I am pleased to present the Summer 2016 edition of Willis Towers Watson’s Cyber Claims Brief.

Dominating the headlines earlier this year was a legal standoff between the U.S. government and one of the world’s leading technology companies over whether the government could force the technology company to unlock an encrypted smartphone that belonged to an alleged terrorist. The standoff intensified the debate over a government agency’s authority weighed against privacy and security concerns. Lisa Nabipour-Sheldon and Ropes & Gray LLP attorneys, Seth Harrington and Kevin Angle, have collaborated to explore various potential liability issues and insurance coverage implications that may arise when companies are directed by governmental authorities to take action (or not) in connection with a cybersecurity event.

We often describe the cyber liability landscape as dynamic. The past six months since our last edition has been no exception. Dan Twersky explains why cyber extortion – and ransomware attacks, specifically – have become an increasingly popular and favored tool of hackers worldwide and discusses the unique exposure presented as well as how companies may mitigate these threats.

What remains a major driver of cyberattacks is the human element, particularly employee negligence. Anthony Rapa takes an in-depth look at the role employees play in creating cyber risk and how emerging technology, BYOD and the changing workforce may create further avenues for employee error.

Through the first half of 2016, we observed a substantial increase in the adoption and implementation of incident response plans. Because vendor selection is a key component of an incident response plan, and many clients continue to struggle with this issue, Kristin Zieser offers sound guidance regarding this process, as well as solutions to the insurance coverage issues that may arise.

Finally, while the potential effects of the recent Brexit vote are being closely monitored by Willis Towers Watson’s European Task Force, Glyn Thoms, FINEX UK Cyber Practice Leader, and Hunton & Williams close out this edition with a thorough analysis of the recent General Data Protection Regulation, which provides consistency in the application and enforcement of data protection laws across the EU, as well as the recently approved EU-US Privacy Shield.

We hope you enjoy reading this edition. As always, we look forward to your comments and feedback.
Defending against cyber liability claims arising from cooperation with law enforcement requests

by Seth Harrington, Esq.
Kevin Angle, Esq.
Lisa Nabipour-Sheldon

Recent criminal investigations have brought law enforcement into conflict with technology companies over the encryption of customer data. Most notably, earlier this year, as part of its investigation into the San Bernardino shooting that killed 14 people, the Federal Bureau of Investigation (FBI) sought to force Apple to unlock an iPhone used by Syed Rizwan Farook, the alleged gunman. Apple resisted, arguing that once such a backdoor was created, “the technique could be used over and over again, on any number of devices,” putting its customers’ data at risk.¹

The questions raised by this and other disputes involving cooperation with the government could impact a variety of companies. In the digital age, many companies are asked by law enforcement to provide access to customer information or information about their security controls. This increased attention on electronically stored personal information and its use in criminal investigations is reflected in recent legislative activity.

To provide a mechanism for private sector entities to share cyber threat indicators with the Department of Homeland Security and, more broadly, the federal government, the S.754 Cybersecurity Information Sharing Act of 2015 (the Cybersecurity Act) was recently enacted. Significantly, Section 106 of the Cybersecurity Act provides that “[n]o cause of action shall lie or be maintained in any court against any private entity” for the “monitoring of an information system” or for the “sharing or receipt of a cyber threat indicator or defensive measure” if the sharing or receipt is conducted in accordance with the Act.² In other words, a company, such as Apple, cannot be sued if its monitoring of communications or sharing or receipt of threat information falls within the protection of the Cybersecurity Act.

The Senate Judiciary Committee is currently evaluating a bill — the Email Privacy Act — which would amend the Electronic Communications Privacy Act to require a warrant before a provider of remote computing or electronic communication services could provide stored content to a governmental entity. The Committee is also considering proposed amendments that would make exceptions to the warrant requirement for civil investigations and emergency circumstances.

