GDR

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

Editor
Mark Deem

The Guide to Data as a Critical Asset 2022

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

Introduction

Mark Deem[1]
Mishcon de Reya LLP

For much of the past decade, the focus of legal practitioners, legislators and regulators alike has been on personal data and the protections that should be afforded data subjects, often the unwitting participants on a journey of technical discovery in which third parties seek to unlock the value of data that has been created. This focus is increasingly being seen for what it is – too narrow.

In 2006, Clive Humby, the British mathematician who with his wife, Edwina Dunn, helped a leading supermarket create its loyalty programme, declared data to be the 'new oil': early recognition of the manner in which big data was set to revolutionise the marketing world. In 2017, *Economist* ran a report under the title, 'The world's most valuable resource is no longer oil, but data'. Indeed, equating innovative applications of data with fossil carbon fuels is increasingly a common refrain. It should be noted that others have equated it with gold, neatly acknowledging that, whether gold or oil, it is now seen as the equivalent of a physical asset.

The analogy (especially as formulated by *Economist*), however, is not without problems. Although data and oil are both commodities, the true value of oil derives from the extent and supply of a finite resource and is achieved through consumption, whereas data has no such constraints either in terms of quantity or availability and it will generally be replicated rather than consumed.

A more nuanced reading of Humby perhaps offers greater insight: that unstructured data, like crude oil, has limited worth but – through refinement – its significant value can be unlocked. Rather than merely a commodity or fixed asset, data performs as any other financial asset of a business.

1 Mark Deem is a partner at Mishcon de Reya LLP.

Given its ability to affect every aspect of our commercial and personal lives, it is increasingly more appropriate to focus on the role of data as a critical asset, perhaps the critical asset.

Indeed, the ubiquity of data and its unparalleled rate of creation means that it has the potential to be a rich source of legal work. From the moment of its creation to its ultimate destruction, data necessarily has a value, capable of and requiring control, commercialisation and protection. Whether seen in a privacy, security, employment, competition, intellectual property, corporate or commercial context, clients will require transactional, regulatory and contentious legal solutions in respect of their wider data assets, rather than simply personal data.

These solutions will need to be delivered in an agile, dynamic and seamless way and will perhaps inevitably be less respectful of more traditional legal service lines. Clients will demand that their lawyers are able to move seamlessly from advising on transactional and early-stage regulatory matters through to new breeds of litigation disputes.

It is therefore timely that the launch of this book by Global Data Review seeks to widen the legal debate concerning data – from issues of privacy and personal data protection to its role as a critical asset – not least because newer internet technologies (whether artificial intelligence, the virtual world of the metaverse or its close cousin, the omniverse) will confirm that we are moving into a world made of and governed by data assets.[2]

A new approach?

For hundreds of thousands of years, leaking oil in the tar pits of California simply served to trap prehistoric mammals. It was only with the advent of the car that a material that was seen as a stain on the land became desirable. A similar analogy can be made between modern technology and data.

In its crude and unrefined form, oil is useless for cars and undefined data is the same, simply a morass. Thus, it is self-evident that what gives oil its value is the manufacturing process; a process that presents challenges, in and of itself, of ownership, storage, protection, transport and security.

---

2 At the time of writing, John Edwards, appointed in January 2022 as UK Information Commissioner, had just delivered his first speech at the IAPP Data Protection Intensive: UK 2022 Health and Safety Conference in London (24 Mar. 2022), in which he said 'business leaders see the financial benefits of good data protection model as a means of protecting the largest business asset that doesn't appear on their balance sheet'.

In the case of data, the issues are very similar. How is the data gathered? How is it combined with other data? What rules govern the use of that data and its relationship with other data? What is the purpose of the exercise? What rules govern the storage of that data? Who can have access to that data? What is the relevance of that data? And how is data made both available and secure?

All these issues raise questions, present challenges and demand support and solutions from a legal perspective.

Emerging technologies promise not only to revolutionise the way that companies use data but will also present huge legal challenges to that use because of the ability that living and working in the metaverse presents to map the behaviour of individuals.

According to those developing the metaverse, these 3D virtual worlds will enable us to shop, play, holiday, become educated and work in a way that will see us becoming inextricably bound up with increasingly more complex computer systems – a process that many involved in technology are calling augmentation.

