European Audit Committee Leadership Network

October 2019

EACLN

VIEWPOINTS

Oversight of privacy

Privacy and data governance are critical issues for companies and their boards as they navigate challenges around data use. On one hand, companies enjoy a wealth of opportunities to capitalize on the data they obtain from customers, employees, and business partners, and they are using new data collection and analysis techniques to improve risk management, operating efficiency, customer relations, and product innovation. On the other hand, companies also face mounting public concerns over security and privacy.

The General Data Protection Regulation (GDPR) became effective last year and brought with it sweeping changes to the rules governing data use and breach notification. GDPR enforcement efforts have already led to substantial fines for companies across a range of industries. However, the issue extends well beyond the challenges of GDPR compliance. Companies must also grapple with the reputational risks associated with certain practices as shifting consumer expectations alter the terms for the collection, storage, and use of data.

On 13 September 2019, members of the European Audit Committee Leadership Network (EACLN) met in Munich to discuss these issues.[1] They were joined by three experts on privacy: Eva Gardyan-Eisenlohr, group data privacy officer at Bayer; Peter Katko, global digital law leader at EY; and Claus-Dieter Ulmer, global data privacy officer at Deutsche Telekom. *For biographies of the guests, see Appendix 1, on page 12, and for a list of meeting participants, see Appendix 2, on page 14.*

Executive summary

In the meeting and in calls before the meeting, EACLN members and their guests touched on four broad topics:

- **Stepped-up enforcement of privacy legislation** *(page 2)*

  The GDPR establishes comprehensive new consumer rights and organizational responsibilities regarding how personal data is handled. National regulators in Europe are now ramping up enforcement efforts, imposing significant fines for alleged violations. Meanwhile, the United States is starting to catch up. Congress is considering legislation, and states such as California have already enacted new laws.

- **Reputational risks** *(page 4)*

  Companies are also concerned about the reputational risks associated with their use of personal data. Consumers and the public could see certain activities as intrusive even if they are legal. Emerging technologies, such as artificial intelligence and the internet of things, could exacerbate the issue, as the collection, analysis, and use of data continually evolve.

- **Company responses** *(page 5)*

  Companies are stepping up efforts to comply with regulations and safeguard their reputations, working hard to create effective processes and organizations. EACLN members and guests underscored the importance of a robust cross-functional privacy team that brings an integrated, collaborative approach to the problem. To help business units implement privacy policies, a "data privacy cockpit" can provide documentation, resources, and services such as a privacy-statement generator accommodating multiple languages.

- **Board oversight of privacy** *(page 9)*

  Boards are assessing and improving their own approaches to overseeing privacy risks. While the full board is ultimately responsible for providing oversight, the audit committee often takes the lead, especially on the control framework. It is becoming more common for privacy to occupy a regular slot on the agenda. Some audit committees now discuss privacy at every meeting, and they are likely to receive reports from a range of functions, such as the legal function, the information security function, internal audit, and marketing.

For a list of discussion questions for audit committees, see Appendix 3, on page 15.

Stepped-up enforcement of privacy legislation

The proliferation of collected data and the emergence of new analytical tools are creating new opportunities for companies to improve and grow their business. Emails, texts, images, internet searches, data from internet of things devices, and consumers' purchasing and entertainment habits are generating a staggering volume of data, and firms across every sector are developing ways to monetize it. For example, tracking and analyzing mobile phone users' locations and movements—sometimes down to the minute—has become a big business. Dozens of companies track location data through applications on users' phones and then use it to sell highly targeted advertising. In the United States alone, location-targeted advertising was an estimated $21 billion industry in 2018.[2] And this is just one of many ways in which companies can harvest and use data.

At the same time, customers, employees, policy makers, and regulators may have concerns about how data is collected and used. In recent years, debate has intensified in many quarters. This has led to regulatory initiatives imposing significant conditions on how companies store, use, and share data. New laws and regulations are in force or in the works in several jurisdictions, and experts believe others will follow suit. Meanwhile, country-level enforcement efforts are underway in jurisdictions across the European Union (EU) and are already leading to substantial penalties.