As is often the case, reputational loss is one of the more significant costs that may be incurred by a company known to have cooperated with law enforcement or governmental efforts to obtain access to information (or to obtain the means to access information). Customers may assume, rightly or wrongly, that the company put their data at risk. But the further costs associated with a potential lawsuit over that cooperation — whether meritorious or not — should not be discounted.

Possible theories of liability

Customers could assert multiple theories of liability, similar to the types of claims typically brought in class action litigation following a data breach. These theories of liability include breach of state consumer protection statutes, negligence and breach of contract. For example, plaintiffs could assert that by providing law enforcement with the tools to exploit vulnerabilities in the company’s software, the company unfairly subjected customer data to the risk of breach, or that the company violated express or implied promises in their consumer contracts regarding data security. Such claims may ultimately be found unmeritorious, but if the claim survives a motion to dismiss and proceeds to discovery, the cost of the ensuing litigation could prove substantial.

Potential defenses

Because of the inherent risks in such litigation, it is important to keep in mind some of the grounds for dismissal that may be available to companies facing such scenarios. As with most data breach claims, a company should consider arguing that the plaintiffs lack standing. In order to have standing to sue in federal court under Article III of the U.S. Constitution (and in many state courts as well), plaintiffs must show that they have suffered, or face a sufficiently high risk of suffering, a concrete injury. Recently, the United States Supreme Court in Spokeo, Inc. v. Robins confirmed that a plaintiff must meet this requirement even when alleging violation of a federal statute for which Congress has provided a statutory damages remedy.

However, since such cases would likely arise in cases involving national security, other unique defenses may also be available. For example, companies could argue that since they provide an exploit or access to data at the request and direction of the government, they should be immunized under the government contractor defense (or government contractor immunity).³ The defense may be invoked where state tort law would create a significant conflict with a “unique federal interest”⁴ and shields contractors from state law.
Therefore important for organizations to work with their insurance broker and insurer(s) to determine what may suffice in the way of a non-descriptive notice, or a pre-authorization to withhold notice until permitted to do so by the government.

Another example of a potential coverage implication is when the involved government agency does not work to eradicate the threat actors, but instead directs the affected organization to allow the agency to monitor and study the hackers’ movements. While the government agency may be interested in delaying notification in order to gather intelligence that may be helpful to them in identifying future and possibly unrelated threats, the insurer may take the position that such monitoring costs are not within the scope of coverage.

The above scenarios are examples of instances where government involvement may not only present additional potential liability to organizations, but may also impact any applicable cyber liability insurance coverage. Because cyberattacks continue to pose a major threat to national security and the economy, we expect that government agencies’ involvement in how organizations respond to cyber threats will only increase. Accordingly, buyers of cyber liability insurance should consider the additional expense and exposure associated with the government’s involvement when making decisions regarding adequacy of limits, as well as the notice provisions in their policies.

Potential insurance coverage implications

Aside from the legal and reputational risks associated with the circumstances described, there are also potential insurance coverage implications. These implications could arise in claims involving suspected terrorism as well as in the typical run-of-the-mill hacking incidents that result in some form of governmental intervention. For example, in the wake of a network intrusion, the involved government agency may direct the affected organization not to disclose any information — even the fact that the incident occurred — to an outside party. This would include the impacted organization’s cyber liability insurance company, whose policy very likely requires notification of such an incident “as soon as practicable,” or some language to that effect. To avoid breach of the notice provision of most cyber liability insurance policies, it is therefore important for organizations to work with their insurance policies.

