businesses are being prompted by news coverage of big breaches suggests that the current penalties aren’t doing their job, says Rik Ferguson, Vice President Security Research at Trend Micro. “Driving change is what the fines are meant to do: the financial incentives aren’t big enough at the moment. It needs to drive the decision away from the IT team to the board.”

However, it’s not just the fine that a business has to pay. “Sony was only fined £250,000 in the UK [in 2011],” notes Ferguson. “But it took a big hit to its reputation. It’s estimated that the breach cost it close to $1bn. That starts to make companies worry.”

That means businesses should not be complacent about their existing security provision: the new framework could mean fines of up to 5% of global turnover or £100m, a level that pushes the potential costs of a data breach firmly into the C-suite’s territory. Says Walker: “Board members will want to make sure costs can be contained. Big cases have highlighted the financial impact businesses can suffer and that’s working in the same way as the new big fines will: These could impact the companies’ bottom line, which will ultimately cost the C-suite their jobs and/or impact their bonuses.”
Taking steps

Businesses are taking steps to protect their customers’ data, Trend Micro’s survey reveals, with the focus being on staff awareness.

That’s an important step, as it’s a given that users are usually the weakest point of any security regime. In the UK, 72% - the highest number in Europe - say they are increasing staff awareness about how they can be targeted by criminals in so-called “spear-phishing” attacks and by clever social engineering, when they are tricked into clicking on links or opening malicious files that allow remote access to the attacker or revealing key information to a hacker posing as someone who is safe to give information to.

“Some organisations are very good at doing education on handling data and how to spot phishing attacks, but some aren’t,” says James Walker. “This forthcoming EU legislation is there to try and ensure that it becomes more important.”

How staff use their own devices in a BYOD environment is already under review, says Walker. Businesses are “ensuring that devices that employees use to access data – especially regulated data – are encrypted and can be remotely wiped”, he says. “They’re also ensuring that certain types of data are either held in a secure container on the device or doesn’t even get on to those devices at all by using virtualisation technology that keeps data on central servers to help reduce accidental loss by employees.”

That is reflected in the survey, which found that businesses are implementing encryption technology, with 32% of those in the UK doing so, as well as adding remote-wipe capability for lost devices (47% of UK businesses) and being much stricter about locking down hardware so that, for example, an infected USB stick can’t cause havoc on the network (44% of UK respondents).

That increased strictness about hardware is even extending to the C-suite, where senior staff have been known to override IT concerns. “It’s definitely a discussion point now,” says Walker. “Two or three years ago, when BYOD really started, it was the board saying ‘I want my iPad connected’. Now it’s a more official process.”

The focus on raising staff awareness dovetails with a perception that cyber-criminals are the biggest threat to the security of business. On average, a quarter of EU businesses identified hackers as their biggest threat, with 29% of UK respondents pointing to criminals. That proportion was even higher in France (35%) and Germany (33%).

However, UK businesses are more concerned about their staff accidentally losing devices leading to a data breach, with 36% identifying that as the main concern. EU counterparts are less concerned: while a similar number of Nordic businesses (31%) said that was a worry, by contrast just 11% of French and 14% of German businesses agreed that it was a concern.
What customers want

Despite growing awareness among businesses about the importance of data security, it seems their customers are less concerned about how and where their data is kept, with 35% of respondents across Europe saying that “slightly more” of their customers were demanding greater transparency from them about how their data was stored, and just 19% saying that “significantly more” were demanding that transparency.

People in the UK seem even less interested than those elsewhere, with just 9% of UK businesses saying their customers wanted significantly more transparency and 28% reporting that slightly more were demanding to know more about how their data is stored. Yet, a third (32%) do not have a formal process in place to notify customers in the event of a data breach and only 26 per cent have a formal process and always notify their customers.

By contrast, EU customers are much more concerned, with 34% of Benelux businesses and 37% of Nordic companies saying their customers were demanding significantly more transparency, and 43% of businesses in Poland and 49% in Italy saying their customers were seeking slightly more transparency regarding their data.

In the UK, 13% of businesses reported that their customers never demanded transparency about how their personal data is kept. That is set to change, says Walker: “We’re going to see a lot more customers invoking the right to be forgotten, he says.