The General Data Protection Regulation

The EU adopted the GDPR in 2016, and it came into effect in May 2018, codifying and enshrining new consumer rights and organizational responsibilities. The GDPR has key provisions that cover the following actions:

- It establishes several principles relating to the collection and processing of personal data, including an overarching principle of accountability, which states that firms using personal data must comply with these principles and be able to demonstrate their compliance.[3]
- It directs that consent to the use of data be clear and easy to understand. Consumers must give unambiguous, affirmative, informed consent; data processors may no longer rely on consumers opting in by default or implied consent. Consent must be freely given, and services that could be provided without the data in question cannot be denied if consent is withheld. Consumers also have the right to withdraw consent, a right that must be disclosed before consent is provided.[4]
- It creates new rights, including an individual's right to know whether and how a firm is using their data, rights to data access and portability, and the "right to be forgotten"—the right to have data erased and no longer disseminated.
- It imposes a 72-hour mandatory breach-notification requirement when a breach is likely to "result in a risk for the rights and freedoms of individuals."[5]
- It requires organizations that process large amounts of sensitive personal data of EU residents to appoint a data protection officer, who should report to the highest level of management, which could be the board of directors.[6]
- It imposes heavy maximum penalties for violations: as much as 4% of the violating firm's annual global revenue or €20 million, whichever is higher.[7]

In January 2019, France's data protection regulator fined a large technology company €50 million for multiple GDPR violations, including failure to obtain proper user consent.[8] Then, in July, the UK regulator announced it would fine a global hotel group £99 million and an airline £183 million, each for failing to protect customers' personal information from hackers.[9] Other investigations are underway, and though many of these investigations are targeting companies that handle lots of individual consumer data, experts note that business consumers are also protected, and business-to-business companies will have to adjust their practices as well.[10] Moreover, the GDPR is not limited to customer data; it also covers personal data about employees and vendors.

In the meeting, Dr. Katko noted the significance of the fine imposed on the hotel group, where the breaches took place at a subsidiary beginning two years before that subsidiary was acquired by the group: *"The UK regulator said that [the parent company] should have identified these deficiencies during the due-diligence process."* An EACLN member inquired about the possibility of class-action suits. The guests noted that while such suits are not prominent in Europe, they expected that more of them could emerge.

US privacy laws

While legislation like the GDPR does not exist at the US federal level, states are taking action. In June 2018, California passed the California Consumer Privacy Act, which, while not as expansive as the GDPR, contains similar provisions. The law, which goes into effect in January 2020, gives consumers the right to be informed about what information has been collected,

rights to data access and portability, and the right to have their personal information deleted.[11] The law also expands the definition of personal information to include biometric data, location, and browsing history.[12]

Partly as a result of developments in California, large technology firms in the United States, even those that opposed privacy laws in the past, have been lobbying for federal privacy legislation.[13] The US Chamber of Commerce released privacy principles that called for "a federal privacy framework that preempts state law on matters concerning data privacy in order to provide certainty and consistency to consumers and businesses alike."[14] Several bills have been proposed in the US Congress, though progress is slow as lawmakers struggle to resolve a variety of disagreements.[15]

Reputational risks

On top of the constraints imposed by regulations, companies face the less explicit but still significant limitations associated with consumer sensitivities and public perceptions. Even if a certain use of data complies with regulatory requirements, customers and the broader public might still view it unfavorably. New and innovative uses of data may be particularly vulnerable to adverse reactions because they are more likely to be unfamiliar or to violate traditional norms. An important aspect of this issue, however, is that consumer sentiment can be volatile and unpredictable—even familiar uses of data that have been tolerated before might suddenly face a change of opinion—creating uncertainty over what might spark a backlash.