We are entering a world in which the gathering, sharing and trading of data assets (and associated permissions) will become huge and extremely controversial and the legal implications will increase in intensity.

The criticality of data assets

It is a future world of data gathering and interpretation for which some companies are already preparing. However, others are woefully unprepared, according to Leslie Willcocks, Emeritus Professor of Work, Technology and Globalisation at the London School of Economics and Political Science, who has researched global work trends for more than 30 years.

According to Professor Willcocks, whose latest book, *Robotic Process and Cognitive Automation: The Next Phase*, examines the adoption of robotics and AI in the economy, the ability of companies to adopt technology is now crucial to their survival.

> *What I see is about 20 percent of the organisations that have moved successfully to digital are breaking away from other companies in terms of profitability and financial health and the gulf they are establishing is likely to become irreversible.*[3]

3 Professor Leslie Willcocks speaking at the Future Intelligence/Cooley AI Conference held by the Institution of Engineering and Technology at Savoy Place, London, on 24 May 2017

This underlying trend, Professor Willcocks says, will now accelerate as a result of the coronavirus pandemic creating early casualties in retail, aviation and leisure.

According to KPMG, the accountancy and consulting firm, many companies are struggling to mine and refine data successfully:

> *The reasons are many, including data fluency, complex and siloed system architectures, access controls and policies, cultural issues, and interoperability issues across the business. However, leading organisations are fundamentally reimagining their relationship with data and, as a result, transforming IT's role to materially impact business outcomes. Over the next three to five years, leading companies are expected to adopt four key data principles into their operating models: clarify data accountabilities across the enterprise; embed data fluency across the enterprise as a strategic imperative; move data curation into the business as a core competency; and reimagine a frictionless data supply chain.*[4]

These are key principles in the journey to becoming footloose, digital, data-driven enterprises and will require legal underpinning. Data will not only be critical to the success of the way a company is organised, the interpretation of it will also be critical to the success of a company's business. This is because, in the future, decisions made using data are highly likely to become embedded in a company and the AI selection and interpretation of data resulting from the quality of this data will be critical, because bad or contested data will instantly become a business risk.

A further trend that also needs to be understood in this fast-moving world is data integrity. For any data asset to be valuable in an organisation it has to be trusted. To ensure that integrity, it has to be protected and it has to have been cleaned. If data from outside is acquired or collated to fulfil a particular purpose, it must also have the same integrity.

A brave new world?

This new data world thus immediately raises a number of legal questions. However, we need to widen the aperture to consider the legal issues of the protection of data, rather than simply data protection.

---

4 KPMG International paper, 'Data as an asset: Initiate your journey to unlock data's full potential' (2019), at p. 3, https://home.kpmg/content/dam/kpmg/uk/pdf/2019/11/future-of-it.PDF (last accessed 3 Mar. 2022).

Whether in a business as usual context, a routine audit or, indeed, as part of corporate merger and acquisition due diligence activity, the questions we can expect to be asked time and again will be: Where did the data come from? How was it obtained? What will our organisation use it for? Do we have the rights to use it in that manner? Are we holding that asset in a secure and safe manner?

Just as important as a process of auditing data will be a constant reassessment of the use of that data to ensure that it is not being processed in a way that can cause legal issues.

In this Guide, we seek to explore with leading practitioners the manner in which we can take a fresh look at data as a wider class of asset within a business context. It requires an assessment, which takes us beyond the more familiar domain of data protection legislation and calls for us to understand the precise value of data and the use to which it is being put. Although we cannot – and must not – ignore the importance of privacy and data protection, the world is starting to embrace the broader context of data assets and we need to respond and frame legal solutions accordingly.

Although seeking to draw an analogy between data and oil might be questionable, the critical role of data assets in our future is undeniable.

I hope you enjoy the Guide.

MARK DEEM
Mishcon de Reya LLP

Mark is a disputes partner in the innovation department and a specialist in technology, media and telecommunications (TMT) litigation, contentious privacy and cybersecurity issues and financial services disputes.

He has considerable experience of complex domestic and cross-border litigation, international arbitration and regulatory matters. He has conducted litigation in all commercial divisions of the English High Court, Court of Appeal, Supreme Court and Court of Justice of the European Union. He has represented clients in international arbitration proceedings under the rules of the ICC, LCIA, RIDR and IFTA, and has a broad experience of mediation and other dispute resolution mechanisms.

