THE GUIDE TO **DATA AS A CRITICAL ASSET**

Editor
Mark Deem

The Guide to Data as a Critical Asset 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in April 2022
For further information please contact Natalie.Hacker@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-859-8

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Preface

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Artificial intelligence and other forms of sophisticated computing and automation are no longer the stuff of science fiction: the future has become the present (or, at least, the near future). None of this would be possible without data. But even 'classic' business models now rely on the use of all forms of data, and its protection – whether in a data privacy or any other sense – is more important than ever.

Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset* takes a unique view of data. Instead of looking at it through a regulatory and risk lens, the contributors to this book – edited by Mishcon de Reya partner Mark Deem – aim to steer companies through the gathering, exploitation and protection of all types of data, whether personal or not.

Global Data Review
London
March 2022

Privacy by Design and Data Minimisation

Alan Charles Raul, Francesca Blythe and Sheri Porath Rockwell[1]
Sidley Austin LLP

Overview

The principle of 'privacy by design' refers to the practice of integrating and embedding privacy and data protection into the development and implementation of information technology systems, business practices and policies, and products and applications. It recognises the limitations of relying solely on consumer choice or after-the-fact privacy regulation (e.g., fines for data breaches) in ensuring the privacy of personal information, particularly in this era of big data when it can be challenging for average persons to comprehend the complex ways in which organisations are collecting and processing their personal data. Rather, privacy by design takes a proactive approach and advocates for the early consideration of privacy when designing technologies, products and management systems, and encourages a holistic view that not only uses privacy-enhancing technologies (e.g., encryption or anonymisation of data) but also integrates privacy considerations into organisational policies and practices (such as mandated data minimisation) and procedures (such as the designation of personnel to address privacy issues throughout the life cycle of a product or system, or conducting privacy risk assessments).

The term 'privacy by design' was originally coined by Ann Cavoukian, PhD, in the late 1990s during her tenure as the Information and Privacy Commissioner of Ontario, Canada. Beginning in 2009, Dr Cavoukian published a series of papers that recommended addressing these limitations by approaching privacy from a 'design thinking' perspective, using a holistic approach that embeds privacy 'into every standard, protocol and process

1 Alan Charles Raul is a partner and Francesca Blythe and Sheri Porath Rockwell are senior managing associates at Sidley Austin LLP.

that touches our lives'.[2] In 2010, she distilled these concepts into The 7 Foundational Principles of Privacy by Design – a framework that was adopted in 2010 by the 32nd International Conference of Data Protection and Privacy Commissioners[3] (now renamed the Global Privacy Assembly). Since that time, regulators around the world have endorsed the concept of privacy by design and a variety of laws have integrated elements of it (e.g., the EU General Data Protection Regulation (GDPR)[4] and certain US sectoral and state data privacy laws). It should be noted, however, that the concept of privacy by design existed long before Dr Cavoukian's branding of it in, for example, the US Privacy Act of 1974, under which data minimisation is a requirement.

However, despite the concept of privacy by design having existed for a large number of years, many organisations still struggle with how to meet and implement the requirements in practice. In this chapter, we seek to demystify the concept, drawing on examples of how privacy by design can be implemented by organisations in practice.

The 7 Foundational Principles of Privacy by Design

The 7 Foundational Principles, as published by Dr Cavoukian, are as follows:[5]

> *1. Proactive not Reactive; Preventative not Remedial*
> *The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, PbD comes before-the-fact, not after.*

---

2 Ann Cavoukian, PhD (www.ipc.on.ca), 'Privacy by Design – The 7 Foundational Principles: Information and Mapping of Fair Information Practices' (rev. 2011), Information and Privacy Commissioner of Ontario, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (last accessed 13 January 2022). The Principles are themselves founded in the Fair Information Practice (FIP) principles (enacted into law in the US Privacy Act of 1974), but the intention was to 'go beyond them to seek the highest global standard possible. Extending beyond FIPs, privacy by design represents a significant "raising" of the bar in the area of privacy protection'.

3 https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf (last accessed 17 Jan. 2022).

4 Regulation (EU) 2016/679.

5 Ann Cavoukian, PhD, 'Privacy by Design – The 7 Foundational Principles' (2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (last accessed 14 Jan. 2022).