For example, artificial intelligence allows companies to analyze data and draw inferences about customers that go well beyond what most people might imagine is possible. These capabilities are likely to change in the coming years in ways that even experts cannot predict. Thus, getting consent for the use of artificial intelligence to analyze personal data may not preclude a negative reaction if customers learn what companies are discovering about them. Even the use of anonymized personal data may prompt concerns, if it emerges that such data can be "de-anonymized." Also, companies that sell data-collection or analysis capabilities to other companies—embedded in products, for example—may think that since they are not the ones using the data, they are not responsible; the end users, however, may see them as accomplices.

Several EACLN members worried about the ethical aspects of data use and its potential impact on reputation. *"It's easy to have a lot of data and use it, but it's not always legitimate,"* one member said. Other audit chairs have brought up emerging technologies and their potential to exacerbate the issue: *"The internet of things is going to bring a lot of these questions to both the commercial and consumer end of things. It's a different dimension, both in terms of the monetization and the risk. I think these things have yet to play out, but they will play out."*

Some sectors and companies may be particularly exposed to scrutiny. Dr. Ulmer noted that Deutsche Telekom is *"a former state-owned company, so we naturally get a lot of scrutiny. There were scandals in 2008–09 that led to significant disadvantages for the company. We had to take massive actions against reputational issues."* The stakes are high because a lack of trust is both common among consumers and likely to influence their behavior. In an April

2018 survey of consumers in seven major countries, 73% agreed with the statement that businesses are more focused on profits than addressing security needs. At the same time, 75% said they would not buy a product, no matter how good, from a company that they didn't trust to protect their data.[16]

Yet EACLN members and guests noted that privacy concerns are emerging across all companies in all industries, even those that are focused on selling to other enterprises rather than consumers. Even if a business is not consumer facing, Dr. Katko noted, *"you have to look to your relationships with business customers and employees."*

Company responses

How are companies responding to the growing challenges around privacy? What issues are proving to be the most difficult to address? Audit chairs and guests saw both similarities and differences in complying with regulations on one hand, and safeguarding trust and reputation on the other. They also saw the dynamic nature of the issue as a major challenge. One EACLN member said, *"This is new and evolving, so how do we adapt to all of this? How do we educate our people? I'm learning things that we are not doing but should do. People might think we're doing the right thing, not realizing the rules have changed."*

Complying with legal requirements

The uncertainty begins with the new laws, a member said: *"In many companies, there is a degree of insecurity about fulfilling the regulatory requirements. You can't be sure that it's the case; you wonder if you have to go to the authorities. Of course, in all cases we clearly require very rigid rules to do the utmost to fulfil the regulatory issues, but in some cases the processes don't exist to make sure you fulfill these requirements."*

Audit chairs and guests mentioned several specific aspects of complying with privacy regulations that they have found challenging:

- **Internal threats.** Keeping out hackers has been an important focus, but threats from the company's own employees should also be a concern. *"What we are failing to do is protect ourselves from internal leaks from employees acting out of revenge or greed, taking advantage of their knowledge. I'm not convinced we've addressed this as well as we should. It's a very difficult problem to address,"* an EACLN member said. There is also the possibility of accidental disclosures, as when laptops are lost or servers left unprotected.
- **Data embedded deeply across complex systems.** Dr. Katko noted that it is crucial for companies to complete their "duty to delete" personal information. German authorities currently investigate deletion in enterprise resource planning applications. The problem is compounded when data about a single individual is stored in dozens of different systems. In general, data deletion requests are expected to be challenging, requiring a detailed understanding of day-to-day business practices.[17]
- **Business partners.** Ensuring that data handled by business partners is protected is also a challenge. Dr. Ulmer observed that cloud providers tend not to comply with GDPR requirements, and that ultimate compliance responsibility remains with the customer.

"GDPR unfortunately didn't put the obligation of privacy by design on IT providers, but on the controller," said Ms. Gardyan-Eisenlohr.

