Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Understanding the compliance

Challenges of GDPR

An e-Book publication sponsored by Hewlett Packard Enterprise

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

http://www.complianceweek.com

Hewlett Packard Enterprise

Hewlett Packard Enterprise provides a powerful portfolio of modular solutions for regulatory compliance such as GDPR, secure content management and litigation readiness. With the analytics and automation to help you gain visibility and control of your data, you can: manage data from creation to disposal; simplify legally defensible retention management; and quickly discover relevant data for internal legal or compliance review. With HPE information management and governance solutions, you can understand, manage, and govern the data that matters.

www.hpe.com/software/infogov
www.hpe.com/solutions/gdpr

Inside this e-Book

TalkTalk's massive data hack fine is dire warning

Neil Hodge explores implications from the TalkTalk cyber-attack incident and regulators' bold new moves on cyber-security.

While the threat of a cyber-attack now features prominently on most U.K. company risk registers, regulatory action so far has been fairly low-key. But a recent case has shown that U.K. enforcement agencies are prepared to show their bite when necessary—and that organisations should take heed.

At the beginning of October, the U.K.'s data protection regulator hit telecom company TalkTalk with a record £400,000 (U.S. $319,160) fine for security failings that allowed a cyber-attacker to access customer data "with ease" (the fine has since been reduced to £320,000 (U.S. $255,328) for early payment).

The Information Commissioner's Office's (ICO) in-depth probe found that a cyber-attack on the firm between 15 and 21 October 2015 could have been prevented if TalkTalk had taken "the most basic cyber-security measures" to protect customer data.

ICO investigators found that the attacker took advantage of technical weaknesses in the company's IT controls to access the personal data of 156,959 customers, including their names, addresses, dates of birth, phone numbers, and e-mail addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.

Information Commissioner Elizabeth Denham said that while "hacking is wrong, that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not, and we have taken action."

The data was taken from an underlying customer database that was part of TalkTalk's acquisition of rival phone and internet provider Tiscali's U.K. operations in 2009. That inherited infrastructure contained just three vulnerable webpages that a hacker could exploit to gain access to customer information. A fix had been available to debug the software since 2012, but TalkTalk had not carried out any assessment to check whether there were any vulnerabilities, and so the company did not realise that the installed version of the database software was outdated and was no longer supported by the provider.

The ICO was unimpressed. The easily fixed bug allowed the hacker to bypass access restriction using a common technique known as an "SQL injection." It involves an attacker introducing malicious code into a company's computer programs to change the way that they work. In some cases, it can enable the hacker to take over and control the entire system.

Plenty of other firms have had their fingers burnt by SQL injections. The 2011 "hacktivist" attack on Sony exploited the same vulnerabilities to access the personal details of over 1 million customers, and Yahoo! came a cropper in 2012 when a similar attack resulted in the login details of 450,000 users being exposed. The House of Commons' Culture, Media, and Sport Committee also said that "there had already been three other occasions when the ICO had issued a fine following an SQL attack (the largest of which was £200,000 [U.S. $159,580]), which should have also served as a warning to others, including TalkTalk."

"SQL injection is well understood, defences exist and TalkTalk ought to have known it posed a risk to its data," the ICO investigation found—especially after the company had already had two early warnings (that it failed to detect). The first was a successful SQL injection attack on 17 July 2015 that exploited the same vulnerability in the webpages. A second attack was launched between 2 and 3 September 2015.

"In spite of its expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting," said Denham, adding that the "record fine acts as a warning to others that cyber-security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers."

The ICO's investigation was limited to TalkTalk's compliance with the eight principles of the U.K. Data Protection Act (DPA).

It concluded that TalkTalk breached principle seven of the DPA because it did not have appropriate technical/security measures to protect the personal data it was responsible for, while the fifth data principle was also contravened since it retained customer data for longer than was necessary. A criminal investigation by London's Metropolitan Police Force has been running separately to the ICO's investigation.

The maximum penalty could have been £500,000 (U.S. $395,950) rather than £400,000 (U.S. $319,160). But since the firm did not appeal the decision and paid promptly before 1 November, the amount was reduced by 20 Percent to £320,000 (U.S. $255,328).

The incident has cost the telecom company around £42m (U.S. $34M) and seen its annual profits more than halve. Some estimates have suggested that the costs of the breach are more like £60m (U.S. $48M), which wipes out the company's gross profit of £32m (U.S. $26M) for 2015.

TalkTalk took down its website on 21 October 2015 and informed both customers and the regulator on 22 October—one week after the attack first began. Under the U.K. Data Protection Act (DPA), there is no legal obligation on data controllers to report security breaches—irrespective of how long ago the breach occurred. However, the ICO believes that "serious" breaches should be reported (and promptly), although—yet again—the term "serious" is not defined within the legislation.