2. Privacy as the Default Setting

. . . Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of individuals to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, Not Zero-Sum

Privacy by Design (PbD) seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

Privacy by Design (PbD), having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PbD ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep It Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Integration into regulatory guidance and privacy legislation

Privacy by design and the principles of the approach appear in several regulatory regimes and have been increasingly cited by regulators as a foundational best practice to fully protect individuals' privacy rights.

US Privacy Act of 1974

The US Privacy Act of 1974 essentially anticipated and embodied the principles of privacy by design. The US Congress stated in the 1974 Act that the purpose of the new law was to mandate 'safeguards for an individual against an invasion of personal privacy by requiring' federal agencies to:

> *collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.*[6]

Federal agencies were required to develop and publish (for review and comment) detailed planning documents to identify, in advance, how they would proceed to implement the fair information principles in practice.[7]

The US Computer Matching and Privacy Protection Act of 1988 amended the 1974 Privacy Act. As summarised by the US Department of Justice, the amendments added:

> *procedural requirements for agencies to follow when engaging in computer-matching activities, provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated, and require that agencies engaged in matching activities to establish Data Protection Boards to oversee those activities.*[8]

Of course, the Privacy Act of 1974 was itself predicated on prior work, especially the 1973 Report of the Secretary's Advisory Committee on Automated Personal Data Systems, US Department of Health, Education and Welfare (HEW), 'Records,

6 Public Law 93-579, as codified at 5 U.S.C. 552a, available at https://dpcld.defense.gov/Portals/49/Documents/Privacy/pa1974.pdf (last accessed 16 Feb. 2022).

7 See 5 U.S.C. 552a(e).

8 See Overview of the Privacy Act: 2020 Edition, available at https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction#LegHistory (last accessed 16 Feb. 2022).

Computers, and the Rights of Citizens'.[9] The 1973 HEW Report focused on the essential need of each 'new personal data system' to incorporate privacy protections in advance by mandating that 'those responsible for the system . . . as well as those specifically charged with designing and implementing the system' should answer questions such as:

> *What purposes will be served by the system and the data to be collected? How might the same purposes be accomplished without: collecting these data? . . . Is it necessary to store individually identifiable personal data in computer-accessible form, and, if so, how much? Is the length of time proposed for retaining the data in identifiable form warranted by their anticipated uses?*

Moreover, the 1973 HEW Report specifically intended that this 'process should at least suggest limitations on the collection and storage of data'.[10]

US E-Government Act of 2002

As the internet began to change relationships 'among citizens, private businesses and Government', Congress passed the E-Government Act, which codified the proactive approach to privacy protection that Dr Cavoukian would later describe as the first of The 7 Foundational Principles of Privacy by Design.[11] Specifically, the Act requires federal agencies to conduct privacy impact assessments before developing or procuring new technologies that process personal information or initiating new electronic collections of personal information. This allows agencies to anticipate privacy risks before they happen and evaluate alternative processes to mitigate such risks.[12]

2010 Jerusalem Resolution

Calls to integrate privacy by design into national privacy legislation were taken up outside the United States in October 2010, at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem. There, privacy regulators

---

9 Available at https://www.justice.gov/opcl/docs/rec-com-rights.pdf (last accessed 16 Feb. 2022).

10 The 1973 HEW Report, at 51–52.

11 Pub. L. No. 107-347, Dec. 17, 2002.

12 E-Government Act of 2022, 44 U.S.C. § 101 et seq. (Office of Management and Budget, 'OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002', 26 September 2003), https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html (last accessed 25 Jan. 2022).

from around the world unanimously passed a resolution recognising privacy by design as 'an essential component' of fundamental privacy protection (the Jerusalem Resolution). The Jerusalem Resolution noted that existing regulations and policies were not sufficient to safeguard individual privacy rights in the face of the 'ever-growing' and 'systemic' effects of information technologies and large-scale networked infrastructure.[13] To fully protect individuals' privacy rights, the Jerusalem Resolution concluded that it was necessary to embed privacy by default into the design, operation and management of information technology systems. To operationalise these goals, the Jerusalem Resolution encouraged organisations to use The 7 Foundational Principles to establish privacy as their default mode of operation and urged privacy regulators to use these principles to develop privacy policy and legislation in their respective jurisdictions.[14]