Mark is a solicitor-advocate, with rights to appear in all courts in England and Wales and is well known for his proficiency in managing clients' exposure to the risk and cost of commercial disputes through the innovative use of after-the-event insurance, third-party and other litigation funding arrangements.

He is also co-author of the forthcoming book, *AI on trial*, examining the legal, regulatory and ethical framework needed to deploy artificial intelligence in a safe and acceptable manner.

Mishcon de Reya

Mishcon de Reya LLP is a law firm with offices in London and Singapore. Founded by Victor Mishcon in a one-room office in Brixton in 1937, it now employs more than 900 people, with over 500 lawyers offering a wide range of legal services to companies and individuals. Mishcon de Reya services an international community of clients and provides advice in situations where the constraints of geography often do not apply. The work the firm undertakes is cross-border, multi-jurisdictional and complex.

Mishcon de Reya prides itself not only on the diverse range of legal services that it offers as a practice, but also on the diverse range of people who provide those services. The central role played by the Academy (the firm's in-house place of learning, development and new thinking), and in its active and innovative social impact strategy are reflected in *The Sunday Times* '100 Best Companies to Work For' list of 2020 — the 13th consecutive year Mishcon featured.

Africa House
70 Kingsway
London, WC2B 6AH
United Kingdom
Tel: +44 20 3321 7000
Fax: +44 20 7404 5982
www.mishcon.com

Mark Deem
mark.deem@mishcon.com

How Best to Protect Proprietary Data in Data-Sharing Deals

Toby Bond[1]
Bird & Bird

This article focuses on the monetisation of data through data-sharing deals. As discussed elsewhere in this Guide, data is a resource that can be used to generate significant value for an organisation. Data will not always be held by the party who is best able to realise that value and, therefore, sharing data can provide another route to monetising its value. However, unlike physical resources, data can be shared with others without excluding the originating party from its use, potentially allowing the data to be monetised both directly and indirectly.[2]

Identifying which categories of data can be shared to generate value and, of these, which should be shared, is a fundamental part of any organisation's overall data strategy. It is generally not a binary question, as an organisation may be willing and able to share data in some circumstances but not others. Nor is it a static question, as decisions regarding data sharing are subject to commercial, technological and regulatory considerations that evolve over time. Understanding how a particular data-sharing deal fits into an organisation's overall data strategy is often the key to ensuring its success.

1 Toby Bond is a senior associate at Bird & Bird.

2 This does not imply that all data an organisation holds should be shared to generate value. Some categories of data deliver a key competitive edge that would be destroyed if those data were made available to competitors, customers or suppliers. Nor does it imply that all data can be shared to generate value, as some data are subject to legal restrictions that limit the circumstances in which they may be shared.

Forms of data sharing

Realising value through data sharing is not a new phenomenon. Sectors such as financial services and sports betting have many years of experience of generating value through the provision of data feeds and historic data sets and have well-developed frameworks and industry norms for data licensing. However, recent developments in data capture, storage and processing techniques have opened new streams of value that may be derived from data across a much wider range of industry sectors. As a result, data-sharing arrangements now arise in many sectors in which they have not been experienced before.

Data-sharing arrangements come in many forms. They include bilateral data licences and assignments and more complex multilateral arrangements such as data pools and exchanges, under which multiple parties contribute data and receive access to data (or analytics derived from the data) in return. Data sharing also occurs in less obvious ways. For example, by providing an SaaS[3] service, the service provider will obtain access to a customer's data. While the focus of the agreement is on the value of the service, having access to the customer's data may also provide substantial value to the service provider.

Some specific categories of data (e.g., personally identifiable information or public sector information) are subject to regulatory requirements that impose additional restrictions or obligations relating to data sharing. A survey of these regulatory requirements would require a far more expansive discussion than this article affords. Our focus here, therefore, is on general issues relating to the protection of proprietary data that may arise in any form of data-sharing deal.

Protecting proprietary data

Many data-sharing deals assume that one party 'owns' the data being shared. While this is a convenient shorthand, if taken too far it can lead to confusion.[4] This confusion arises because English law (along with many other legal systems) does not recognise that data per se is capable of being owned, in the sense of granting an 'owner' rights against third parties. In contrast, a hard drive or USB stick on which data resides are clearly forms of property, capable of being owned and protected against unlawful interference and taking. The absence of a general in rem property right that applies to all forms of data, however, does not prevent parties obtaining and exercising legal rights to control access, use and dissemination of data.

