Data privacy and protection

On 28–29 June 2016, members of the North American and European Audit Committee Leadership Networks (ACLN and EACLN) met in Zürich for their 11th summit meeting. In one session, members discussed evolving rights and obligations related to data privacy with Steve Holt, Partner, Financial Services Advisory, Ernst & Young, and Fabrice Naftalski, EMEIA Head of Digital and Data Privacy, Ernst & Young Société d'Avocats.1 For further information on the networks, see “About this document,” on page 9. For biographies of Mr Holt and Mr Naftalski, see Appendix 1, on page 10. For full list of participants, see Appendix 2, on page 12.

Executive summary

- **The path to data protection regulatory reform (page 2)**

  Historically, a fragmented set of national laws has governed how companies protect the vast quantities of data that they manage. Recent reforms, particularly the European Union’s (EU’s) adoption of the General Data Protection Regulation (GDPR), attempt to harmonize data protection laws to enhance protection for individuals and make obligations clearer for companies. These reforms also come with increased sanctions – up to 4% of annual global revenue – for companies that fail to comply.

- **Data privacy rights and obligations (page 3)**

  The GDPR creates a range of new rights for EU citizens and obligations for companies that obtain and process individual data about EU citizens, whether or not those companies are located in the EU. Audit committee chairs were most focused on enhancements to the form and substance of consent that companies must obtain in order to process individual data and on the new requirement that companies notify national authorities within 72 hours of learning of a data breach. In addition, audit committee chairs discussed the GDPR’s requirement that companies create new safeguards for the data that they possess, under the direction of a senior-level data protection officer (DPO), a new role at many companies.

- **Oversight of data privacy and protection (page 7)**

  Companies must implement these changes by May, 2018. Timely compliance will require a thoughtful planning process, with contributions from a wide range of participants who do not traditionally work together. Given the stakes, audit committee chairs said it is important for senior management to take a leadership role in the implementation, with close attention and cooperation from the board.

For a list of discussion questions for audit committees, see Appendix 3 on page 13.

---

1 ViewPoints reflects the networks’ use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members in connection with the meeting.
The path to data protection regulatory reform

Recently, the European Commission and governments both within and outside the EU have taken steps to unify data privacy rights and responsibilities. In 2012, recognizing the dramatic changes in how data is generated and transmitted around the world and the challenges presented by patchwork regulation, the European Commission proposed overhauling Directive 95/46/EC (hereafter the 1995 Directive), stating, “EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens.”2 At the time, EU Justice Commissioner Viviane Reding said, “The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data.”3

In December 2015, after nearly four years of negotiation, the European Commission, Parliament, and Council agreed on the terms of the GDPR, a comprehensive set of data protection reforms.4 The GDPR becomes law in all EU member states on 25 May 2018 and is designed to protect the personal data of European citizens, regardless of where or by whom the data is held.5 Mr Holt explained that the scope of the GDPR is very broad: “If you actively target EU customers, then you, including all your employees and all outsourced providers, are required to comply.”

The GDPR is a regulation, and therefore binding law across the EU.6 Mr Naftalski explained, “The old regime was an EU directive, versions of which had to be implemented by 28 legislatures. The purpose of the GDPR is to create a new, uniform, consistent framework to catch up with advances in technology. The existing framework provides a set of principles, and the GDPR operationalizes those principles for current times." Audit committee chairs generally support the effort to harmonize data privacy laws. One member said, “It is hard to know when we can share data, because the whole digital world knows no borders, yet the legal world always knows borders.”