US Federal Trade Commission report on protecting consumer privacy

In 2012, the US Federal Trade Commission (FTC) recognised privacy by design as one of the three pillars of the FTC's new privacy framework set forth in its innovative report 'Protecting Consumer Privacy in an Era of Rapid Change' (the FTC Report). The FTC Report was informed by a series of roundtable discussions about the future of privacy regulation with stakeholders convened by the FTC between December 2009 and March 2010. Participants concluded that the existing privacy regulatory frameworks – the 'notice and consent' model (i.e., reliance on privacy policies and consumer notices) and the 'harm-based' model (i.e., protecting consumers from privacy harms after the fact) – were failing adequately to regulate new business models that collected and used consumers' information in ways that were often invisible to consumers.[15]

Privacy by design was identified as one of three pillars of the FTC's new privacy framework designed to address these shortcomings in privacy regulation.[16] The FTC's conception of privacy by design reflects the holistic approach and requires companies

13 Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners, 27–29 October 2010, https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf (last accessed 13 Jan. 2022).

14 id.

15 Federal Trade Commission, 'Protecting Privacy in the Era of Rapid Change' (March 2012) (FTC Report), at p. 2.

16 The other two pillars were simplified choice for businesses and consumers and greater transparency. FTC Report at p. i.

to implement both substantive and procedural privacy protections. The substantive protections include adopting reasonable security measures, practising data minimisation and limiting data retention periods, and taking steps to ensure the accuracy of data collected when it could cause significant harm or be used to deny consumers' services.[17] The procedural safeguards include implementation of comprehensive privacy programmes that designate personnel responsible for privacy protection, and require risk assessments that address product design and development, controls designed to address identified risks, oversight of service providers, and evaluation and adjustment of the programme in light of regular testing and monitoring results.[18] Taken together, the goal is to shift the burden for protecting privacy away from consumers and to encourage companies to integrate, by default, strong privacy protections that do not rely on individual choice or action.[19]

The FTC Report does not have the force of law and the FTC has not issued rules that prescribe how companies should implement privacy by design in practice. Nevertheless, the FTC Report has served to guide privacy practices and introduce to organisations in the United States privacy by design concepts such as data minimisation and rights to correct data. As described below, some of these principles have been incorporated into new US state data privacy laws.

Privacy by design and by default in European Union and United Kingdom

In the European Union, privacy by design became an enforceable legal obligation in May 2018 by virtue of the GDPR.[20] The obligation was retained by the United Kingdom, where the GDPR is retained in domestic law post-Brexit as the UK GDPR.

Article 25 of the GDPR (Data protection by design and default) provides that controllers (i.e., the organisation responsible for deciding how and why personal data is processed) must implement 'appropriate technical and organisational measures . . . designed to implement data protection principles . . . to meet the requirements of the GDPR and protect the rights of data subjects'.[21] Further, Article 25 requires that such measures be implemented to ensure that 'by default, only personal data which are

17 FTC Report at p. vii.

18 ibid., at p. 31.

19 ibid., at p. 23.

20 Note that certain elements of the principle of privacy by design existed in Data Protection Directive 95/46/EC, which was repealed by the General Data Protection Regulation (GDPR).

21 GDPR, Article 25(1).

necessary for each specific purpose of the processing are processed'.[22] These concepts should be implemented 'both at the time of the determination of the means for processing and at the time of the processing itself'.[23]

Although the requirements of privacy by design and by default under the GDPR strictly apply only to controllers, the GDPR recognises that processors (e.g., vendors acting on the instructions of the controller) and product manufacturers play an essential role in compliance. In particular, controllers often outsource a given processing activity to a processor (e.g., a cloud service provider) or purchase a product that allows the controller to process personal data (e.g., a device that facilitates access via biometric data). In such cases, the processor and product manufacturer can be best placed to identify the data privacy risks involved, and should use their expertise to design and implement products that embed the principle of privacy by design and by default.

US sectoral and state data privacy laws incorporating privacy by design

In addition to the laws described above that apply to the US federal government, several US federal and state laws regulating private companies' use of personal information also incorporate principles of privacy by design. For example, the US Children's Online Privacy Protection Act incorporates the principle of data minimisation in that it requires operators collecting personal data of children under 13 years of age to ensure they are only collecting information that is reasonably necessary to participate in a given activity.[24] Data minimisation requirements are also included in federal laws regulating financial information[25] and health data.[26]

22 ibid., Article 25(2).