---

3 Software as a service.

4 For example, who 'owns' a data set created through the combination of multiple other data sets? Is it jointly owned by the entities who contributed the data, or the entity who undertook the combination?

But what is data? Some use the term narrowly to refer to records of purely factual matters.[5] Others use it more expansively to refer to a much broader category of subject matter.[6] As a result, data is not a homogenous legal object and the legal rights that apply will vary depending on the nature of the data, and the circumstances in which it is created and shared. However, these rights provide the legal framework for any data-sharing transaction and understanding them is essential to ensuring effective protection.

The four legal rights provided by English law that can be used by commercial organisations to control access, use and dissemination of data in data-sharing deals are (1) rights of confidence, (2) copyright, (3) database rights and (4) contractual rights. We also discuss below the extent to which each right is harmonised across jurisdictions.

Rights of confidence

Rights of confidence arise under English law where information has the necessary quality of confidence and it is disclosed in circumstances importing an obligation of confidence on the recipient.[7] The right arises in equity and entitles the party to which the obligation of confidence is owed to prevent misuse of the information[8] through its unlawful acquisition, use or disclosure.[9]

Rights of confidence are often closely related to contractual rights as contractual terms are commonly the manner in which an equitable obligation of confidence is imposed on the intended recipient of information. However, the remedies available where an equitable right of confidence exists are generally more flexible than those

5 For example, the temperature in Trafalgar Square every day in December 2021, or the number of cups of coffee drunk during the writing of this chapter.

6 A photograph of Nelson's Column or a drawing of a cup of coffee could, for example, be referred to as 'training data' for an AI image recognition system.

7 *Coco v. A.N. Clark Engineers Ltd* [1968] F.S.R 415.

8 Protection for confidential information arises out of English common law, although the protection offered to the subset of confidential information that qualifies as a trade secret under Article 2(1) of Directive (EU) 2016/943 (the EU Trade Secrets Directive) has been partly codified by way of The Trade Secrets (Enforcement, etc.) Regulations 2018.

9 While the legal basis of a right of confidence has been the subject of debate before the English courts, the currently accepted view is that it is not a proprietary right in the information – see *Shenzhen Senior Technology Material Co Ltd v. Celgard, LLC* [2020] EWCA Civ 1293 at [58]. Instead, the right is founded in the law of equity and the public policy that parties should not breach obligations of confidence owed to others.

that arise following a breach of contract.[10] Furthermore, contractual rights may only be enforced against another contracting party whereas rights of confidence may be enforced against anyone who receives information in circumstances that give rise to an obligation of confidence. This does not require the recipient to have actual knowledge that they are under an obligation of confidence and is assessed from the viewpoint of a reasonable person in the position of the parties.[11]

While rights of confidence provide a powerful and flexible basis for the protection of data and databases in data-sharing deals, they are subject to several limitations:

- Rights of confidence cannot be enforced with respect to information in the public domain.[12]
- Enforcement will not be possible against 'innocent' recipients of the data who could not be expected to know that they were under an obligation of confidence, for instance because they were reasonably entitled to rely on reassurances from the party who supplied the data that the provision was lawful.[13]
- Rights of confidence may be subject to several public policy and public interest-based restrictions on their enforcement, including fundamental rights such as freedom of expression, the exposure of fraud or dishonest conduct, and cases involving public safety and wellbeing.

Although a limited degree of harmonisation in the protection of undisclosed information was achieved in Europe by way of Directive (EU) 2016/943 (the EU Trade Secrets Directive), the Directive only specifies the minimum protection that Member States (including the United Kingdom, prior to its departure from the Union) are required to

10 For example, both interim and final injunctions prohibiting the use or disclosure of confidential information are commonly awarded by English courts and relief may be granted in relation to goods that significantly benefit from the unlawful acquisition, use or disclosure of confidential information. See The Trade Secrets (Enforcement, etc.) Regulations 2018, Regulations 11 and 14.

11 *The Racing Partnership Limited v. Sports Information Services Limited* [2020] EWCA Civ 1300 at [70].

12 In other words, information that has a sufficient degree of accessibility such that it would be unjust to require the party against whom a duty of confidence is alleged to treat it as confidential.