Because the GDPR applies to data about employees as well as consumers, the implications extend to all companies that do business in Europe. And because the primary focus of the GDPR is on commercial transactions, one legal expert warned, “Multinational employers – especially those engaged in business-to-business commerce (“B-to-B”) – must carefully parse the Regulation to figure out how it applies to their management of a global workforce … Virtually all U.S. multinational employers likely will need to update at least some of their existing policies and procedures, and re-align some of their practices, for handling the personal data of employees of their EU subsidiaries.”7

---

3 Ibid.
4 “Reform of EU Data Protection Rules,” European Commission, updated 12 July 2016. These reforms also included a new data protection directive for the police and criminal justice sector.
With consistent rules across Europe also come consistent punishment for violations of those rules. Mr Holt explained, "The big difference between the GDPR and the old rules is that the GDPR has teeth." The GDPR authorizes national data protection authorities to impose administrative sanctions of up to the greater of €20 million or 4% of global annual turnover (revenue). Mr Naftalski added, "The GDPR's fines are intended to demonstrate the importance of protecting fundamental rights. It provides an incentive to establish a strong compliance program."

### Transatlantic safe harbor and privacy shield

The 1995 Directive prohibited transferring the personal data of EU citizens outside the EU unless the data was transferred to a country with adequate data protection standards. While US standards were not considered by the EU to be adequate on their own, the EU, together with the US government, developed a framework (a "safe harbor") that provided a way for US companies to comply with European law. Safe Harbor certification allowed any US company to transfer personal data from the EU if it self-certified its compliance with a set of broad principles for protecting that data. Since its implementation, more than 4,400 companies have relied on Safe Harbor certification to transfer data from the EU to the United States.

In October 2015, the European Court of Justice (ECJ) declared the Safe Harbor invalid on the grounds that it was incompatible with EU law. In response, EU and US officials worked together to create a new framework, reaching an agreement in February 2016. This agreement – the EU-US Privacy Shield – requires US companies to commit to robust obligations when processing data and specifies that the US Department of Commerce will oversee the program and the US Federal Trade Commission will handle enforcement. The privacy shield was formally adopted by the EU on 12 July 2016, and companies can sign up to use it beginning on 1 August 2016.

### Data privacy rights and obligations

The GDPR requires companies to do more to protect the individual rights of customers and employees and creates new obligations concerning the protection and processing of personal data.

---

11 Ibid.
Personal data privacy rights

The recent reforms include an emphasis on personal data privacy rights. In a statement following adoption of the GDPR, leaders from the European Commission said, “The new rules will ensure that the fundamental right to personal data protection is guaranteed for all … These rules are for the benefit of everyone in the EU. Individuals must be empowered: they must know what their rights are, and know how to defend their rights if they feel they are not respected.”17

Right to provide and withdraw consent

Unlike the 1995 Directive, which allowed companies to rely on implicit consent to transfer and process personal data, the GDPR specifies that individuals must provide unambiguous, affirmative consent.18 Mr Holt said that the reforms to the consent requirements are among the most important policy changes for companies that obtain and process personal data: “Asking someone to click a box on a website that authorizes the use of personal data is no longer sufficient. Companies need to be very clear with what data they have and how they will use it.” Individuals may also withdraw that consent at any time, a right that companies must disclose before consent is provided.19 Additionally, companies may not withhold services on the grounds that an individual objects to a particular use of their data.20

Mr Holt emphasized that it will be challenging for companies to establish the scope of the consent to seek when collecting data: “You can’t get informed consent until you figure out and disclose how you are going to use the data you collect. This will be difficult for companies that, today, gather large quantities of information and don’t even think about how they will use it in the future.”

Members observed that these requirements also pose difficult questions about the data that companies already possess, which was likely obtained without the level of consent specified in the GDPR. One said, “This is a big deal. We don’t know where all this data is in our systems, never mind what kind of consent we obtained when we received it.” Mr Holt said that many companies share this challenge: “In many cases, the consent you obtained is not good enough. Companies will either have to go back to customers and ask for broader consent, or stop processing the data. Many companies in the financial services sector are preparing to get consent again.”