In a statement released on 5 October, TalkTalk said that the ICO's decision was "disappointing," especially since the company "had cooperated fully at all times." TalkTalk also pointed out that "there is no evidence to suggest any customers have been impacted financially as a direct result of the attack."

TalkTalk's statement also inferred that the company had been disproportionately treated, as other companies that lost customer's unencrypted financial data received much lower penalties. For example, The Money Shop—a short-term loan company and pawnbroker—was fined £180,000 (U.S. $143,622) in August 2015 for the loss of an undisclosed number of unencrypted customer details (including financial information), while in February 2015 online insurer Staysure.co.U.K. was fined £175,000 (U.S. $139, 633) for the loss of up to 100,000 live credit card details (including security numbers) and medical records, resulting in some 5,000 customers having their cards used by fraudsters. Furthermore, in November 2014 hotel booking website WorldView was fined just £7,500 (U.S. $5,984) after 3,800 customers had their credit card details (including security numbers) stolen by hackers.

However, experts do not share the company's sense of being hard done by. "For many years, when the ICO's focus was on encouraging a culture of data security, the regulator was happy if companies engaged with its investigations and took its recommendations seriously. TalkTalk appears to have believed this would still be the case," says Mark O'Halloran, a partner at law firm Coffin Mew. Halloran believes TalkTalk "was lucky not to be hit with the maximum £500,000 (U.S. $398,950) fine," adding that the penalty "was a very clear signal to companies handling large quantities of people's financial and other sensitive data that they need to pick up their game."

Mark Skilton, a professor of practice at Warwick Business School, also believes that "TalkTalk seems to have got off lightly here," saying that the size of the ICO's fine is "insignificant" in respect of the size of the company's turnover and customer base and "little more than a sting to TalkTalk's finances."

"Even by factoring in the reported numbers of 157,000 personal details and, of those, the 16,000 who had bank details stolen, it still only equates to £2.50 (U.S. $1.99) per head or £25 (U.S. $20) per person who lost banking data," says Prof. Skilton. "The fine seems

to be 'proportionate' to the impact, but shows little regard for the possible risks and lack of due diligence of a company with four million subscribers."

The severity of the hack attack on TalkTalk, had it happened two years from now, could have triggered even more punitive fines from the European Union (EU). Under the long-awaited (and debated) EU General Data Protection Regulation (GDPR), which will come into force in May 2018, the fine could have been much higher: potentially 4 percent of global turnover or €20m (U.S. $17M)—whichever is higher—plus a separate fine of 2 percent of global turnover or €10m (U.S. $9M) for failure to comply with breach notifications. "In the case of TalkTalk, that could have been £72m (U.S. $57.5M) based on 2015 turnover. In that respect, the company has got off lightly," says Gunter Ollmann, CSO of Vectra Networks, a threat management software company.

And according to Emma Wright, commercial technology partner at technology and digital media law firm Kemp Little, signs are that the United Kingdom has every intention of implementing the EU regulation. Karen Bradley MP, the U.K.'s Secretary of State for Culture, Media, and Sport, said at the end of October that the U.K. will be implementing the EU's General Data Protection Regulation (GDPR)—despite leaving the European Union—and will "then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public." ■

PARLIAMENT'S RESPONSE

Below is Parliament's response to the TalkTalk hack:

1: To ensure this issue receives sufficient CEO attention before a crisis strikes, the report recommends that "a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the board."

2: The Committee report says that in major organisations, where the risks of attack are significant, "the person responsible for cyber-security should be fully supported in organising realistic incident management plans and exercises, including planned communications with customers and those who might be affected, whether or not there has been an actual breach."

3: The report also recommends that "companies and other organisations need to demonstrate not just how much they are spending to improve their security but that they are spending it effectively." As a result, the Committee recommends that organisations holding large amounts of personal data (on staff, customers, patients, taxpayers etc.) should report annually to the Information Commissioner's Office (ICO) on:

- Staff cyber-awareness training;
- When their security processes were last audited, by whom and to what standard(s);
- Whether they have an incident management plan in place and when it was last tested;
- What guidance and channels they provide to current and prospective customers and suppliers on how to check that communications from them are genuine;
- The number of enquiries they process from customers to verify authenticity of communications;
- The number of attacks of which they are aware and whether any were successful (ie – actual breaches).

Source: Parliament report on TalkTalk

EU-U.S. Privacy Shield passes: Now what?

It's baaaack: In July 2016, the European Commission formally adopted the long-awaited transatlantic data transfer framework, establishing stringent new data privacy compliance obligations on U.S. companies seeking to transfer personal data from Europe into the United States.

Participating in Privacy Shield is voluntary. For companies that choose to participate, however, any non-compliance with Privacy Shield principles will be enforceable under U.S. law by the relevant enforcement authority, either the U.S. Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT). The U.S. Department of Commerce will begin accepting certifications Aug. 1.