13 See, for example, *The Racing Partnership Limited v. Sports Information Services Limited* [2020] EWCA Civ 1300, in which the majority of the Court of Appeal held that there was no breach of confidence by a recipient of horse racing data because they had been entitled to rely on an express contractual warranty that the supplier had all necessary rights from third parties to provide the information and that the recipient's use of the data would not breach any third-party rights.

provide. International harmonisation is also limited to Article 39 of TRIPS,[14] which requires World Trade Organization members to ensure the protection of certain categories of undisclosed information against acquisition, use or disclosure contrary to honest commercial practices. The circumstances in which data and databases can be protected as undisclosed information and the protection that arises can vary significantly, therefore, between jurisdictions and local advice is recommended whenever relying on this form of protection in a data-sharing deal.

Copyright

Copyright can potentially protect both data and databases. Where copyright arises, the owner is provided with a powerful right to prohibit further dealings with the data or database, including the creation of copies and communicating the data or database to the public. Although copyright is a national right, the creation or publication of a copyright work in one country will generally give rise to a copyright in most other countries.[15]

However, copyright will only arise when the work is original[16] or if a sound recording or film has not been copied from an earlier sound recording or film:[17]

- Data (other than sound recordings or films) will only qualify for protection by copyright in relation to subject matter that is original in the sense that it is its author's own intellectual creation.[18] This requires a reflection of the author's personality where the author is able to express his or her creative abilities in the production of the work by making free and creative choices.[19] The existence of technical constraints on the possible forms of expression is a factor that can reduce the scope for originality,[20] such that the more restricted the choices, the less likely it is that the product will be the intellectual creation (or the expression of the intellectual creation) of the person who produced it.[21]

14 The Agreement on Trade-Related Aspects of Intellectual Property Rights.
15 By operation of The Berne Convention for the Protection of Literary and Artistic Works and other international treaties.
16 Copyright, Designs and Patents Act 1988, Section 1(1).
17 ibid., Section 1(2).
18 *Infopaq International A/S* (Case C-5/08), at [37]).
19 *Painer* (Case C-145/10), at [88]–[89].
20 *Bezpečnostní softwarová asociace* (Case C-393/09).
21 *SAS Institute Inc v. World Programme Ltd* [2013] EWCA Civ 1482, at [31].

- A database may be protected by copyright as an original literary work when it is an author's intellectual creation by reason of the selection or arrangement of its contents.[22] As with copyright in data, copyright in a database will not arise if the selection or arrangement of the contents is entirely dictated by technical function, such that the author has no freedom to express creativity.

The requirement for originality prevents copyright applying to all data and databases. When individual data is captured to provide a record of objective facts, there is little scope for each datum to reflect an author's intellectual creation. Data capture through automated processes is therefore unlikely to qualify for copyright protection. The selection and arrangement of data in many databases will also be dictated solely by technical function, limiting the application of database copyright.

Copyright is partially harmonised through several international agreements[23] and at the EU level through various directives.[24] The United Kingdom continues to implement the EU copyright directives in its national law.[25]

Database rights

A database right arises in the United Kingdom when a substantial investment is made in obtaining, verifying or presenting the contents of the database.[26] 'Verification' means ensuring the reliability of data and monitoring its accuracy and covers checking, correcting, maintaining and updating the contents of a database.[27] 'Presenting' covers the structuring and organisation of the data and making it accessible to users (including the creation of indexes, thesauruses, etc.). An investment in 'obtaining' data refers to the resources used to seek out existing independent materials and collect them in the

22 Copyright, Designs and Patents Act 1988, Section 3A.

23 Including The Berne Convention for the Protection of Literary and Artistic Works and the World Intellectual Property Organization Copyright Treaty.

24 Directive 2001/29/EC (on the harmonisation of certain aspects of copyright and related rights in the information society), Directive 2006/116/EC (on the term of protection of copyright and certain related rights) and Directive 2009/24/EC (on the legal protection of computer programs).

25 Except for Directive (EU) 2019/790 (on copyright and related rights in the Digital Single Market), which the United Kingdom chose not to implement as the transposition date fell after the end of the transition period under the EU–UK Withdrawal Agreement. This Directive provided exceptions to copyright for the purposes of text and data mining, that have not been replicated in UK law to date.