1 Tim Cook, Customer Letter (Feb. 16, 2016).
2 https://www.govtrack.us/congress/bills/114/s754/text.
3 The defense was first articulated in Boyle v. United Tech. Corp., 487 U.S. 500, 505-06, 512 (1988).
4 See, Hudgens v. Bell Helicopters/Textron, 328 F.3d 1329, 1334 (11th Cir. 2003).
5 To assert the government contractor defense, a defendant must show that: (1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3) the supplier warned the United States about the danger in the use of the equipment that were known to the supplier but not to the United States.” Boyle, 487 U.S. at 505-07, 512.
6 See Bennet v. MIS Corp., 507 F.3d 1076, 1089-90 (6th Cir. 2010) (finding it plausible that government contractor defense could be applied to protect mold remediation firm hired by the FAA); Hudgens, 328 F.3d at 1334 (applying government contractor defense to contract for maintenance of army helicopters).
7 Cabalce v. VSE Corp, 922 F. Supp. 2d 1113, 1125 (D. Hawai‘i 2015). The doctrine arises from the Supreme Court’s decision, Yearsley v. W.A. Ross Construction Co., 309 U.S. 18 (1940) and has two elements: a company generally must show that (1) it “was working pursuant to the authorization and direction of the federal government,” and (2) “the acts of which the plaintiff complained fell within the scope of those government directives.”
Cyber extortion is the new hack

by Dan Twersky

2014 was the year of the retail data breach, 2015 was the year of the health care data breach, and, thus far, 2016 is the year of cyber extortion.

Cyber extortion can generally be described as a threat to attack/disrupt a computer system or to publicly release confidential information for the purpose of demanding something — usually money — from the targeted company. No segment of cyber extortion has seen as meteoric a rise as ransomware, a form of malware installed on an unsuspecting computer user’s system, holding that system or specific files hostage until a ransom is paid. Bitcoin is the currency most commonly demanded, as it is difficult to trace and not controlled by any particular country. Ransomware infection commonly occurs after an individual falls victim to a social engineering scam and opens an attachment or clicks a link within what appears to be an innocuous and legitimate email message.

Historically, ransomware attackers strategically targeted individuals and small businesses, demanding relatively small amounts of money. For businesses, the ransom sought was nuisance value, which encouraged the business to pay the hackers thereby avoiding the hassle and expense of engaging in-house or outsourced IT professionals to unlock the data. Law enforcement has also typically recommended that businesses pay the ransom, particularly if a backup of the data does not exist. This common guidance may have unintentionally assisted a criminal industry with low barriers to entry. A recent white paper by Web intelligence firm Flashpoint, which tracked a specific ransomware operation based in Russia, estimates that the average “ransomware boss” nets approximately $90,000 annually and pays his or her team members (a/k/a “affiliates”) about $600 a month, with an average ransom amount of $300 per attack.

But the stakes were raised this year — and significantly so. First, ransomware has become far more sophisticated. Not only is certain malware able to quickly identify the most critical files on a network to encrypt, it can also successfully delete backups. Second, attacks appear to have spiked against certain high profile industries, such as health care, which is particularly vulnerable to a ransomware attack because an inability to access critical information could endanger the lives of patients. In two recent well-publicized incidents, a large hospital paid approximately $17,000 in Bitcoin (negotiated from a reported initial demand of over $3 million), while another hospital was able to restore its network and data within five days via its backup system without paying the demanded ransom.

Mitigating cyber extortion incidents

What can organizations do to prevent or mitigate cyber extortion attacks? Once ransomware has successfully infiltrated an organization’s network, the most important step is not to panic. In addition to informing law enforcement and providing notice under any applicable insurance policy, organizations should engage their attorneys and computer forensic teams to: (1) determine if the threat is legitimate, (2) determine whether or not data at issue has been backed up, and (3) ensure that the malware has not led to the compromise of confidential information.
The human element in cyber extortion

Organizations continue to underestimate the value of employee cybersecurity awareness training — a critical component of cyber risk mitigation strategy. It is well-documented that the overwhelming majority of ransomware attacks are the result of employees being tricked into opening malicious email attachments and/or clicking on fraudulent links. Studies consistently show that employers who regularly test employees with mock phishing campaigns are able to significantly reduce the percentage of initiated clicks. As highlighted in a recent Willis Towers Watson survey, workforce culture, particularly training, plays a significant role in an organization’s susceptibility to data breach.