23 ibid., Article 25(1).

24 16 C.F.R. § 312.7; FTC, 'Complying with COPPA: Frequently Asked Questions' (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last accessed 17 Jan. 2022).

25 16 C.F.R. § 314.4(c)(6)(ii) (FTC Safeguards Rule implementing Gramm-Leach-Bliley Act) (effective 9 December 2022) (requiring financial institutions to periodically review data retention policies to minimise unnecessary data retention).

26 See, e.g., 45 C.F.R. § 164.502(b) (Health Insurance Portability and Accountability Act Privacy Rule requiring disclosures of protected health information be limited to minimum necessary to accomplish intended purpose).

Privacy by design principles are also increasingly found in consumer data privacy laws being enacted at the state level. These laws expressly require businesses to implement data minimisation requirements, disclose data retention periods or principles governing their data retention periods, and to assess privacy risks before processing certain types of data by conducting privacy impact assessments.[27]

Implementing privacy by design – strategic considerations

As acknowledged by the European Data Protection Board Guidelines, there is no 'one-size-fits-all' solution to implementing privacy by design and default. The needs and complexity of organisations vary so widely, as do their internal design processes. How organisations operationalise privacy by design will depend on a number of factors, including available resources and the nature of data that is being processed, taking into account legitimate interests and other needs of the business.

We provide a high-level overview below on how to incorporate privacy considerations into the design process based in part on the work of Jaap-Henk Hoepman[28] and R Jason Cronk.[29]

Understand specific goals and objectives of product or system

What is the purpose of the system or product being designed? Articulation of what the system or the product aims to achieve provides the necessary context from which privacy protection choices can be considered. Consistent with design principles, it is important that the goal of the system or project be as concrete and specific as possible.[30] For example, if considering an electricity smart metering system, defining the goal as 'billing users depending upon how much electricity they consume at each billing rate' is more useful than 'billing users based upon their energy consumption habits'.

---

27 See, e.g., California Privacy Rights Act, Cal. Civ. Code, § 1798.100(c) (requiring data minimisation) and § 1798.100(a)(3) (prescribing limits on data retention periods); Virginia Consumer Data Privacy Act, § 59.1-578 (F) (limitations on data collection and retention) and § 59.1-576 (data protection assessments); Colorado Privacy Act, § 6-1-1308(2) (duty of data minimisation), § 6-1-1308(3) (purpose limitation) and § 6-1-1309 (requiring data protection assessments).

28 Jaap-Henk Hoepman, *Privacy is Hard and Seven Other Myths: Achieving Privacy Through Careful Design* (The MIT Press, Cambridge, Massachusetts, 2021); Jaap-Henk Hoepman, *Privacy Design Strategies (The Little Blue Book)* (Jan. 27, 2020).

29 R Jason Cronk, *Strategic Privacy by Design* (IAPP, Portsmouth, New Hampshire, 2018).

30 Seda Gürses, Claudia Diaz and Carmela Troncoso, 'Engineering Privacy by Design Reloaded' (2015), http://carmelatroncoso.com/papers/Gurses-APC15.pdf (last accessed 13 Feb. 2022).

Identify information needed to accomplish goals and objectives

Entities should conceptualise the data that will be needed to accomplish the goal (e.g., billing users based on electricity consumption per billing period) and additional requirements to ensure the quality and integrity of the system or application. For example, consider whether additional data may be needed to verify the identity of users or to prove that a customer has received a product.[31] Consideration should also be given to special categories of individuals in scope (e.g., children or vulnerable individuals) and the types of personal data processed (e.g., information about health), as such considerations will inform the types of controls to be implemented.

Evaluate applicability of privacy design strategies

With the goal and the types of personal data at issue in mind, entities should evaluate various privacy-protective strategies to determine the controls (both technical and organisational – see below) that are best suited to minimise privacy risks in the product or system being evaluated while taking account of the costs, legitimate interests and desirable business purposes. The process should be a holistic endeavour that takes account of the different types of processing at issue and the business needs and legitimate interests of the organisation, and that involves diverse stakeholders, including the project owner, marketing, finance and technical experts, and privacy officers.[32] Non-technical participants in the process can use the various strategies as questions to ask or talking points to raise in the design process to help ensure privacy has a 'seat at the table'.