26 The Copyright and Rights in Databases Regulations 1997, Section 13(1).

27 *Fixtures Marketing I* (Case C-338/02), at [27].

database. It does include the resources used for the creation of materials that make up the contents of a database.[28] As a result, an investment in creating new subjective information is unlikely to give rise to a database right protection, whereas investment in capturing pre-existing objective information can give rise to such protection.[29] When a qualifying investment arises, the maker of the database is afforded an intellectual priority right that can be licensed and assigned, and enforced to prevent third parties from extracting or reutilising all, or a substantial part, of the database without consent.

The maker of a database is the person who takes the initiative in and assumes the risk of obtaining, verifying or presenting the contents. However, for a database right to arise in the United Kingdom in relation to a database created before 1 January 2020, the maker of the database must be either a national or habitual resident of a Member State of the European Economic Area (EEA) or a company (1) formed in accordance with the laws of an EEA Member State and (2) having its central administration or principal place of business in an EEA Member State, or a registered office in an EEA Member State with a genuine link and continuing link to the economy of an EEA Member State. For databases created after 1 January 2020, references to a EEA Member State are replaced with the United Kingdom (i.e., makers based in the EEA will no longer obtain protection for their databases in the United Kingdom, and vice versa).

Database rights are harmonised in the European Union by way of the Database Directive,[30] which continues to be implemented in UK national law.[31] An equivalent right has not been implemented outside the European Union, although other jurisdictions may offer similar forms of protection through a broader application of their copyright law or through laws relating to unfair competition.

Contractual rights

Contracts can be used to define the scope of a permission granted under another right, such as a copyright or database right[32] or to impose (and define the scope of) an obligation of confidence on the recipient. Contracts can also be used to impose direct obligations on a party in receipt of data or a database regarding access, use and

28 *The British Horseracing Board Limited v. William Hill Organisation Limited* (Case C-203/02).

29 *British Sky Broadcasting Group Plc v. Digital Satellite Warranty Cover Ltd* [2011] EWHC 2662 (Ch) at [21] and *Football Dataco Ltd v. Sportradar GmbH* [2013] EWCA Civ 27.

30 Directive 96/9/EC (on the legal protection of databases).

31 The Copyright and Rights in Databases Regulations 1997.

32 The contract defines the scope of the permission granted to the data recipient to undertake acts in relation to data or a database that would otherwise infringe that copyright or database right.

dissemination. If the data or database is protected by an intellectual property (IP) right or an obligation of confidence, these contractual rights exist in addition to the underlying legal right.[33] However, contractual obligations regarding access, use and dissemination of data can be imposed on a recipient even when the data is not subject to an IP right.[34] In these circumstances, a contractual obligation restricting access, use or dissemination of data or a database is a negative covenant for consideration that the court will enforce 'provided only that the covenant itself cannot be attacked for obscurity, illegality or on public policy grounds such as that it is in restraint of trade'.[35] Subject to the limitations on contractual terms discussed below, contractual restrictions are therefore commonly imposed in relation to data that is in the public domain and cannot be made the subject of an obligation of confidence.

The flexibility of contractual rights to protect data irrespective of any underlying legal rights and to impose fine-grained controls on the access, use and dissemination of that data makes them a crucial tool in any data-sharing deal. However, contractual rights are subject to two key limitations:

- They are rights *in personam* and can only be enforced against specific persons.[36]
- The remedies available for breach of contract are generally more limited than those available for infringement of an IP right or a breach of confidence.[37]

Other than some limited areas (e.g., prohibitions on anticompetitive agreements), contract law is not harmonised between different jurisdictions and local advice under the governing law of the contract is recommended.

---

33 For example, acting outside the scope of a contractual licence to a database protected by a database right would give rise to a claim for both IP infringement and breach of contract.

34 See *Atheraces & Anor v. British Horse Racing Board* [2007] EWCA Civ 38, at [153], in which the Court of Appeal agreed with the High Court's conclusion that the British Horse Racing Board was entitled to charge for use of its data irrespective of whether it had any IP rights in that data.

35 *Attorney General v. Barker* [1990] 3 All E.R. 257, at 259.

36 Once the data 'escapes' beyond the control of the contracting parties, the data supplier may have a breach of contract claim against the data recipient if it is responsible for the 'escape', but will not have a breach of contract claim against third parties who receive the data. Tortious claims for procuring breach of contract or unlawful means conspiracy, however, may be available if the third party has played an unlawful part in securing access to the data.