Insurance coverage implications

There are several potential coverage gaps to avoid and there are creative ways to best leverage overlapping and complementary insurance coverages. One thing that makes ransomware and other types of cyber extortion unique is the inaccessibility of critical and/or confidential information, rather than the theft of information, typically involved in those attacks. Thus, while the most common goal of ransomware attackers is to obtain the negotiated ransom for release of the information, such attacks can trigger every aspect of coverage, including cyber extortion, under a cyber liability insurance policy.

Cyber extortionists generally keep up their end of the bargain, either by providing a decryption key to unlock the ransomware, or by not disclosing confidential information in their possession, ending the attack. Occasionally, however, the attack may take a number of different directions, resulting in unintended consequences and loss. For example, the malware initially uploaded onto the victim’s computer system may also have penetrated the network to access and exfiltrate confidential information to the attackers. Such a scenario would likely create an obligation on the part of the company to notify the individuals whose information may have been compromised. It could also necessitate the operation of a call center and the offering of credit/identity theft services, triggering the Incident Response Expenses Coverage.

Third-party claims and/or regulatory investigations may also be commenced against the entity, which could trigger the Privacy Liability and Regulatory Coverage. Similarly, some or all of the data held hostage may become lost or corrupted, requiring data recovery assistance, which is also provided under the Data Loss Coverage of cyber insurance policies. Finally, the lockup of critical information for an extended period of time could result in a slowdown or complete shutdown of operations, addressed by the Network Business Interruption Coverage.

What we are seeing is likely just the dawn of the rise in cyber extortion incidents, and ransomware incidents in particular. Organizations are therefore well advised to work with their insurance brokers to tailor an insurance program to respond to this unique risk. Furthermore, a combination of security awareness training of employees and IT investment will be crucial in combating this growing threat.
First line of defense
Empowering employees to make security-conscious decisions

by Anthony Rapa

Businesses are attractive targets to cyber criminals due to the vast economic advantage that can be gained from theft of money and information, as well as network intrusion. Understanding and protecting against outside threats should not, however, create a blind spot to an organization’s first line of defense: their own employees. What employees do—or fail to do—can make or break an organization’s cybersecurity strategy.

Recent studies suggest that approximately 60% of data security incidents are non-hacking-related. Phishing (broadly defined in the business context as sending fraudulent emails to unsuspecting employees to gain network access and/or obtain confidential, sensitive information or money) remains an effective attack. Symantec’s most recent Internet Security Report notes that over half of inbound business email last year was spam. Even more disturbing is that the 2016 edition of Verizon’s Data Breach Investigations Report (DBIR) notes that 30% of phishing emails in the data group were viewed by employees, and that 12% of employees opened the malware-containing attachment. Both numbers actually represent an increase over the previous year’s data, suggesting that, despite knowledge of the danger, companies may not be placing adequate emphasis and focus on employee cybersecurity awareness.

Additionally, Willis Towers Watson’s Claims and Legal Group (CLG) has observed an appreciable uptick in claims involving impersonation fraud, where an employee is tricked via email to transferring money or divulging sensitive information to someone posing as a high-ranking company official. This new twist on phishing has resulted in multi-million dollar losses to sophisticated firms. An April 2016 FBI Alert indicated that incidents of so-called “CEO spoofing” were up 270% since January 2015.

Lost laptops, phones, and physical files continue to serve as a major source of data security incidents. The 2015 Net Diligence Cyber Claims Study found approximately 10% of claims submitted to cyber insurance carriers were the result of lost or stolen devices. Along similar lines, Verizon noted in the DBIR that employees are 100 times more likely to lose a device than to have it stolen. The DBIR also noted that theft was most likely to occur in the victim’s own work area (39%) or from the employee’s personal vehicle (33.9%).