The Privacy Shield replaces the Safe Harbor framework, which the European Court of Justice invalidated in October 2015 in the case of ***Schrems v. Data Protection Commissioner***. That decision effectively meant that personal data transferred from Europe to the United States was no longer presumed to be adequately protected, leaving the more than 4,000 companies that self-certified under the Safe Harbor principles in a state of limbo.

For the most part, all the core data privacy principles in the Safe Harbor remain in Privacy Shield. "Thus, companies that previously certified under the Safe Harbor don't have that much work to do to prepare for Privacy Shield," says James Koenig, a partner and of counsel in the privacy and cyber-security practice at Paul Hastings.

For many other companies that are just thinking about self-certifying under Privacy Shield for the first time, the transition will demand significantly more costs and burdensome data privacy obligations. All companies—even if they self-certified under Safe Harbor—first and foremost need to review and update their privacy policies and procedures.

Under the Choice Principle, Privacy Shield requires companies to provide notice to EU citizens regarding how their data is collected and processed. Individuals must also be provided with the choice to "opt out" when their personal data is to be disclosed to a third party or to be used for a purpose that is "materially different" from the purpose for which it was originally collected. "Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice," Privacy Shield states.

Because privacy policies must disclose the purposes for which data is collected and used, the company has to actually know what those reasons are in the first place. "Unfortunately, a lot of companies historically have inserted language into their privacy policies without really thinking through what it means," says Tanya Forsheit, a partner and co-chair of the Privacy & Data Security group at law firm Frankfurt Kurnit Klein & Selz.

A good starting point is to review that privacy practices actually align with the privacy policy. If the privacy policy spells out certain practices, and Privacy Shield company isn't practicing what it preaches, that could constitute a violation under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices."

Different from the old Safe Harbor, a Privacy Shield company must include in its privacy policy links to both the Commerce Department's Privacy Shield website and a link to the independent recourse mechanism that is available to investigate and resolve complaints, and disclose the right of data subjects to access their data. The Commerce Department has warned that it will be searching for and addressing false claims of Privacy Shield participation.

In the privacy policy, the company must further acknowledge that it is under the jurisdiction of U.S. enforcement agencies, and is required to give personally identifiable information in response to lawful requests from law enforcement. As another change, the company must include a stated acknowledgement about its liability regarding onward transfers.

New principles

One of the most significant provisions establishes accountability regarding the "onward transfer" of personal data. That provision explicitly requires companies transferring data to enter into a contract with the third-party data controller stating that such data may only be processed for limited and specified purposes consistent with individual consent.

Furthermore, third parties that process data on behalf of Privacy Shield companies must guarantee the "same level of protection" as the Privacy Shield companies themselves. If the third-party data processor is no longer able to ensure the necessary level of data protection, it must then inform the certified company.

For companies that were not previously certified under Safe Harbor, they may need to start by mapping their data flows to get a good handle on exactly what data is coming and going: Who are your service providers? What information do those service providers handle? What are you transferring to them?

The final Privacy Shield framework does offer a carrot: Firms that certify within the first two months of the effective date of the Privacy Shield will get a grace period of nine months from the date of certification to bring contracts into compliance; companies that wait until Oct. 1 will need to have all their contracts already in compliance before they can be Privacy Shield certified. "Companies that are interested in Privacy Shield certification will want to move quickly to take advantage of the grace period," Koenig says.

Being Privacy Shield compliant, as under the Safe Harbor, calls for having robust security controls in place. Companies that create, maintain, use or disseminate personal information must take "reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction," the Privacy Shield states.

A stricter limitation has also been placed on data processing by requiring companies "not to process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual."

The Privacy Shield makes more explicit the limitations on data retention provisions by stating that companies may retain personal data only for as long as it serves the purpose for which it was initially collected, a requirement that for mature companies shouldn't be too burdensome.

EU citizens will have multiple avenues through which they can seek recourse from those that may have violated their rights under the Privacy Shield, increasing the prospect for more liability, including

more enforcement actions and greater accountability.

For example, the Privacy Shield encourages individuals to raise any concerns with the company itself, which must have in place a free-of-charge Alternative Dispute Resolution mechanism, and must respond to any complaints within 45 days. Although many companies already have a dispute resolution mechanism in place, those that don't will now have to decide what independent dispute resolution body they want to use.

EU citizens can also go to their national data protection authorities, who will work with the Commerce Department and FTC to ensure that unresolved complaints are investigated and resolved. If a case is not resolved by any of the other means, individuals will have the option of a "prompt, independent, and fair mechanism" to resolve claimed violations of the principles not may not be resolved by any of the other Privacy Shield mechanisms.

Given that many U.S. companies try to insert arbitration provisions into their consumer contracts as a way to stay out of court, this should be a welcome option. "When the dust settles and the business community steps back, they're going to realize they actually like this provision," Zetoony says.