37 For example, damages for breach of contract are generally limited to placing the claimant in the same position had the contract been performed and equitable remedies such as injunctions are less commonly awarded in breach of contract claims than in IP infringement and breach of confidence cases.

Four dimensions of control in data-sharing deals

Whatever form a data-sharing deal takes, there are four 'dimensions' of control that a party sharing data can use to protect their interests:

- Who can access the data?
- What data can they access?
- How can they access the data?
- What can they use the data for?

Decisions regarding each dimension of control will ultimately be informed by a range of commercial, legal and technical factors, including the value and sensitivity of the data, the benefit each party hopes to realise through the arrangement, the legal rights that protect the data and the technical infrastructure that will facilitate the sharing. Decisions regarding control should also be informed by any overall data strategy of the organisation sharing the data.

Who can access the data?

A starting point for any data-sharing arrangement is to establish limits on how far the data can be shared. Most data-sharing arrangements restrict access to members of certain groups, such as the employees and professional advisers of an organisation. Access may be made subject to certain legal conditions (e.g., a request for access that is approved by the data provider or an agreement to certain terms of use). It may also be subject to technical restrictions. Controls on who can access data should consider both the original data supplied to the data recipient and any materials created based on that data (e.g., the results of analysis of the data by the data recipient).

What data can they access?

Modifying data to remove or reduce its sensitivity is one dimension of control that a data provider can exercise to protect its interests. This modification can take the form of removing specific data fields from a data set, aggregating data or providing insights based on the data rather than the actual data. In some circumstances, controlling the nature of the data that can be accessed can facilitate a data-sharing transaction that would otherwise not be possible for legal or commercial reasons.

How can they access the data?

The method by which data is accessed can be an important factor in its protection. The least protected form of access is direct transfer, where the entirety of the data set is available for the recipient to download onto its own systems as direct control over the

data is lost once a copy of the data set leaves the data supplier's systems. More protection is offered by hosting the data set on the data supplier's systems and exposing it to the data recipient over the internet via an API.[38] This approach does not require the full data set to be provided to the recipient and allows access to be dynamically removed or altered. Further protection can be afforded by providing a more limited interface to the data (such as a web interface allowing a limited range of user-defined queries) or by only permitting the data user to access the data in a secure environment hosted by the data provider, such that the data always remains under the data provider's direct control.

What can they use the data for?

Data can often be reused for many purposes, some of which will be more acceptable to the data provider than others. Controls on the purpose for which data can be used are therefore important in ensuring that the data-sharing arrangement provides value to the data provider, while avoiding potential harm. Controls on use can be defined in positive terms, with a list of permitted uses and all other uses being prohibited, or in negative terms, with any use allowed unless it falls within a prohibited category. A commonly prohibited category of use is the creation of products or services that would compete with the business of the data provider.

Key contractual terms to implement controls

Contractual terms that control the legal rights of a data recipient to access, use and disseminate data received as part of a data-sharing deal are commonly found in clauses dealing with IP, confidential information, data licences and data protection. Practical restrictions on access, use and dissemination of data may also be found in other clauses, such as conditions for accessing a service and obligations on termination. Issues that commonly arise when drafting and negotiating data-sharing agreements include the following:

- *Conflicting clauses*: As the issues of data access, use and dissemination can arise in more than one place in a data-sharing agreement, it is not uncommon for inconsistencies to arise between different clauses. For example, data may be included in the definitions of confidential information and IP, such that the IP and confidential information clauses conflict with a data licence clause.