Human error also continues to account for a large percentage of security incidents. For example, Verizon notes that weak, default or stolen employee passwords played a role in 63% of security incidents. “Miscellaneous errors” accounted for 17.7% of the incidents, 26% of which were caused by an employee sending an email to the wrong person. Although these figures are by no means exhaustive, the message is clear. Despite knowledge of the danger and investment in employee training, a large percentage of cyber incidents continue to arise from employee errors.
Increased connectivity, personal devices and a 21st century workforce

Given the risk, one would expect that future changes in corporate strategy and technology will reduce the amount of behavior-based breaches. The truth, however, may be the opposite. Coming changes to technology, corporate policy and the composition of the workforce itself may have the potential to greatly increase the risk human behavior plays in data security. With more avenues for hackers to gain access to an organization’s system there are also more opportunities to fool employees into making poor decisions. The internet of things (IOT) is a term used to describe the increasing number of connected devices that capture and share data with one another. As technology advances, even seemingly innocuous items, such as kitchen appliances, cars and wearable technology will gather data about everyday lives and share it over a wider network. McAfee Labs’ 2016 Threats Predictions report noted that there were approximately 15 billion IOT devices in the 2015; by 2020 that number may grow to 200 billion. On the positive side, the IoT will allow businesses to collect massive amounts of new data, improving product design, safety and consumer satisfaction. At the same time, such data collection will make corporate networks all the more tempting as targets.

Bring Your Own Device (BYOD) programs continue to increase in popularity. BYOD allows employees to connect their personal mobile device to corporate systems and access company data from anywhere. Aside from saving companies the cost of purchasing mobile devices, BYOD is highly convenient for employees. BYOD allows employees to stay mobile and connected on a single device while simultaneously enabling multitasking. Cloud-based computing also continues to gain traction in the corporate world. Employees now have access to important work information — and the corporate network — from anywhere.

Although companies can manage the risk created by BYOD through the use of encryption software and implementation, and enforcement of BYOD use policies, effective security requires a commitment from the users. While it is expected that employees who use their personal devices for work purposes may also download various apps, this practice poses a risk to organizations. In this regard, Ponemon Institute’s “May 2016 report, Managing Insider Risk Through Training and Culture,” noted that 54% of responding organizations are concerned about employees using unapproved cloud or mobile apps in the workplace. Therefore, it is imperative that employers include BYOD-specific training to employees, highlighting the potential risks in downloading suspicious apps. While the risks inherent in BYOD cannot be completely negated, through proper training they can at least be mitigated.

Finally, the Millennial Generation is becoming a larger percentage of the workforce. They are more tech-savvy than their older colleagues. Millennials are more comfortable sharing information on social media (including information that may not be appropriately shared) and more willing to experiment with new and untested technology.

In this environment of increasing connectivity and mobility, the need for employees to practice cybersecurity-conscious behavior is clear, but how can companies encourage such behavior?

Workforce culture as a solution

In May 2016, Willis Towers Watson published the results of a study analyzing the cyber risk inherent in employee behavior. We analyzed employee opinion results from more than 450,000 employees corresponding to a period during which significant data breaches were experienced within their organizations. The results were benchmarked against high performing companies (that had not experienced data breaches) and global information technology (IT) staff.

The study revealed that both the employees and IT professionals at impacted firms reported a lack of or inadequate training and leadership, suggesting that organizations may also not be keeping employees informed on the latest trends and attack vectors. And with respect to the IT professionals, employees specifically charged with the security of the company’s network, a lack of training at onboarding creates an immediate and potentially lasting blind spot.