One member asked, “Our companies are doing a lot of work with big-data analytics. How will this work be affected by these consent requirements?” Mr Naftalski said that companies can continue to perform large-scale data analysis, but they must take steps to ensure the data they analyze cannot be traced back to an individual: “The GDPR encourages anonymization and/or pseudonymization techniques, where data can be processed in a compliant way. It is in line with the privacy by design and privacy by default principles promoted by the GDPR.”

19 Ibid.
Additional data privacy rights

Audit committee chairs also discussed other individual rights related to data privacy:

- **Right to be forgotten.** In a 2014 case involving a Spanish citizen who requested that certain data about him be removed from Internet search results, the ECJ ruled in the man’s favor, declaring that individuals have a right to be forgotten.\(^{21}\) The GDPR codifies this right and takes it further, requiring companies to erase personal data “without undue delay” upon request, with limited exceptions.\(^{22}\)

- **Right to data portability.** The GDPR allows individuals to have their personal data transported from one service provider to another.\(^{23}\) Companies will, upon request, have to bundle data in a structured format and provide it directly to another company. In some cases, this will require companies to work with competitors to complete the transfers, raising concerns about intellectual property and confidentiality rights.\(^{24}\)

- **Right to object to profiling.** Individuals can also prohibit companies from processing their personal data to analyze or predict things like “performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.”\(^{25}\) In addition, companies that use data for these purposes will be required to disclose their methods of collecting and processing the data.\(^{26}\)

Members said that providing these new rights to customers and employees may be a challenge for companies with legacy systems. One explained that “most large companies have data about people in a number of different places, including with offshore vendors. It will be difficult to know with certainty whether you have identified all of the information a company has about an individual.”

Mandatory notification of data breaches

The GDPR also requires companies to notify national authorities in the event of a personal-data breach “leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed,” unless the breach is unlikely to cause any harm to individuals.\(^{27}\) These reports must include (1) the nature of the breach, (2) the company’s data protection officer’s contact information, (3) the likely consequences of the breach and (4) the plan to address and mitigate the breach.\(^{28}\)

Mr Holt said that while the default is that these reports be made only to a national regulator, “if there is a high risk that customer data is lost, you may need to notify customers, too.”

\(^{21}\) Alan Travis and Charles Arthur, “EU Court Backs ‘Right to Be Forgotten’: Google Must Amend Results on Request,” *Guardian*, 13 May 2014.


\(^{26}\) Ibid.


\(^{28}\) Ibid.
Data privacy and protection

reports are required to be made within 72 hours of the company having become aware of the breach, though Mr Naftalski explained “this timeline is an objective, but you have some flexibility. If you cannot notify in 72 hours, you need to explain the delay.”

Audit chairs wondered how these new notification requirements will work in practice. One said, “These investigations often go on for many months. There are risks to going to the regulators before we understand exactly what happened.” Members also discussed complications related to the requirement to notify individuals, especially when in some cases, regulators prefer that a breach remains confidential while an investigation proceeds. Mr Holt said, “There is a tension in the system where companies may be asked not to notify individuals by some regulator, but [choose] to notify because of other compliance concerns.”

Some members were concerned about the risk of breach notification overload. One recent review of a new breach notification requirement in the Netherlands found that the Dutch government was likely to face 4,200 notifications in the first year.29 The authors of that study predicted, “If this number is indicative of the number of notifications under the GDPR (which it is because the threshold under the GDPR is lower and notification requirements will be more easily triggered), larger European countries may be in for a surprise.”30

Corporate data protection safeguards

Corporate accountability is another emphasis of the GDPR. Companies are accountable for reviewing, documenting and assessing data-processing procedures, minimizing data processing and retention, safeguarding data-processing activities and sharing data-processing policies with supervisory authorities.31

In this vein, the GDPR creates additional operational obligations for companies that control or process personal data:

- **Appoint data protection officers.** Companies that conduct large-scale monitoring of data subjects or process sensitive categories or personal data are required to appoint a data protection officer (DPO) with “expert knowledge of data protection law and practices.”32 Mr Naftalski said that while the regulation’s description of the role is vague, “this person should have the budget and means to execute the role and work with people across the organization.” Describing the DPO, Mr Holt said, “To date, this kind of role has been pretty far down in the organization, usually reporting to legal. The idea is to elevate the role and have someone with access to senior management and the board.” Members said it was important to appoint DPOs that understand the business, not just the regulatory environment, since companies will be faced with a range of judgment calls as they implement these new requirements.