- **Operations in multiple jurisdictions.** Experts have highlighted the challenge of dealing with regulations from different jurisdictions, which could be costly if companies do not address them in an integrated way. For example, the rights that people have under both the GDPR and the California Consumer Privacy Act to have data about them deleted could be handled using the same technologies and processes.[18] A member asked, *"For those businesses in different jurisdictions, did they take a single, unified approach or did they let the local jurisdictions drive things?"* At the same time, different jurisdictions may have different requirements, which also creates challenges, as Ms. Gardyan-Eisenlohr explained: *"If there is a country that has a stricter law, you apply the stricter law, but the question is, How to enable cross border data transfer?"* She noted that the GDPR, though meant to harmonize requirements, does not itself guarantee consistent requirements in EU member states: *"The GDPR has so-called opening clauses, and member states have made ample use of such opening clauses and adopted local legislation. This has rendered European data privacy law pretty complex."*
- **Timelines and thresholds for disclosure.** The tight timelines within which companies must disclose means they need the right process in place to respond within the appropriate time frame. Dr. Ulmer noted that even *"really minimal issues have to be reported,"* which presents difficulties if there is a large number of these issues.

Despite the challenges, however, some EACLN members expressed positive views on complying with the GDPR. One said, *"It was painful, but in the end, we ended up a better company. We discovered a lot of gaps, and we also improved processes. It made the topic more top of mind."*

Safeguarding reputation and trust

Successful compliance is a necessary first step in protecting a company's reputation. However, as participants pointed out, initiatives that technically comply with privacy regulations may nevertheless fail to go over well with the public or customers. Innovation based on personal data should stay within regulatory bounds, but companies must also consider the harder-to-discern and more volatile vagaries of public opinion and customer sensitivities. Members in consumer-facing industries see the reputational consequences as potentially catastrophic.

At the same time, innovative uses of data may provide enormous benefits for both consumers and society at large, as an EACLN member noted: *"There are benign uses of data, like helping governments predict and prevent the spread of disease. There are very positive elements that it would be very sad for society to lose."* The challenge will be to find the right balance: *"It's really about this balance between constructive and destructive use."* One member suggested that American companies—particularly those in the IT sector—may be further along than European companies in considering these issues because they are further along in discovering new ways to gather and benefit from personal data.

Audit chairs mentioned several strategies that might help companies strike the right balance:

- **Having a process for vetting new uses of data.** Is there a disciplined process for screening new uses of data? As with regulatory compliance, various functions within the company can weigh in on how customers and the public might react, using clear criteria to escalate matters that could be problematic.
- **Being transparent with customers.** Communications with customers may need to go beyond the disclosures required by regulations. Explanations of what the company is doing should be open, relevant, and easily understood. An audit chair explained, *"You have to understand what's important to customers, and if you're using their information, they have to know. Don't use a 92-page user agreement."*
- **Offering customers value.** Surveys suggest that an important factor in determining how willing customers are to accept that their data is being collected and analyzed is the perception that they are getting value in return. When asked what would encourage them to share their data, respondents in a 2018 survey said that trust was the most important factor, followed by opportunities to receive free services or special offers.[19] For some kinds of data, customers might recognize that there is a broader public interest in sharing the data, making them more likely to consent. Ms. Gardyan-Eisenlohr noted that patients and doctors interacting with the healthcare industry are more likely willing to share at least parts of their personal data if they see it as *"contributing to the health and well-being of millions."*

Experts recommend that companies think strategically about how privacy fits into the business model. Part of that approach is to balance the risks and rewards of various initiatives so that they align with the company's risk appetite. In addition, a well-designed and effectively executed privacy program can itself be a competitive differentiator.[20] Ms. Gardyan-Eisenlohr noted that Bayer is stepping up its efforts: *"People's trust in our willingness and ability to protect their personal data is key to the management of our corporate reputation."* The healthcare industry has made significant efforts to create more transparency as to the use of personal data, funds going into medical education, etc. *"This however has not been triggered by GDPR but rather it has been reinforced,"* she noted.