Customers will be asking “Do organisations even know where my data is? Do they know how to delete it?” says Walker, adding: “It’s being driven by the right to be forgotten, which is a key bit of law that businesses are nowhere near where they need to be.”

The search giant Google has been most in the spotlight over the right to be forgotten, with high-profile individuals such as the BBC’s economics editor, Robert Peston, flagging up concerns about the visibility of his journalism.

Peston described on his blog how Google had notified the BBC that it had removed links to a post he had written under the right to be forgotten, saying: “A blog I wrote in 2007 will no longer be findable when searching on Google in Europe. Which means that to all intents and purposes the article has been removed from the public record. Google... has responded to someone exercising his or her new ‘right to be forgotten’.”
Says Walker: “If a company like Google is struggling, imagine what it’s going to be like for mere mortals.”

He adds: “It’s the most contentious part of the legislation. For organisations that have registration information for users – addresses etc. – the key thing is to have one data source, with unique identifiers for user records. Companies need to understand where your data is, how it’s stored, how it’s accessed and searched, who is accessing that data and how the data will be effectively removed when requested.”

Walker concludes: “There’s a lack of awareness – we are going to see a lot more customers invoking the right to be forgotten, so it is important for organisations to ensure that they have those processes in place to deal with this part of the regulation.”

“The impending EU General Data Protection Regulation stipulates that customers must be notified of a data breach without undue delay and the applicable regulator to be notified within a timescale that may be as short as 24 hours,” said Vinod Bange, partner at law firm Taylor Wessing. “The majority of UK organisations don’t have this capability and this is a perfect example of how organisations will need to upscale their readiness against tough new standards.

“The European Court of Justice ruling earlier this year provided that European citizens can ask search engines to remove particular links from online search results, and also established that EU data laws apply in a context that was not previously envisaged, so organisations need to ensure that they have processes in place to address compliance with EU data laws which they may have previously considered as not applicable to them.”
Final thoughts

Awareness is growing among companies that the new EU General Data Protection Regulation will have a significant impact on their businesses, but there is still some way to go, says James Walker. “It’s frightening considering how close it is to being ratified and how little some organisations know.

“Large enterprises are aware they have to be compliant, but smaller organisations don't have the right people looking at it. Ultimately it's the government's responsibility to make sure that business is aware of what this means, but whether that's the UK government or EU government is a key question,” says Walker.

The EU Data Protection Regulation survey

Were you aware of the EU General Data Protection Regulation that has been proposed by the European Commission?

European Total

| YES | NO |
| 64% | 36% |

Breakdown by Country

- Nordic: 60%
- Benelux: 60%
- Germany: 87%
- Poland: 73%
- France: 65%
- Italy: 72%
- UK: 90%
Do you think that a new EU General Data Protection Regulation is required to improve data protection?

52% YES

Do you know when your company would need to become compliant by?

21% YES

Do you think that the proposed EU General Data Protection regulation is realistic for businesses to adhere to?

51% YES
Data Protection Challenges

What are the biggest challenges for your business to comply?

- 30% RESTRICTED BY EXISTING LEGACY IT SYSTEMS
- 31% LACK OF EMPLOYEE AWARENESS
- 30% LACK OF EFFICIENT DATA SECURITY

Are businesses adequately consulted by the European Commission before setting such data protection regulations?

<table>
<thead>
<tr>
<th>YES</th>
<th>MAYBE</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>28%</td>
<td>44%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Being informed

Are you aware that the proposed EU General Data Protection regulation, once ratified, would replace local legislation, e.g. the data protection act in the UK?

- UK 44%
- FRANCE 63%
- BENELUX 49%
- GERMANY 79%
- POLAND 62%
- NORDICS 36%
- ITALY 70%
Five Steps Businesses Should Take Now to Prepare for the EU General Data Protection Regulation

Events over the past couple of years, in particular the Snowden revelations have had a huge influence on how we think about privacy and our personal data. In line with this, the European Union is set to dramatically change the regulations which govern what businesses can do with our data and what rights we have to protect it.

There’s no question this regulation will have an impact on almost every business in the UK, but recently research revealed that only half of UK organisations were even aware it was happening (this compared with 87 per cent awareness in Germany).