The final version of the Privacy Shield clarifies that the U.S. ombudsperson—a position that has been established to oversee complaints—must be independent of U.S. intelligence agencies. In this regard, the final framework states that the ombudsperson will be able to rely on independent oversight bodies with investigatory powers—such as the Inspector Generals or the Privacy and Civil Liberties Oversight Board.

The first step is deciding whether it's in the company's best interest to self-certify to Privacy Shield, whether a company previously certified under the Safe Harbor or not. The answer depends on a number of factors, including: the maturity of the data compliance mechanisms (such as model contracts and biding corporate rules) the company has in place; the maturity of the company's data privacy program; the scope of the company's global footprint; the level of exposure the company has to EU citizens; the company's overall regulatory profile; and the company's current state of third-party contracts. The next step would be to have an actual action plan to become Privacy Shield certified. Koenig recommends a five-step checklist:

» Develop and maintain a privacy policy based on Privacy Shield principles.
» Validate security safeguards with a customized security questionnaire deployed to system, application and interface owners who handle data that are subject to the certification.
» Address onward transfers by review and revising existing contracts for third-party vendors and other onward transferees.
» Update training for employees who have access to EU citizen data.
» Compile within a single compliance binder documentation that supports the company's Privacy Shield certification—such as policies, a gap assessment report, and contract addendums.

If firms wish to transfer HR data, they will have to indicate that separately in their self-certification submission and include details, such as their HR privacy policy. Unlike the Safe Harbor, companies transferring HR data will have to agree to cooperate with EU data protection authorities in connection with complaints from data subjects regarding HR data.

Many companies may be reluctant to become Privacy Shield compliant because they don't want to pour time and resources into a framework that could suffer the same fate as the Safe Harbor: invalidation.

"The biggest concern is the uncertainty," says Cynthia O'Donoghue, a partner and law firm Reed Smith and leader of the firm's international information technology, privacy & data security team. "Most of what I'm hearing is that companies want to take a wait-and-see approach."

Even if Privacy Shield is challenged in European courts—and further complicated by Brexit if the U.K. adopts its own approach to data privacy—waiting is not the answer. First, companies deferred prosecution because of uncertainty around the Safe Harbor, then Privacy Shield, and now some companies are deferring data privacy compliance even further as they wait for EU member states to implement the provisions of the General Data Protection Regulation (GDPR), Zetoony says. "You can't put off compliance forever," he says.

For any U.S. company that collects and handles data on EU citizens, the time to review privacy policies and practices and contracts with service providers and customers is now. "It's not too soon to be thinking about GDPR compliance," says Kendall Burman, cyber-security and data privacy counsel at law firm Mayer Brown. "We've been advising folks to think about them in combination, to think about Privacy Shield as being an additional step toward GDPR regulations." ■

Hewlett Packard
Enterprise

GDPR:

7 questions CIOs must answer to achieve compliance

Time is running short. Enforcement of General Data Protection Regulation (GDPR) begins in May 2018 and penalties are severe: Up to **€20 million or 4%** of the preceding year's worldwide turnover. Don't let GDPR compliance slide to the bottom of your priority list.

Here are the top seven questions to ask yourself now:

1.

What is my readiness status?

- Raise internal awareness now to get resources on board for GDPR implementation.
- Launch a group-wide risk assessment to gauge your company's preparedness level, including technology facilities, under existing National and EU regulation.

2.

Where is the information and sensitive PII that will fall under these regulations?

GDPR Articles: 5, 24; GDPR Recital 74

- Information in any format must be addressed: hard copy, audio, visual and alphanumeric.
- You should be able to unify records to provide a 360-degree view of a private customer.
- Understand data flows—where is sensitive data used and moved between databases and applications.

3.

How can I cost-effectively respond to legal matters requiring information under my management?

GDPR Articles: 79, 58; GDPR Recital 122, 123, 143

- Ensure legal policies and procedures are in place to meet requirements.
- Evaluate the technology used to isolate information required by in-house counsel as well as compliance and risk officers.
- Determine whether internal or external counsel will handle breach reporting.

How can I best ensure sensitive data is protected, stored and backed up securely?

GDPR Articles: 6, 32, 33, 34, 83

4. 

- Evaluate the effectiveness of my total records management.
- Determine whether my existing backup safeguards PII.
- Review my retention policy enforcement for the defensible deletion of data.

---

5. 

How can I identify information for disposition, in accordance with the "right to be forgotten?"

GDPR Articles: 4, 15-22, 24; GDPR Recital 59, 63-71, 74

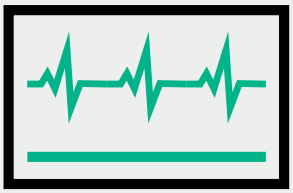
- Gain legal advice as to how PII is defined.
- Deploy a policy enforcement tool.
- Establish a process that can be monitored and audited for compliance.