Building out a robust privacy system

Achieving compliance with regulations and safeguarding reputation requires a robust privacy system characterized by effective leadership and coordination with other corporate functions as well as the business units.

Effective leadership

Audit chairs noted that centralized leadership on privacy is key for addressing both regulatory and reputational issues. Many companies that are not legally required to appoint a data protection officer are appointing chief privacy officers. Experts say that elevating the privacy role to senior-management level is a growing and beneficial trend, giving the chief privacy officer the focus and authority necessary to succeed.[21] In some companies, however, privacy remains a topic within the jurisdiction of an existing role, such as the general counsel or the head of compliance.

Dr. Ulmer noted that local leadership can complement centralized leadership: *"We have international data privacy officers in each country. They know the culture, so they take care of training people and supporting us."*

Coordination across silos to achieve privacy by design

Participants underscored the importance of getting input from several relevant functions in a comprehensive and integrated way that overcomes the silos that are common in many big companies. Dr. Ulmer described the formation of a privacy audit council, which includes internal audit, compliance, IT, and business unit leaders. A member commented, *"I think that an audit council is a very strong practice: coming up with a privacy audit plan and presenting that to the audit committee. It raises the level of internal audit and focus on privacy, and it challenges management to look at things in an integrated fashion."* Another audit chair remarked, *"If you let engineers just play in their silos and optimize that feature or product as accurately and aggressively as they can, they're not thinking about GDPR. So before the engineers enhance things, we have to engage people across legal and compliance."*

Audit chairs noted that coordination with business units is key: *"The privacy piece has to be integrated in overall business decisions. There are other people brought into that, including the general counsel's office, but ultimately it's a business owner's responsibility."* Business units can help implement "privacy by design,"[22] whereby privacy is a chief consideration in the design and implementation of all business processes, from start to finish. Audit chairs also mentioned the importance of training employees: *"The privacy element has forced companies to look at training around privacy. It has been rolled out very actively across the workforce."*

The value of outside advice for meeting and exceeding current practices also emerged. Dr. Ulmer explained, *"You don't have to be stricter than others to gain trust in data privacy, but you have to do something to stay near the top. We have a data privacy advisory board, which includes politicians, NGOs, and other experts. We collect a lot of information around our planned business model and discuss it with media representatives and the data privacy community."*

An integrated data-privacy management system

Ms. Gardyan-Eisenlohr highlighted the importance of a privacy management system that integrates into business processes and makes privacy advice and measures readily available to those tasked with implementing privacy policies: *"The data privacy and business colleagues work in one digitized work process supported by the data privacy platform called Data Privacy Cockpit. The platform provides documentation, resources, and self-services. If you're a marketer, you have the data privacy cockpit available at any time. If you are setting up a new website or marketing app, you can launch the privacy statement generator for websites or apps, and it produces a privacy statement in one of nine languages and jurisdictions, together with a cookie banner and an implementation guide for IT. It's a self-service solution to meet the rising demand for privacy compliance solutions."*

Again, cross-functional collaboration is important, this time in the design of the system. *"We need to collaborate to manage privacy risks jointly. My major allies are IT, human resources, and procurement in this regard,"* Ms. Gardyan-Eisenlohr said. Along similar lines, Dr. Ulmer

mentioned *"creating a management tool that is integrated into the central processes of the company."*

Board oversight of privacy

Boards that are trying to understand and assess their companies' efforts on privacy face a familiar dilemma: navigating a complex issue with limited time and resources. How should boards delegate this task? How deep should they go in assessing how well their companies are complying with regulations and managing the issue of privacy more broadly?