Cybersecurity is largely the result of the decisions made by organizations’ employees each and every day. Teaching employees to practice regular security-conscious behavior, however, is easier said than done. Ultimately, investment in appropriate technology and a positive workforce culture that promotes training, company pride, and pay for performance can all help mitigate cyber risk, along with other risk mitigation strategies.
After the breach
Your vendor or mine?

by Kristin Zieser

By now, it is generally understood that a strong incident response plan and the availability of cyber liability insurance are key components of a prudent cyber risk mitigation strategy. To achieve maximum effectiveness, however, they must work together seamlessly. Perhaps the most important step a company should consider after a cyber breach is retaining appropriate vendors, including legal, computer forensics and credit monitoring experts. Based on the number of claims handled by Willis Towers Watson’s Claim and Legal Group (CLG), vendor selection continues to be a common coverage issue at the onset of a claim. Certain policies require insureds to select vendors from a pre-approved list; insureds must be aware of this requirement prior to the occurrence of a breach. Failure to do so could result in a coverage dispute at a critical juncture when the insured needs to make an immediate decision regarding its vendor(s). While choosing to retain a non-approved vendor could cause unnecessary delays and possibly jeopardize coverage, there are advantages to retaining insurer-approved vendors.

Time is a luxury that rarely exists when responding to a breach or an incident. The insurer’s vendors are pre-approved, which means the insurer’s consent is not required before retaining those vendors — affording peace of mind that the vendor’s fees and expenses will be considered as a covered loss and reimbursable subject to any applicable retention and other terms and conditions of the policy. Insureds also receive pre-negotiated discounted rates when they select from an insurer’s pre-approved vendor list. These vendors have a working relationship with the claim adjuster often making for a smoother claim process. Like the insured, the insurer has an interest in ensuring that the vendor provides quality services and, as such, regularly vets the panel vendors. Because the vendor generates a significant volume of business through its relationship with the insurer, the vendor is incentivized to deliver quality services.

Notwithstanding the advantages in insurer-approved vendors, there are legitimate reasons for an insured to prefer its own vendors. For example, an insured may have a pre-existing relationship with a vendor that has intimate, in-depth knowledge of the insured’s business — knowledge that the insurer’s approved vendor likely does not possess. Additionally, cyber incidents are sensitive — not only from a time perspective, but also as respects protection of confidential and proprietary information.

Therefore, it is understandable that an insured may prefer to retain a vendor that the organization has already entrusted with that information. The key take-away is that insureds should consider the advantages and disadvantages of selecting a vendor from an insurer’s pre-approved list prior to binding coverage in order to determine whether it is comfortable with the insurer’s list. If the insured prefers a non-approved vendor, it is important to discuss alternatives and exceptions to the panel list prior to binding coverage. An insurer’s refusal to consider or approve the insured’s request should factor into the insured’s overall decision to bind coverage with the particular insurer. Premium and other coverage terms are important; having the right vendor in place when a breach occurs may be equally important.
New data regulations in the EU

by Bridget Treacy
Partner, Hunton & Williams LLP and
FINEX UK Cyber Practice

On April 14, 2016 and after three years of discussion, the European Parliament voted to adopt the General Data Protection Regulation (the Regulation). The purpose of the Regulation is to further harmonize national data protection laws across the European Union (EU), strengthen the obligations on those who use personal data, and enhance individuals’ privacy rights. The Regulation will be directly applicable across the EU, without the need for national implementation.¹ Businesses are likely to face fewer national variations in their data protection compliance obligations. However, there remain areas in which there will continue to be differences from one member state to another. The Regulation is due to take effect in 2018 and will impact all business sectors. The Regulation will apply to all U.S. and non-European organizations handling data relating to EU-based data subjects. Organizations should start now to assess how the Regulation will change their current data protection compliance obligations to mitigate potential exposure as a result of non-compliance.

The key changes

Changes that could be challenging for businesses

1. Increased enforcement powers. The Regulation will significantly increase the maximum fine for breaching data protection law to €20 million (approximately $26.5 million), or 2 – 4% of annual worldwide revenue, whichever is greater. This is a significant change from the current fines, which vary from country to country, but are comparatively low (e.g., the U.K. maximum fine is £500,000 — approximately, $666,000).