Technical privacy strategies

- *Minimise*: The most privacy-protective strategy has always been to minimise the collection of personal data. For data that has already been collected, minimisation can also include deletion and destruction.
- *Abstract*: Attempt to collect personal data at the highest possible level of abstraction. For example, rather than collecting precise geolocation data, assess whether processing purposes can be met if users are instead identified by an area code or street name.

---

31 R Jason Cronk, *Strategic Privacy by Design*, op. cit. note 29, above.

32 Jaap-Henk Hoepman, *Privacy is Hard and Seven Other Myths: Achieving Privacy Through Careful Design*, op. cit. note 28, above.

- *Hide*: Protect personal data from unauthorised disclosure or access. This may involve implementing access controls, encrypting data, or anonymising or pseudonymising data.

Organisational strategies

- *Inform*: Be transparent about what data is collected, and how and why it is processed. This is typically achieved through the development of privacy policies and notices.
- *Control*: Give data subjects some control over the processing of their data by, for example, allowing them to provide consent, opt-outs or rights to delete data.
- *Govern*: Implement internal privacy governance structures and the assignment of personnel who are responsible for compliance and educating the workforce.
- *Demonstrate*: Include procedures for the organisation to document and demonstrate its compliance with privacy regulations (i.e., the concept of accountability). This may include keeping records of responses to data subject requests, completing data privacy impact assessments, undertaking privacy audits or obtaining privacy compliance certifications (e.g., HITRUST or TRUSTe).

Review and re-evaluate

The requirements of privacy by design should be considered throughout the life cycle of the processing. As technologies evolve, organisations may need to make changes to the measures implemented and require their vendors to do the same.

Security by design – Secure Silicon project

Design thinking also exists in the cybersecurity space, under the moniker of 'security by design'. One area of focus in this area is chip design, as the vulnerabilities of integrated circuit chips are posing growing security threats. One of the organisations that is attempting to address security by design is the US Defense Advanced Research Projects Agency (DARPA), through its Automatic Implementation of Secure Silicon (AISS) programme.[33] The programme, which is in an early stage of development,

33 'DARPA Selects Teams to Increase Security of Semiconductor Supply Chain', Defense Advanced Research Projects Agency (May 27, 2020), https://www.darpa.mil/news-events/2020-05-27 (last accessed 12 Feb. 2022).

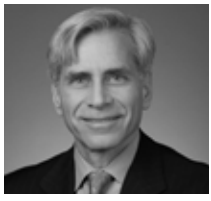
aims to bring together academic, commercial and defence industry researchers and engineers to design tools that will allow security to be worked into chip design from the outset.

Conclusion

Organisations globally are seeking to incorporate the concept of privacy by design into their systems, products and processes. However, the means for doing so will differ between organisations and depend on the processing activity and types of data in question, as well as the costs and other legitimate interests and business needs of the organisation. Key is to ensure privacy by design is considered at the initial stages of planning – whether this be for a new IT system, policy, data-sharing initiative or processing purpose.

To date, enforcement for non-compliance with the principle of privacy by design has primarily been in the European Union. The fines have varied from the significant (e.g., €14.5 million by the German data protection authority) to the relatively smaller (e.g., €130,000 by the Romanian data protection authority). However, what is clear is that this principle, and non-compliance with the same, is garnering attention from privacy regulators and probably will increasingly continue to do so. This should therefore be viewed as a priority by companies at the outset of any new initiative. As confirmed by Tim Cook (chief executive of Apple) at a conference in 2019: 'You don't bolt on privacy, you think about it in the development process of products . . . You have to design it in.' [34]

34 Salesforce Dreamforce Conference held on 19 November 2019, see https://www.salesforce.org/events/dreamforce-2019/ (last accessed 23 Feb. 2022).



ALAN CHARLES RAUL
Sidley Austin LLP

Alan Raul is the founder and leader of Sidley Austin's highly ranked privacy and cybersecurity practice. He represents companies on US and international privacy, cybersecurity and technology issues. Alan advises on global regulatory compliance, data breaches and crisis management. Alan also focuses on issues concerning national security, constitutional and administrative law. He handles enforcement and public policy issues involving the FTC, state attorneys general, SEC, DOJ, FBI, DHS/CISA, the intelligence community, as well as other federal, state and international agencies.