- **Implement privacy by design.** The GDPR emphasizes implementing data protection both at the project design phase and throughout development. It stipulates that the default

---

29 Lokke Moerel and Alex van der Wolk, “130 Days, 1,500 Notifications: Does Dutch Breach Rule Foreshadow GDPR?” Privacy Advisor, 16 May 2016.
30 Ibid.
setting for products and services should be to protect data privacy. Mr Holt identified this element as among the things to do even before the 2018 effective date of the GDPR: “If there is anything new, from this point forward, companies should make sure to build in adequate privacy protections. Then you only have to deal with fixing legacy issues, not reforming new systems.”

- **Perform privacy impact assessments.** In cases where data-processing activities put individuals’ rights and freedoms at “high risk,” companies will be required to conduct privacy impact assessments (PIAs). The GDPR requires a PIA to include “a systematic description of the processing operations, their purposes and the interests pursued by the company; an assessment of the necessity and proportionality of the processing; a risk assessment with regard to individual rights; and the safeguards and accountability measures that are envisaged.”

**Oversight of data privacy and protection**

New data protection obligations require oversight and cooperation among several functions within a company’s management. Boards, too, will have greater oversight obligations to ensure that their companies are adopting the necessary policies and practices.

**The implementation timeline**

Members discussed the requirement that companies be compliant with the GDPR by May 2018. One said, “When I heard about this, I immediately raised the issue with the general counsel at all of my companies. It is hard enough to integrate all of our data systems, and these new requirements make it even more challenging.” Another asked, “Is the expectation that come May 2018, everything will be good to go?” Mr Holt responded, “Regulators will expect it, but the reality is that most companies will still be in the process of making the necessary changes. What you will need to know is where you are and what you still have to do.”

Mr Holt recommended breaking down what a company needs to do to become compliant into smaller pieces: “I have one client that identified 14 key workstreams to create systems and processes to comply with the GDPR. Each of these teams is examining a particular issue and the changes the company will have to make.” Mr Naftalski reassured members that their companies are likely well on their way to compliance: “Keep in mind that about 80% of the regulation is a recognition of what companies should have already done in practice to reach compliance with existing data protection framework. For the rest, there are already solutions at companies; they just need to be updated.” He pointed out that the incentives for adopting these practices go beyond the compliance necessity: “Good data protection practices build trust, and that is worth a lot in the long term.”

---
34 Alex van der Wolk, Sotirios Petrovas, and Bastiaan Suurmond, “The EU General Data Protection Regulation: A Primer for International Business,” 23 March 2016.
35 Ibid.
Management responsibilities

Protecting data privacy requires a coordinated, cross-functional team of leaders with different backgrounds. Mr Holt emphasized, “The consequences of the GDPR mean that data privacy requires business buy-in across the organization. This is not just a legal issue or a compliance exercise – it is much more than that.”

At a minimum, the following units will have a role in implementing data protection reforms:

- **Legal.** Network members emphasized that with so many changes happening at once, legal departments and outside counsel must be heavily involved in all phases to ensure compliance.

- **Information technology (IT).** In some cases, the new rules will require dramatic changes to IT systems, policies and practices. IT professionals will be charged with considering the privacy implications of the company’s current and future practices.

- **Sales and marketing.** At consumer-facing companies, the sales and marketing organizations will be required to rethink their practices and ensure that they abide by consumers’ requests. Mr Holt said, “Marketing teams will have to be aware of what they can and cannot do with data. If they get this wrong, it could stop the business.”