Can I report a breach within the timeline required by the EU data protection regulation?

GDPR Articles 33, 34; GDPR Recital 85, 86, 87, 88

6. 

- 72 hours is a tough target to reach. A comprehensive and defensible policy and system needs to be in place.
- The security breach alerting mechanism must be provided in the form of technology-assisted monitoring.
- Well-trained compliance staff is needed to use technology and report as required to national Data Protection Regulators.

7. 

How can I reduce my overall risk profile?

GDPR Articles: 5, 24; GDPR Recital 39, 74

- Perform a sound and rigorous risk assessment of policy, procedure and technology.
- Invest in technology as required to achieve risk reduction.
- Establish both proactive defense and post-event handling to protect corporate reputation and avoid both fines and business-limiting criminal enforcement.

Preparing for the EU's new data protection rule

The European Parliament has greenlit an EU-wide cyber-security initiative that will impose new compliance rules on firms across the board. But, asks **Jaclyn Jaeger**, will CCOs feel these are helping protect the company or adding more regulatory liability?

For any U.S. company that collects and handles data on citizens of the European Union and doesn't think EU data privacy laws apply to you, think again.

After nearly four years of back-and-forth negotiations, the European Parliament and Council of the European Union in 2015 approved a final draft of the EU General Data Protection Regulation (GDPR), backed by the European Parliament's Civil Liberties, Justice & Home Affairs Committee. Once it's officially adopted, which is expected to take place this spring, member states will have two years to implement its provisions.

Designed to bring EU data protection laws into the digital age, the GDPR will replace the current EU Data Protection Directive, enacted in 1995, marking the most sweeping changes to EU data privacy legislation in the last 20 years. "It's an entire revamping of the data protection legislative framework," says Neal Cohen, an associate in privacy and security practice at Perkins Coie.

Although the GDPR imposes several new compliance obligations on companies, the overall outcome will be a uniform approach to EU data protection laws, "which could make things logistically easier for companies operating across multiple EU jurisdictions," says Courtney Bowman, an associate with law firm Proskauer.

One of the most significant changes is the global scope of the GDPR's application. Under the current Directive, only companies physically located in Europe may be found liable for data privacy violations. The GDPR, in comparison, would make any company—even those outside the European Union—liable so long as it offers goods or services to individuals in the European Union, or that monitors the behavior of EU citizens.

For U.S. companies that weren't previously obligated to comply with the EU's data privacy regime, the GDPR "may come as a bit of a shock," says Rohan Massey, partner and co-chair of the privacy and data security practice at Ropes & Gray in London. The GDPR broadly defines personal data as employee, customer, and supplier data, "all of which need to be treated with the data protection framework in mind," he says.

Given that most companies use behavioral advertising as part of their business model, the GDPR would bring just about every company in every industry sector within its scope. "It's a game changer, primarily because it sets standards that many companies haven't had to worry about," Hilary Wandall, associate vice president of compliance and chief privacy officer at global healthcare giant Merck, said during a panel discussion at the EU Data Protection conference in Brussels.

The scope of European data protection laws has been expanded in another significant way: whereas the current Directive applies only to data controllers (companies that decide how and why data is being collected), the GDPR will jointly hold liable data processors—essentially service providers—as well.

Penalties for non-compliance are now more se-

vere than ever. Companies that don't meet the new requirements can face fines up to 4 percent of total annual global revenue or €20 million ($21.5 million), whichever is higher. For corporate giants like Apple, Facebook, and Google, fines can potentially amount to billions of dollars.

Data Minimization

Many U.S. companies may have to completely overhaul their data collection and data removal programs to become GDPR-compliant by the 2018 deadline. One requirement posing significant compliance obstacles for companies, for example, is the "right to be forgotten," which requires companies to scrub personal records from all company systems upon request, and then prove that the information has been deleted permanently.

Specifically, individuals can request that their personal data be erased "without undue delay" when it's no longer needed for the purposes for which it was collected or processed, or if individuals withdraw consent or objects to the processing, and there are no legitimate or lawful grounds for retaining the data. "The actual requirement to have to erase data is fundamentally problematic," said Wandall.

Recent reports indicate that many companies still have a long way to go. According to a survey conducted by Blancco Technology Group, for example, 41 percent of 511 IT professionals polled around the globe said that they don't maintain documentation of the defined processes used to remove outdated or irrelevant customer data, and 60 percent said it would take one year or longer to develop and implement the necessary IT processes and tools to pass a right to be forgotten audit.

Consent must be "freely given, specific, informed, and unambiguous." Examples include ticking a box when visiting a website or by another statement or action clearly indicating acceptance of the proposed processing of the personal data. No response, pre-ticked boxes, or inactivity will not constitute consent, the European Parliament said.

The GDPR also establishes a right to data portability, allowing individuals to request, where technically feasible, that the data controller transfer personal data to another service provider.