Alan previously served in government as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the US Department of Agriculture, and Associate Counsel to the President. He maintains a national security clearance. He holds degrees from Harvard College, Harvard Kennedy School of Government and Yale Law School. Alan serves as a lecturer on law at Harvard Law School, where he teaches the course 'Digital Governance: Privacy and Technology Trade-offs'. He is a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the governing board of directors of the Future of Privacy Forum, and the Council on Foreign Relations.

FRANCESCA BLYTHE
Sidley Austin LLP

Francesca Blythe advises international clients on a wide range of data protection, privacy and cybersecurity issues. Francesca has in-depth experience with a number of industries, including asset management and private equity, payments, technology, e-commerce and manufacturing. She has a particular focus on life sciences, where she advises on a broad range of issues in relation to, for example, real-world evidence and secondary research, clinical studies and investigations, digital health and use of novel technologies (including artificial intelligence).

Francesca was previously in-house counsel at the largest international health and beauty retailer in Asia and Europe. While there, she regularly gave advice on compliance and strategies relating to data protection laws, including subject access requests, privacy impact assessments, direct marketing campaigns, biometrics and employee monitoring. She also assisted in the planning and delivery of a UK-wide privacy audit and managed a global privacy compliance project.

SHERI PORATH ROCKWELL
Sidley Austin LLP

Sheri Porath Rockwell focuses on privacy and cybersecurity law, as well as complex commercial litigation. She advises companies on privacy compliance and corporate data protection programmes, including compliance with federal and state privacy laws. Sheri is also a member of Sidley's California Consumer Privacy Litigation Task Force, a dedicated group of lawyers focused on the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), counselling clients on how to mitigate litigation risks. Sheri regularly counsels businesses about compliance with the CCPA and CPRA, the Health Insurance Portability and Accountability Act, and other state and federal privacy laws. She is an International Association of Privacy Professionals Certified Information Privacy Professional/US and regularly blogs and delivers presentations regarding emerging domestic privacy law. Sheri serves as the chair of the Privacy Law Section of the California Lawyers Association, which she helped found.

Sheri has experience in litigating a variety of complex commercial matters, including copyright, trademark and right of publicity actions, commercial class actions, complex real estate actions and contract disputes. She has litigated in federal and state court and in arbitration and mediation settings. Additionally, Sheri has successfully negotiated with state and federal regulators to avert and settle administrative proceedings.

SIDLEY

Sidley Austin LLP's privacy and cybersecurity practice group offers clients a global and interdisciplinary team of lawyers focused on a broad range of emerging issues. We have been practising actively in this ever-changing sector since 1998 and have more than 70 lawyers worldwide who work on data privacy and cybersecurity issues in the United States, Europe and Asia and closely monitor the rapidly developing privacy laws around the world. Our global presence allows Sidley to offer our international clients both great depth of knowledge and experience, as well as 24/7 coverage, which can be important in time-critical situations.

Our lawyers have significant experience in addressing cutting-edge cybersecurity risks, both from a proactive counselling and compliance assessment perspective, as well as from a reactive incident response to internal reviews, government investigations and litigation. Based on our extensive experience with companies that need to protect sensitive corporate and personal data, we have developed a depth of knowledge about the rapidly evolving legal standards for cybersecurity across the United States and internationally.

Our lawyers remain on the leading edge of cyberlaw with innovative thought leadership. In addition to frequent speaking engagements, national media appearances, news alerts, webinars and publications, we keep clients abreast of emerging issues through our industry-leading blog, Data Matters, and by organising many industry privacy and cyber networks and roundtables, including Women in Privacy and dplegal.

With more than 1,900 lawyers and over 40 focused practice groups worldwide, Sidley provides best-in-class legal services to meet the needs of executive leaders and counsel.

70 St Mary Axe
London, EC3A 8BE
United Kingdom
Tel: +44 20 7360 3600

www.sidley.com

1999 Avenue of the Stars,
17th Floor
Los Angeles, CA 90067
United States
Tel: +1 310 595 9500

1501 K Streeet, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000

Alan Charles Raul
araul@sidley.com

Francesca Blythe (London)
fblythe@sidley.com

Sheri Porath Rockwell
sheri.rockwell@sidley.com

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset*, edited by Mishcon de Reya partner Mark Deem, offers a unique approach to data that helps steer companies through their gathering, exploitation and protection of all types of data – whether personal or not – and looks at data as an asset class that is increasingly important across all industries.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-859-8