The committee in charge

EACLN members noted that at many companies privacy is still an emerging issue and their boards are still trying to establish how to divide up oversight responsibilities among the full board and its committees. One member described a company-wide review of privacy activities: *"It was supervised by the audit committee, with updates on a quarterly basis, and on a half-year basis, updates to the full board. The audit committee checks into any issues that might have come up."* Another member said, *"The audit committee focuses on the control framework, but if there are big risks, the board should understand them."*

Some boards have set up compliance committees to dig deeper and uncover the root causes of emerging challenges, including compliance with privacy laws. These committees have emerged as boards have realized that the tasks required to oversee corporate compliance are becoming too burdensome for the audit committee, given all its other duties. In cases where a board has a compliance committee, it coordinates its work with the audit committee, using overlapping memberships and joint meetings.

Oversight practices

The frequency and intensity of discussions about privacy still vary among boards. At some boards, discussions are regular and frequent. *"Privacy is reported on at every audit committee meeting,"* one audit chair said. Another said, *"I suspect we talk about it in some form at every board and committee meeting."* At other boards, in-depth discussions might take place at longer intervals. *"Once a year, we put these things together. We ask about the work of the council. We have a regular agenda and then we have a focus on special topics—deep dives,"* an audit chair said.

Several members of management report on the issue. *"It lies at the intersection between the chief legal officer and the chief information security officer. Together, they report to the audit committee,"* one EACLN member said. Others mentioned reporting by internal audit, the risk management function, the chief of marketing, and even the CEO, who should *"bring this together and report to the board."*

One member noted the value of a simulation for understanding the issue and its potential demands: *"We do simulations of an event—a breach, an earthquake. We did one on data privacy a few months ago, and it was an eye-opener as to the high level of subject matter expertise and specialization that's required to address and manage these issues."*

Some boards are just getting started with privacy oversight, especially when it comes to discussions about using data in new and innovative ways that might have privacy implications. Navigating the trade-off between opportunities and risks is a challenge, a member noted: *"As a board and audit committee, many of us are not well prepared to discuss the opportunities and balancing protection against these opportunities, not only looking at risk but also at how to use data. What kind of frameworks should we use?"* Discussions are sometimes more ad-hoc and dependent on management's initiative. Boards of companies that do not process large amounts of consumer data may simply see the privacy issue as less urgent, though EACLN members' comments suggest that this attitude is starting to change.

Questions for audit committees to ask management

Audit chairs and chief privacy officer guests at Tapestry meetings have suggested several questions that boards can ask management about company privacy policies and practices:

- Is there a chief data privacy officer in place, and where is that person located?
- Has the company developed a coherent set of privacy principles?
- Is the privacy policy consistent with those principles?
- Is the policy easy to read and understand?
- Are business practices consistent with the policy?
- How does the company ensure privacy by design, and document that it does so?
- Has there been a data mapping exercise? Do you know about all of the data that the company has? Does the company have a data strategy? How does the company onboard and offboard data?
- Is data viewed as a company asset? How will the company's strategy need to change if consumers were to "own" their data?
- Are data deletion efforts meeting requirements?
- What are key performance indicators for privacy?
- What is the internal control framework? What kind of assurance is applied?

Conclusion

Companies today enjoy a wealth of opportunities to collect and capitalize on personal data. At the same time, customers, employees, and other stakeholders care about their privacy, so the pursuit of these opportunities is increasingly constrained by both regulatory and reputational considerations. These emerging concerns present significant challenges, requiring a robust

privacy team that coordinates its activities with other functions, including internal audit, IT security, and the first line of defense, the business units. Boards, too, are expanding their oversight of privacy, with audit and compliance committees taking the lead in many cases. Though practices vary, discussions of privacy are now regular and frequent on many boards, and several layers of management may report to the board, from the CEO to managers several levels down in the organization.

About this document

The European Audit Committee Leadership Network is a group of audit committee chairs drawn from leading European companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is 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, management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Biographies of guests

Ms. Eva Gardyan-Eisenlohr is Group Data Privacy Officer for Bayer. She has built the Bayer Data Privacy Function with a team of data privacy attorneys and managers across the globe. She advises the Bayer business covering the entire value chain globally in the area of data privacy, including information governance.