Both requirements demand that personal data be readily accessible in the event that data users make such requests. "It's not just sitting all in one location," Barbara Sondag privacy counsel for North America and global product at eBay, said during the panel discussion.If you don't already have one, now is the time to organize an internal taskforce made up of stakeholders from across the business—management, IT, legal, compliance, marketing, HR, finance—and across geographies to figure out how to map all that data.

Pat Clawson, CEO of Blancco Technology Group, a provider of data erasure solutions, recommends that companies create and maintain a detailed register of all physical and virtual places where data is held—whether by the business, customers, employees, and third-party suppliers or vendors. "Distribute and communicate all items in this list with all internal departments and stakeholders," he says.

The GDPR also introduces the concept of "privacy by design," requiring that data protection and privacy controls be considered from the outset.

"It's a game changer, primarily because it sets standards that many companies haven't had to worry about."

Hilary Wandall, Chief Privacy Officer, Merck

From a practical standpoint, complying with the GDPR necessitates far more than a box-ticking exercise on data minimization requirements; it means embracing a whole new mindset. "If you're not as a company thinking holistically about privacy and data protection—how it's embedded into the business—then you're not prepared," Wandall said.

Data Protection Officer

The data protection rule additionally requires the appointment of a data protection officer among companies whose "core" business activities include large-scale processing of "special categories" of personal data. The GDPR broadly defines "special categories" of data as information that reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, or sexual orientation.

"Companies should be aware that even if they do not collect this type of information from their customers, they may collect some of this information from their employees for human resources purposes," says Bowman.

Companies will need to consider the required skills of the data protection officer role, and then determine whether to recruit someone in-house or if they will need to recruit someone externally. Keep in mind, the data protection officer will serve as the main point of contact for communications with the relevant supervisory authority.

On a positive note, the GDPR introduces a "one-stop shop," meaning that companies that handle the personal data of EU residents in multiple EU member states will only have to contend with one "lead" data protection authority (generally the authority for the member state in which the company has its EU headquarters).

Until companies have guidance on how the GDPR will be enforced, "it may be prudent to avoid costly external audits and the creation of new policies or data control processes," says Massey. "It would be foolish to leap forward only to have to rework later." ■

PREPARING FOR EU DATA PRIVACY

Below David Smith, deputy commissioner & director of data protection at the Information Commissioner's Office, says what firms should be looking at to prep for the GDPR.

Consent and control: How far do you give your customers genuine control over what information you keep about them and how you use it? If you're relying on their consent, do they know that they are consenting and the implications of this? This is especially pertinent if they are children. Can they easily say no or withdraw their consent later on?

Accountability: Do you have effective processes in place to ensure that you are data protection compliant? Can you explain what these are and demonstrate that they work in practice? Can individuals easily find out not just what information you hold about them and how you might use it but also more generally about your personal data handling practices?

Staffing: It may not be clear yet whether you'll be required to designate a Data Protection Officer but even so, do you have the right people in place to help you understand and meet the requirements of the Regulation? If not, do you at least have some idea where you might get the necessary expertise from? It's a myth that the Regulation will require every business to recruit a Data Protection Officer, but they will need resources to help them deliver the necessary change, even if these resources come through training and developing existing staff.

Privacy by Design: What steps do you take to make sure that your systems and processes, particularly new ones, deliver data protection compliance as a matter of course? Are you reviewing the personal data you hold and why you hold it to ensure that you can meet the requirement for 'data minimization'? Do you know what a privacy impact assessment is?

Source: Information Commissioner's Office

SUMMARIZING THE GDPR

Below are some statistics from TRUSTe on how firms are preparing for the European Union GDPR.

Executive Summary

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.

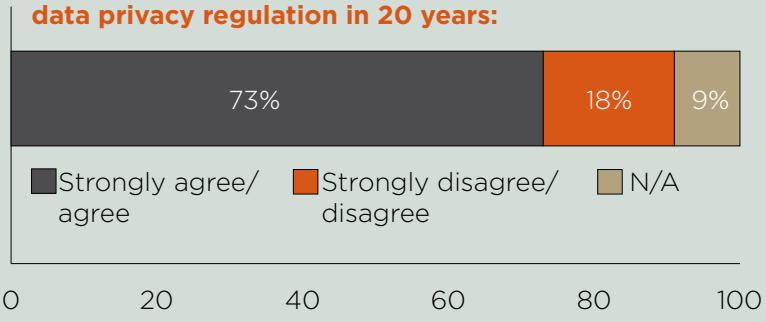
Of those aware of the GDPR, two thirds (65%) are starting to prepare even before the law is finalized. 83% had already allocated budget with 21% allocating $0.5 million or more to address the changes and 56% placing this currently 'High' or 'Very High' on their Corporate Risk Register.