- **Human resources (HR).** HR professionals also play a critical role in the company’s approach to data protection. One expert said that the new consent requirements pose special challenges in the employment context: “Employers who consider relying on employee consent as a lawful ground for processing personal data should carefully assess whether consent would be freely given or voluntary. Any threat of discipline, termination or other significant detriment for refusing to consent likely would invalidate the employee’s consent.”

Members also discussed who within management should oversee the company’s data protection changes, since most companies do not yet have a DPO with the seniority described in the GDPR. One member said, “It is important to give this responsibility to someone with the right skills. We tend to give these kind of projects to legal, but this has more complexity and requires leadership from within the business.” Mr Holt said, “At some companies, the chief operating officer is responsible. This is a process-driven problem. If the implementation is led by the legal function, it can be treated as solely a compliance issue. Ultimately, it is much more than that. It is an operational issue, and failure to do this right can imperil the way that the business operates and imperil the business itself.”

Board oversight of data protection programs

Network members said that the scope of the new rules and the size of potential fines for violations make data protection a critical issue for boards and audit committees. Mr Holt agreed: “This should be treated as a key risk to the company, reviewed regularly by both the board and management committees that are responsible for risk oversight.”

---

said, “At the moment, data privacy sits with the audit committee, but this should be an issue for the full board.” Another added, “From where I sit, we understand the rules, but we still struggle with how to manage the process in depth.”

Given the complexity of overseeing data protection, members said that boards must stress the need for new and creative thinking throughout the organization. Before the meeting, Steve Wright, Chief Privacy Officer at John Lewis, said, “Directors have a real opportunity here because they don’t have the political or bureaucratic hang-ups that some managers face. They can afford to be focused on what should be, ask tough questions and offer different solutions.” One way that members suggested doing this is by discussing data protection practices with executives from several different disciplines and listening for consistency.

Conclusion

Large companies, whether or not they interact directly with consumers, control and process a substantial and growing quantity of data about individuals around the world. The GDPR provides a new framework for how companies protect the personal data of EU citizens. Audit chairs recognized the need for reform and the benefits of a uniform set of requirements, while also raising concerns about the level of change required in a relatively short time. Effective compliance will require the dedication of a cross-functional team, with close supervision by both senior management and the board.

About this document

The European Audit Committee Leadership Network (EACLN) and Audit Committee Leadership Network (ACLN) are groups of audit committee chairs drawn from leading European and North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The networks are organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of ViewPoints lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive ViewPoints are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

EYG no: 02461-162GBL
Appendix 1: Biographies of guests

Steve Holt
Steve Holt is a Partner at Ernst & Young (UK), and responsible for leading the EMEIA Financial Services Cyber Security practice, which covers 12 countries. He has more than 25 years of experience in leading IT audit, IT risk, cybersecurity, regulatory and data privacy projects, and he has worked globally within retail banking, investment banking, broking and asset management.

Mr Holt has extensive experience leading global cybersecurity engagements, covering a breadth of subjects. He has provided advice to clients on their overall strategic security direction to reduce existing and future external and internal threats and has supported the development of security road maps to implement their strategies.

Mr Holt is currently working with a number of financial services clients on assessing their approach to cybersecurity and cybercrime risks. He has led a number of data privacy reviews and data loss investigations for clients to assess compliance with the UK Data Protection Act 1998 and other global regulations and is currently helping a key bank to establish its GDPR program.

Mr Holt regularly presents on the topics of technology risk management, data privacy, cybersecurity, third-party management and data leakage. He has facilitated workshops at a number of central banks to assess how they oversee the IT operational risks associated with their payment systems.

Mr Holt is one of the EY’s leading professionals on IT regulatory requirements. This experience has been developed over the last 12 years, during which time he led 166 Skilled Persons reviews, completed systems authorization forms and advised clients on FCA consultation policies, including the FSA April 2008 Data Security paper.