Until its dissolution, she served as member of the Bayer Digital Excellence Council, driving the digitalization of the corporation at board level. Digitalizing legal operations and client experience is one of her passions. She understands and guides digital business models to preserve trust and protect values.

In her prior role she was global general counsel and compliance officer for Bayer Pharma. During that time, she co-led the development and rollout of a worldwide compliance management system for the Bayer Group, covering nine compliance risk areas in 80 countries and the German headquarter organization.

She held diverse positions as senior legal and general counsel in the Bayer Group and advised Bayer's Healthcare Business as antitrust counsel. Before moving to Schering as legal counsel, Eva started her career in the crop science industry at Hoechst Schering AgrEvo.

Eva is an attorney at law, admitted to the bar of Berlin. She studied law at the University of Freiburg in Germany and holds a postgraduate degree in antitrust law from the University of Constance. Her academic training led her to study at the Institut d'Etudes Politiques and to graduate from the Ecole Nationale d'Administration, both in Paris, France.

Dr. Peter Katko is leading a global team of more than 130 lawyers in his role as Global Digital Law Leader. With digital law, EY Law supports clients mastering digital transformation in a legally compliant way. This comprises areas such as digital regulatory, digital intellectual property, e-commerce, and data privacy law. Thus, Peter specializes in data privacy law and is acting as external data privacy officer for major clients. In his projects, his goal is to combine legal expertise with operational implementation of privacy frameworks. He has more than 20 years' experience in the field of IT, intellectual property, and data privacy law.

He started his career with the Bavarian government as expert for media policy. Following that, he worked for Roland Berger Strategy Consultants and then headed the German IP/IT law practice of a US law firm. Peter has worked with several clients in the tech, telco, automotive, consumer products, pharma, and financial services industries.

Peter earned his PhD at the Max Planck Institute for Innovation and Competition in Munich.

Dr. Claus Ulmer studied law in Germany with practical studies in Haifa, Israel. He worked for a law firm in Germany focused on corporate law, mergers and acquisitions, and labor law before he joined debis Systemhaus, a DaimlerChrysler subsidiary, as legal adviser. Shortly after Claus joined debis Systemhaus it merged with Deutsche Telekom subsidiaries, and there he took

over the position as head of the data protection/privacy organization at T-Systems International Group.

In July 2002, Claus was appointed Group Data Privacy Officer at Deutsche Telekom and has been responsible since then for the worldwide data privacy strategy and governance of Deutsche Telekom. Today, Claus leads the headquarter unit for group privacy, which was formed in 2007 with over 60 data protection experts.

Claus has made many publications in national and international specialized press and published the “Data Protection Handbook Telecommunications.” He has also been a speaker at several national and international conventions.

Claus is a lecturer for the Data Protection and IT Security Academy in Ulm, Germany, which is a training institute for data protection and privacy officers. He represents the German Industry Association in the advisory board of the Data Protection Foundation of the Federal Republic of Germany.

Claus also supports start-up companies and visionary new ideas in the digital area. He is a member of the advisory board of Motionlogic, a company that provides traffic information on the basis of anonymous call records.

Claus has also supported governmental delegations of several states and companies with strategic and managerial advice for data privacy processes and management systems. He is a member of the task force of the UN Special Rapporteur on the Right to Privacy.