Even though this survey wa 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:



Source: TRUSTe

Advice for U.S. companies, post-Brexit:

KEEP CALM AND CARRY ON

Joe Mont has more on what the United Kingdom's vote to leave the EU means for U.S. companies with a multinational presence.

It is a truism that business hates uncertainty. It was therefore no surprise to see bold proclamations regarding the United Kingdom's planned exit from the European Union, the so-called "Brexit" vote in June.

Such talk may be a bit premature. Buyer's remorse among some Leave voters sparks a long-shot prospect for a second vote. It also remains to be seen when the U.K. will formalize the split and how the months-long negotiations to do so will unfold. That process could have a tremendous effect on companies that do business throughout Europe.

The message for U.S. companies that do business throughout Europe, to use a very British phrase: Keep calm and carry on.

"This could be much ado about nothing," says Ashley Craig, co-chair of the law firm Venable's international trade group. Nevertheless, companies are asking for clarification that no one can give.

"U.S. companies want consistency," Craig says. "They want some sort of stability, but we are not going to get that right away. In the meantime, they need to be cautious and practical and monitor what's going on."

Amid chatter by bank holding companies that they may relocate to Dublin, Frankfurt, or a number of other countries, Craig suggests not worrying about such a scenario just yet. "A lot of what is going on right now is more rhetoric than reality," he says, pointing out that it will be hard to leave London, built-up over the past 25 years as one of the world's international financial hubs.

Craig's pitch for rationality, however, isn't meant to mask very real challenges that may be ahead for U.S. firms operating from the United Kingdom.

A key reason many U.S. companies establish in the United Kingdom is its access to other EU and third-country markets through Customs Union and Free Trade Agreements (FTAs), he says. Upon exit, the United Kingdom will likely lose preferential access, and exports of U.S. businesses from the United Kingdom may be subject to duties and other taxes. While the U.K. will likely negotiate an FTA with the European Union, doing so will take time and probably not match the level of preferential access that currently exists. As a result, many U.S. manufacturers currently operating in the United Kingdom may eventually want to establish themselves in other EU Member States.

"The British are going to have to quickly stand up an entire trade authority which they haven't had to do in generations," Craig says. "On top of it, they are going to have to go about negotiating multilateral trade agreements around the world. That's not a slam dunk and it is certainly not something that can be expedited. Practically speaking, it is not going to affect the day-to-day trade flow, but it is a long-term concern."

Of the financial institutions and insurance companies that currently operate from the U.K., many do so because "passporting" enables them to provide services across the EU. Unless otherwise agreed between the European Union and the United Kingdom, this will no longer be an option after the latter's exit, Craig says. Firms might then consider leaving the UK as a whole and establishing themselves in other EU countries, such as France, Germany, Ireland or the Netherlands.

Access to human capital is another concern that Craig highlights. Many U.S. companies enjoy access to a large pool of qualified employees from other EU countries, whose citizens are largely free to work without borders and visas. If free travel for workers is restricted, U.S. companies will face a labor and talent shortage unless they maintain both a U.K. and EU presence.

What will be among the more challenging matters for American companies amid a European divorce are issues of data privacy and protection.

Europeans, as evidenced by the difficulty obtaining a comparable compliance regime with U.S. companies, may see their own regulatory regime splintered by a U.K. exit. That doesn't mean, however, that American enterprises can stop worrying about rigid new data privacy rules that become effective in May 2018, which will affect any company that collects and handles data on citizens of the European Union.

In January the European Parliament and Coun-

cil of the European Union approved a final draft of the EU General Data Protection Regulation (GDPR). It will replace the current EU Data Protection Directive, enacted in 1995, and impose compliance obligations on any company—even those outside the EU—that offers goods or services to individuals in is Member States, or that monitors their behavior. Companies that don't meet the new requirements can face fines up to 4 percent of total annual global revenue or €20 million ($21.5 million), whichever is higher. For corporate giants like Apple, Facebook, and Google, fines can potentially amount to billions of dollars.

When the U.K. has to put its own rules in place, do they follow the GDPR or come up with something a little more business-friendly?" Craig asks. "How far does the U.K. go to match the rest of the EU to be deemed adequate? How far do they want to go to match the GDPR?

Despite the Leave vote, "it is vitally important that the controllers and processors of personal data do not fall into the trap of thinking that GDPR no longer matters to them," says Stewart Room, co-leader of PwC's Global Privacy Centre of Excellence. "Compliance with the standards of EU data protection law will be a 'red line' requirement for the U.K.'s continuing access to the single market."

While the United Kingdom (always more business-friendly in its approach to data issues) could create its own rules, the GDPR will likely become effective before its split is finalized. If the United Kingdom is still a part of the European Union in May 2018, the new law will apply automatically, exposing non-compliant organizations to a risk of high regulatory fines for non-compliance, as well as new forms of litigation risk.