2. New obligations of data processors. Data processors (i.e., those persons or entities that process personal data on behalf of data controllers, the latter of the two being the custodians of the data) will be subject to enforcement action and fines of up to the same levels as controllers if they breach their obligations under the Regulations. Currently, processors are generally not subject to fines or other penalties.

3. Expanded territorial scope. Non-EU businesses will be subject to the Regulation if they: (i) offer goods or services to data subjects in the EU or (ii) monitor data subjects’ behavior in the EU irrespective of the nationality of those data subjects. Many non-EU businesses not previously required to comply may now be brought into scope.

4. Consent, as a legal basis for processing, will be harder to obtain. Consent must be freely given, specific, informed and unambiguous, and demonstrated by either a statement or a clear affirmative action. The data controller must be able to demonstrate that consent has been obtained and can be withdrawn at any time.

5. Privacy by design and by default. Businesses will be required to implement data protection by design (e.g., when creating new products, services or other data processing activities) and by default (e.g., data minimization). Businesses will also be required to perform data protection impact assessments to identify and address privacy risks in new products.
6. **Strict data breach notification rules.** The Regulation will require businesses to disclose data breaches within 72 hours where there is risk to affected individuals. If the data controller cannot do this, it will have to justify the delay to the supervisory authority (SA). If the breach has the potential for serious harm, data subjects must be notified without undue delay.

7. **The ‘right to be forgotten’.** Individuals will have an expanded right to request that businesses delete their personal data in certain circumstances (e.g., the data is no longer necessary for the purpose for which it was collected).

8. **The right to object to profiling.** Under the Regulation, individuals will have the right not to be subjected to profiling that “significantly” affects them. Profiling includes most forms of online tracking and behavioral advertising, making it harder for businesses to use data for these activities.

9. **The right to data portability.** The Regulation will give data subjects the right to obtain a copy of their personal data from the data controller in a commonly used format. This will, in theory, enable data subjects to have their data transmitted directly from one service provider to another seamlessly.

**Changes that could be positive for businesses**

1. **Greater harmonization.** The Regulation will introduce a single legal framework that applies across all EU member states. This means that the issue of member states implementing the existing requirements differently will (to a large extent) fall away so that businesses will face a more consistent set of data protection compliance obligations across EU member states.

2. **Risk-based approach to compliance.** Under the Regulation, businesses will be responsible for assessing the degree of risk their processing activities pose to data subjects and for implementing appropriate measures to ensure compliance. Low-risk processing activities may face a reduced compliance burden.

3. **The ‘one-stop-shop’.** Businesses with operations across the EU will be able to deal with the SA in the jurisdiction of its main establishment, as lead authority. This will not prevent other SAs from taking enforcement action but will encourage closer working relationships with lead SAs. U.S. and global organizations with subsidiaries or other substantial operations in the EU may be deemed for these purposes to have their “main establishment” in a specific EU member state.

4. **‘Pseudonymization’.** The Regulation introduces the concept of ‘pseudonymized data’ (i.e., data that can no longer be attributed to a specific individual, such as key-coded data). Pseudonymous data will still amount to personal data but may be subject to fewer restrictions on processing, provided that the risk of harm is low.

5. **Binding Corporate Rules (BCRs).** BCRs are agreements used to lawfully transfer personal data out of the European Economic Area (EEA). The Regulation will formally recognise BCRs. They will still require SA approval, but the approval process should become less onerous than under the current system.

**Areas remaining unharmonized**

Although the Regulation increases the harmonization of data protection law across the EU, some existing core concepts will remain largely unchanged. For example, the concepts of personal data, data controllers and data processors, which are broadly similar in both the existing directive and the Regulation. In addition, there will still be areas under the Regulation where the applicable requirements vary among member states (as some categories of information fall outside of the EU’s legislative remit). For businesses, the relevant areas include:

- **Employment law:** Member states may continue to adopt their own rules regarding the processing of personal data in an employment context.
- **Professional secrecy laws:** Some member states have laws on professional secrecy that prevent the processing of certain data, even where the Regulation would otherwise permit that processing.
- **Laws on interception of communications:** Member states have interception laws under the E-Privacy Directive, which are not uniform across the EU.