Mr Holt is a chartered accountant (ACA), certified information systems auditor (CISA), a PRINCE 2 practitioner, member of the IAPP and holds the ISEB certificate in data protection.

Fabrice Naftalski
Fabrice Naftalski is a Partner/Attorney at law with the EY Legal practice in France and is the EMEIA head of the IP/IT/Data Protection Law practice. He has been an attorney for 20 years. Mr Naftalski graduated with a degree in English and North American business law (University Panthéon/Sorbonne) (DEA) and held a Paris Bar specialty in information technology and telecom law.

A member of the Europe Advisory Board of the International Association of Privacy Professionals from 2010 to 2012 and currently an IAPP faculty member, Mr Naftalski is also a CIPP/E & CIPM holder and a EuroPrise legal expert (ULD - EuroPrise - 102-2009e), able to certify compliance of IT services and products with European Directive 95/46 (data protection) and 2002/58 (privacy). He serves clients from the pharmaceutical, banking and insurance sectors, technology industries, nonprofit organizations and industrial groups (including the
airplane, automotive and luxury industries), working with various stakeholders from legal, IT, research and development, compliance, risk management and HR.

He works on contractual and regulatory projects in connection with the use of IT (e.g., data protection and privacy law, outsourcing agreements, software implementation agreements, Internet law and e-commerce and e-invoicing) and also on transactions dealing with intangibles (e.g., trademarks, patents, know-how, technology, databases and software). He assists clients with compliance with French and European data protection laws and with inter-alia inventory of data files, compliance audit and privacy impact assessment, drafting of notifications to data protection regulators, personal data management procedures (including binding corporate rules and other tools to secure international transfers of data), relations with EU institutions and bodies, relations with national regulators, retention policies, whistleblowing policies and codes of conduct.
Appendix 2: Participants

Members participating in the summit sit on the boards of over 40 public companies:

- Les Brun, Audit Committee Chair, Merck
- Aldo Cardoso, Audit Committee Chair, ENGIE
- Mary Anne Citrino, Audit Committee Chair, HP Inc.
- Pam Daley, Audit Committee Chair, BlackRock
- Edgar Ernst, Audit Committee Chair, TUI AG
- Tim Flynn, Audit Committee Chair, Wal-Mart Stores
- Liz Hewitt, Audit Committee Chair, Novo Nordisk
- Lou Hughes, Audit Committee Chair, ABB
- Shonaid Jemmett-Page, Audit Committee Chair, GKN
- Blythe McGarvie, Audit Committee Chair, Viacom
- Hanne de Mora, Audit Committee Chair, Sandvik
- Nasser Munjee, Audit Committee Chair, Tata Motors
- David Vitale, Audit Committee Chair, United Continental

EY was represented in all or part of the meeting by:

- Andy Baldwin, EY EMEIA Area Managing Partner – elect
- Jean-Yves Jégourel, EY EMEIA Assurance Leader
- Frank Mahoney, EY Americas Vice Chair of Assurance Services
- Allister Wilson, Assurance Partner, Ernst & Young LLP
Appendix 3: Questions for boards and audit committees

? How are the recent changes in data protection law being discussed by your boards or audit committees?

? What are the benefits for your companies of the EU’s more holistic approach to data protection regulation?

? Will the GDPR influence companies’ strategic decisions about how data is analyzed and utilized?

? How can data companies effectively demonstrate their accountability for data protection to customers and employees?

? Has your board discussed the concept of privacy-by-design? What are the challenges to implementing a privacy-by-design policy?

? How will the new breach notification requirements change the way boards and management teams oversee the response to a data breach?

? How can the board ensure that a company develops the right controls to comply with the new rights and obligations established by the GDPR?

? How do you ensure that the company has included all the appropriate constituencies in the team tasked with bringing the company into compliance with these new rules?

? Does your company plan to increase the number of employees dedicated to data privacy in the next two years?

? Who presents to your board on issues related to data privacy?