"It is certainly a possibility that the U.K. will pass legislation to give effect to the GDPR," Room adds. "Failure to do so will not only lock out the U.K. from the single market, but it will effectively prevent any form of business with the EU where personal data is involved. That would be a disaster for multinationals that operate in both the European Union and the United Kingdom. It would also mean UK citizens would not receive privacy protections and civil liberties equivalent to those on the continent.

Any organization based in the United Kingdom that wants to engage with the EU, whether or not as part of the single market, needs to continue with their preparations for the GDPR, he advises.

"Not only is the GDPR still as relevant as before for American companies with U.K. operations, but the uncertain nature of the U.K.'s adoption of it is an added reason for them to get C-suite visibility into their GDPR implementation roadmaps," says Jay Cline, co-leader of PwC's Global Privacy Centre of Excellence. "American companies that are considering changing the headquarters of their EU operations from London to a German city should first perform a complete cost-benefit assessment of how Germany's stricter approach to data privacy could impact their entire enterprise architecture."

First there was the U.S.-EU Safe Harbor, then the EU-U.S. Privacy Shield, and now there may be the EU-U.K. Privacy Shield as well, says Aaron Tantleff, a lawyer in the privacy, security and information management practice at Foley & Lardner.

"Shouldn't the U.K. be subject to the same security with respect to compliance with EU data protections laws, including the upcoming GDPR? The UK will now get to experience the same joys as the U.S. in ensuring the protection of the personal data of EU citizens," he says. "The basic premise of GDPR and the 'harmonization' of data protection laws across the entire European Union just went out the window.

"I would be lying if I claimed this to be anything but a fundamental shift of the flow of personal information across Europe," Tantleff says. "That said, the sky is not falling and Chicken Little has not been hit over the head with bits of data. While there are more questions than answers at the moment, for now the sky remains clear, though I would carry an umbrella just for protection."

Regardless of what happens, any company, located in the United Kingdom, United States, or elsewhere, that is collecting, processing, or storing personal data of EU citizen will still have to comply with the laws of the European Union, including GDPR, or will be subject to significant fines, he adds. The unfortunate side effect: "The cost of compliance will go up."

"At the end of the day you are still trading with the rest of the EU and you are still collecting information on its citizens," he says.

Efforts to harmonize international financial regulations have also been a long-evolving process, in particular as the U.S. and EU look to realize regulatory adequacy and "substituted compliance" between

their derivatives regimes. The U.K. exit could affect that scenario as well.

"From a financial services perspective, the key issue will be whether the U.K. can continue to maintain at least partial access to the EU market for financial services," says Peter Green, a London-based partner with Morrison Foerster. Various scenarios could unfold as the U.K. strikes out on its own, but it remains to be seen if it remains part of the European Economic Area (EEA) and its free trade agreements.

That participation would preserve the single market for financial services, he says. "The 'big but' is that the U.K. would need to continue contributing to the EU budget and accept most of its rules regarding movement across the economic area. Politically, that would seem pretty unlikely. What is more likely is that the U.K. will exit both the EU and the EEA. We will then see some sort of negotiated free trade."

The effect on U.S. firms based in the United Kingdom that are conducting business across the EU will depend on the nature of how those negations proceed and whether "passporting" is retained. Similarly, the forthcoming Markets in Financial Instruments Directive II, a framework for supervision and oversight of firms providing financial services across the European Union would complicate matters. U.S. companies in the United Kingdom may need to relocate if the United Kingdom's own regime doesn't meet its standards for "substituted compliance" across the remaining Member states. ■

ALL ABOUT GDPR

The following is from a fact sheet, issued by the European Commission, on the General Data Protection Regulation—new rules that apply to non-European countries that do online business in Member States. Compliance begins in 2018.

What will change under the Regulation?

The Regulation updates and modernizes the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on: reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The changes will give people more control over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected—no matter where it is sent, processed or stored even outside the EU ...

What are the benefits for citizens?

The reform provides tools for gaining control of one's personal data, the protection of which is a fundamental right in the European Union. The data protection reform will strengthen citizens' rights and build trust. Nine out of 10 Europeans have expressed concern about mobile apps collecting their data without their consent, and seven out of ten worry about the potential use that companies may make of the information disclosed.

Right to be forgotten: How will it work?

Already the current Directive gives individuals a possibility to have their data deleted, in particular when the data is no longer necessary.

For example, if an individual has given her or his consent to processing for a specific purpose, e.g. display on a social networking site, and does not want this service anymore, than there is no reason to keep the data in the system. In particular, when children have made data about themselves accessible, often without fully understanding the consequences, they must not be stuck with the consequences of that choice for the rest of their lives.

This does not mean that on each request of an individual all his personal data are to be deleted at once and forever. If for example, the retention of the data is necessary for the performance of a contract or for compliance with a legal obligation, the data can be kept as long as necessary for that purpose ...

Source: European Commission