Appendix 2: Participants

EACLN members participating in all or part of the meeting included the following:

- Werner Brandt, Siemens
- Aldo Cardoso, Bureau Veritas
- Carolyn Dittmeier, Generali
- Eric Elzvik, Ericsson
- Renato Fassbind, Nestlé and Swiss Re
- Margarete Haase, OSRAM Licht
- Liz Hewitt, Novo Nordisk
- Dagmar Kollmann, Deutsche Telekom
- Helman le Pas de Sécheval, Bouygues
- David Meline, ABB
- Guylaine Saucier, Wendel
- Erhard Schipporeit, RWE
- Alan Stewart, Diageo
- Charlotte Strömberg, Skanska
- François Thomazeau, Bolloré

North American Audit Committee Leadership Network members participating in all or part of the meeting included the following:

- Chuck Noski, Microsoft and Booking Holdings

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

- Ute Benzel, Germany, Switzerland, and Austria Regional Managing Partner
- Jean-Yves Jégourel, EMEIA Assurance Leader
- Julie Teigland, EMEIA Area Managing Partner

Appendix 3: Questions for audit committees

- ? What new and emerging privacy regulations are your board most worried about?
- ? What kind of reputational issues related to privacy have come up as concerns of your board?
- ? What kind of efforts are underway at your company to assess and comply with privacy regulations? What kind of challenges are emerging?
- ? How is your company thinking about issues of trust and reputation as it develops new ways of using the data at its disposal?
- ? How is your company's privacy team structured? How does the board ensure that its leader has clout in the organization?
- ? Which committee of the board takes the lead on privacy? How do other committees and the full board get involved?
- ? What kind of practices do you use to oversee privacy? Who comes to the board and how often is the issue discussed?
- ? Should boards be more proactive about addressing forward-looking privacy issues? How much should they rely on management to alert them to any issues?

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members in connection with the meeting.

[2] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018.

[3] "Art. 5 GDPR: Principles Relating to Processing of Personal Data," GDPR.EU, accessed August 30, 2019.

[4] "Art. 7 GDPR: Conditions for consent," GDPR.EU, accessed August 30, 2019.

[5] "GDPR Key Changes," EU GDPR Portal, accessed August 21, 2019.

[6] "GDPR Key Changes," EU GDPR Portal.

[7] "GDPR Key Changes," EU GDPR Portal.

[8] Neil Hodge, "French Data Regulator Fines Google Under GDPR," *Compliance Week,* January 22, 2019.

[9] Madhumita Murgia, "Marriott to Be Fined £99m for GDPR Breach," *Financial Times,* July 9, 2019.

[10] Paul Demery, "What the EU's GDPR Means for B2B Companies," *Digital Commerce 360*, May 25, 2018.

[11] Daisuke Wakabayashi, "California Passes Sweeping Law to Protect Online Privacy," *New York Times,* June 28, 2018.

[12] Dipayan Ghosh, "What You Need to Know about California's New Data Privacy Law," *Harvard Business Review,* July 11, 2018.

[13] Cecilia Kang, "Tech Industry Pursues a Federal Privacy Law, on Its Own Terms," *New York Times,* August 26, 2018.

[14] US Chamber of Commerce, "U.S. Chamber Releases Privacy Principles," news release, September 6, 2018.

[15] John Hendel, "'Embarrassing': Congress Stumbles in Push for Consumer Privacy Bill," *Politico,* July 12, 2019.

[16] "IBM Survey Reveals Consumers Want Businesses to Do More to Actively Protect Their Data," Harris Poll, Harris Insights and Analytics, accessed August 21, 2019.

[17] Warwick Ashford, "Businesses Bracing for GDPR Data Deletion Requests," *ComputerWeekly.com,* December 1, 2017.

[18] Jaclyn Jaeger, "Elements of a Best-in-Class Data Privacy Program," *Compliance Week,* November 26, 2018.

[19] Foresight Factory, *Global Data Privacy: What the Consumer Really Thinks* (Acxiom and the Global Alliance of Data-Driven Marketing Associations, May 2018), 12.

[20] Jaeger, "Elements of a Best-in-Class Data Privacy Program."

[21] Doug Pollack, "Privacy Is Taking Its Place in the C-Suite," IDExperts, January 24, 2017.

[22] "Data Protection by Design and Default," Information Commissioner's Office, accessed September 24, 2019.