**Staying ahead of the developments**

Data protection will become as significant a compliance risk for organizations as antitrust issues, with substantial regulatory sanctions. Under the Regulation, data protection will no longer be an area in which businesses can afford to take casual risks. The Regulation is likely to require company-wide changes for many businesses. Organizations in the EU or with EU interests should consider the impact of those changes and start working toward compliance. It is already clear that some changes will take time to embed within businesses, while others may require considerable changes to existing processes. As a first step, businesses need to take stock of their existing data assets and compliance profile and systematically assess how the Regulation will impact existing compliance, as well as risk transfer decisions. For most organizations, this will be a sizeable project.
International insight: The Privacy Shield

The European Commission, on July 12, 2016, adopted the EU-US Privacy Shield (Privacy Shield), an agreement between the EU and United States. The Privacy Shield will provide a framework for EU-U.S. transfers of personal data, replacing the Safe Harbor framework — declared invalid in October 2015 by the Court of Justice for the EU in the case of Schrems v Data Protection Commissioner. Like the previous Safe Harbor regime, the Privacy Shield will require self-certifying companies to comply with a set of core privacy principles:

- **Notice**: informing individuals about the Privacy Shield, their rights under it, and how their data is processed
- **Choice**: allowing individuals to object to the disclosure of their information to third parties or the use of their data for materially different purposes, and opting out of direct marketing
- **Security**: requiring security measures appropriate to the nature of the data and the proposed processing; these obligations must be flowed on to sub-processors
- **Data integrity and purpose limitation**: limiting data to what is relevant, and keeping it accurate, complete and current
- **Access**: allowing individuals to access their data without giving a reason and to arrange for the correction, amendment or deletion of their data where it is inaccurate or has been processed in violation of Privacy Shield
- **Accountability and onward transfer**: limiting the onward transfer of personal data to specified purposes on the basis of a contract that provides the same level of protection as guaranteed under the Privacy Shield
- **Recourse, enforcement and liability**: putting in place robust mechanisms to ensure compliance with the Privacy Shield, and independent and free redress mechanisms capable of providing effective remedies

There has been a strong appetite on both sides of the Atlantic for an agreement that will enable companies to transfer personal data with greater ease. On April 13, 2016, European Data Protection Authorities (known as the Article 29 Working Party or WP29) recognized the Privacy Shield as an improvement to the now invalid Safe Harbor but highlighted several shortcomings, challenging whether the Privacy Shield afforded European citizens essentially equivalent safeguards when their data are processed in the U.S. The shortcomings concerned data retention, purpose limitation, onward transfers, and the complexity of rights of redress. The WP29 was also concerned about national security guarantees.

Notwithstanding those concerns, the Privacy Shield will now be effective in the EU as soon as the adequacy decision has been formally notified to the EU's member states. It's anticipated that, once the Privacy Shield is published in the U.S. Federal Register, the Department of Commerce will adopt the Privacy Shield so that organizations will be able to self-certify as of August 1, 2016.

The United States has pledged to address the WP29’s concerns and to enforce the new stricter requirements on U.S. organizations self-certifying under the new regime. The Department of Commerce is expected to remove non-compliant organizations from the list of certified organizations, and the Department of State has announced an ombudsman scheme to provide redress to EU data subjects who believe their rights have been violated. U.S. businesses should therefore review their procedures prior to self-certification to ensure they are compliant with the stricter requirements of the Privacy Shield.

¹ The Regulation was passed several months before the recent Brexit vote. We are monitoring this new development closely, particularly as to the potential impact, if any, of Brexit on the Regulation. Please visit the regularly updated EU Referendum page of our website for more information on our Brexit-related perspectives, webinars and upcoming events.
About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.