In March the European Parliament voted overwhelmingly in favour of introducing the EU General Data Protection Regulation. While there are a number of legislative rivers still to be navigated before it becomes law – we can now say with some certainty that it’s coming, and it’s coming soon. It will cover any company that processes data belonging to a European citizen, regardless of where it’s based. No organisation is exempt, though smaller companies (less than 250 employees) will not necessarily have to comply with some of the tougher requirements, like appointing a data officer.

With all that in mind, we wanted to pull together five steps that every business should be doing right now to ensure that the transition to compliance is as pain free as possible. There are many places to find out further information on the regulations, and we advise you to do as much background reading as you can. Hopefully these thoughts are helpful starting point.

1. Where is it

Hopefully this won’t be too hard to answer, but then again you might be surprised. And it’s important to remember that this is not only digital data. Any data, be it customer, employee or partner data that can be personally identifiable will be covered - regardless of whether it’s stored in a manila envelope or massive server. Find out where documents are stored in the company. Is the storage manageable, secure, insured, easily accessible and well understood?

2. Who can access it

Another set of vital questions: Who’s accessing this data? How are they accessing it and should they be accessing it at all? Are they educated as to the dangers of misusing data? This is also a good time to introduce the concept of a data officer.

Most companies with over 250 employees will be obliged to appoint a data officer who will be in charge of managing all of these issues and ensuring compliance. However, regardless of whether it’s their sole job or not, every organisation should have someone who is responsible for its data policies. Traditionally this has been an IT team function, but surprisingly that’s probably no longer the case. The person in this position should have a good basic technical grounding, but what’s even more important is that they are educated in the legal, procedural and financial implications of managing data.
Chain reaction

It’s not nice to think about, but your organisation should decide ahead of time exactly how it will react if there is a breach. Who is responsible for contacting the authorities, and which bodies need to be informed? Do we even know how to contact the Information Commissioners Office? If the breach is significant enough, who within the organisation will be dealing with press enquiries? How will the news be communicated with customers? And, of course, what is being done to repair the breach and protect the company against further breaches? It’s never going to happen to you until it does. Don’t be the guys that weren’t prepared.

Protection

Ultimately with the best intentions in the world, mistakes get made. There are also plenty of bad guys out there who would more than happily steal your valuable data. So you’ll need to look at the protection technology available, such as:

• Data leak protection solutions that can identify key words and regular expressions like Credit card number, National Insurance numbers etc. in sensitive documents to stop them being sent out
• Encryption technologies so if data is sent out it is still protected
• Advanced threat technology to stop or identify quickly when your network has been breached and stop thieves stealing your sensitive data

It’s also worth looking at some sort of liability insurance to help cover you against damages that may occur.

Education

Sanctions for breaching the rules are significant: the fines could go up to 5% of a non-compliant business’s global turnover, or £100m, whichever is greater. With those kinds of numbers in play, it’s crucial that the whole organisation is aware of the challenges of data privacy. It’s now a board issue. This isn’t some boring techy issue like what mouse shall we get. The whole suite of senior decision makers need to understand the importance of the issue and empower staff to act on it. This might be the toughest task of all.

Honestly though, most of this is all just common sense. If you ask yourself one simple question you shouldn’t go too far wrong: if this was my data would I be happy with how it’s being handled.

There is also a fine line to be tip toed along. Information is vital to everything we do - locking it away and applying overly strict rules on how to access it will stifle your business. However, I believe that there is a middle ground where we can take advantage of the significant opportunities presented by the big data movement, while at the same time respecting and protecting all of our personal data.

If you have any questions or comments on the EU General Data Protection Regulation, get in touch on Twitter: @TrendMicroUK or visit http://www.trendmicro.co.uk/campaigns/eu-data-regulation/index.html
About the research

The research was carried out in April 2014 by Vanson Bourne and surveyed 850 senior IT decision makers across Europe. Specifically, there were 250 respondents in the UK and 100 respondents from each of the following regions: France, Germany, Benelux, Nordics, Poland and Italy. For more information please contact trendmicro@3-monkeys.co.uk

For more information, visit http://www.trendmicro.co.uk/campaigns/eu-data-regulation/

About Trend Micro

Trend Micro Incorporated (TYO: 4704), a global leader in security software, strives to make the world safe for exchanging digital information. Our solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe.

For more information, visit www.trendmicro.com. Or follow our news on Twitter at @TrendMicroUK.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice. Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document.

Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes. Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.