38 Application programming interfaces allow software programs to communicate with one another.

- *Unclear purpose limitation*: Purpose limitations are key in controlling the use of data under a data-sharing agreement and may give rise to a dispute if they are not sufficiently clear. Although general definitions such as 'for the purposes of this agreement' or 'in the ordinary course of business' may be appropriate in some data-sharing agreements, parties may arrive at different understandings of the extent of the permission granted, resulting in the potential for future conflict.
- *Status of derived data*: If a data recipient is permitted to process the data it has received, or combine it with other data, a data-sharing agreement should address the ownership of any new IP rights that may arise and whether the data recipient is permitted to disseminate this 'derived data' to others. In some circumstances, the derived data may embody IP rights or confidential information contained in the original data and dealings with the derived data without the permission of the rights holder would be a breach of those rights. In others, the derived data is not subject to earlier rights and the data recipient will be free to use and disseminate the data unless expressly prohibited from doing so by the contract. In either case, the parties to a data-sharing agreement should consider what is permitted in respect of derived data. A common approach is to draw a distinction between derived data that can be reverse engineered to obtain the original data and derived data that cannot.
- *Status of metadata*: In addition to data that is directly shared through a data-sharing arrangement, interactions between the contracting parties may give rise to new data (e.g., metadata regarding the use of a service by a customer). Data-sharing agreements should address the ability of each party to the agreement to access, use and disseminate this metadata.
- *Audit rights*: To ensure compliance with the terms of a data-sharing agreement, the data supplier may impose the right to audit the data recipient's use of the data. Audit rights will commonly include record-keeping requirements along with rights to access records and systems to ensure compliance.
- *Post-termination obligations*: Data-sharing agreements will commonly have a defined term or the possibility of termination under certain circumstances (e.g., a material breach of the terms or the insolvency or change of control of the parties). The agreement should address how the termination of the agreement affects the parties' respective rights to access, use and disseminate data, derived data and metadata. For example, the data provider may want the data recipient to delete all copies of the data following termination. Special consideration is required where the data has been used to train an artificial intelligence system, and the training data set needs to be retained for regulatory or technical reasons.

Limits on contractual terms in data-sharing agreements

Although freedom of contract is a basic principle of English common law, other principles exist that can prohibit certain contractual terms in data-sharing agreements. The most relevant in the context of business to business data-sharing agreements are likely to be the following.

Restraint of trade

Under English common law, covenants in restraint of trade are prima facie unenforceable unless (1) there is a valid interest that the party imposing the restraint of trade seeks to protect, (2) the restraint is no wider than is reasonable to protect that interest and (3) it is not contrary to the public interest.[39] The doctrine can potentially be engaged in the context of data-sharing agreements by way of terms that prohibit a party from carrying out trade with parties identified in the data, or from engaging with certain parties while they remain in possession of the data.[40] It is also generally considered that an obligation of confidence that remains in force once the information has entered the public domain through no fault of the recipient could engage the doctrine.

Competition law

Section 3(1) of the UK Competition Act 1998 prohibits agreements between undertakings that may affect trade within the United Kingdom and have as their object or effect the prevention, restriction or distortion of competition within the United Kingdom (referred to as the 'Chapter I prohibition'). An infringing agreement is invalid, although if the infringing provision can be severed, the rest of the agreement will remain in force. Data-sharing agreements can potentially engage the Chapter I prohibition. For example, an exclusive licence to data could restrict competition, particularly if the data set cannot easily be replicated, and the exclusivity granted under the licence is perpetual or for a substantial number of years. Section 9 of the Competition Act provides a general exception to the Chapter I prohibition. A safe harbour also exists for some data-sharing agreements by a set of block exemptions,

39 For a recent summary of the principles and main authorities from which the doctrine arises, see *Harcus Sinclair LLP v. Your Lawyers Ltd* [2021] UKSC 32.

40 See, for example, *Jones v. Ricoh UK Ltd* [2010] EWHC 1743 (Ch), in which an obligation not to deal with certain parties while in possession of confidential information was said to be likely to engage the doctrine.

such as the Technology Transfer Block Exemption (TTBE).[41] To benefit from the TTBE, the raw data provided under the licence would need to qualify as know-how under the TTBE:

> *a package of practical information, resulting from experience and testing, which is (i) secret, that is to say, not generally known or easily accessible, (ii) substantial, that is to say, significant and useful for the production of the contract products, and (iii) identified, that is to say, described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfils the criteria of secrecy and substantiality*

To benefit from the TTBE, an agreement should also not contain any of the hard-core restrictions listed under Article 4 of the Technology Transfer Block Exemption Regulation and the parties' market shares must be below the relevant thresholds set out therein.

A strategy for protecting data in data-sharing deals

Drawing together the strands discussed above, a successful strategy for protecting proprietary data in data-sharing deals will include the following steps.

- Which legal rights apply? Assess the legal rights that can be used to control access, use and dissemination of the particular data set that will be shared. These rights will depend on the nature of the data, the circumstance in which the data has been generated or collected and the way in which the data will be shared. They can also vary between different jurisdictions. Understanding the legal rights that can be used to protect the data will inform the subsequent steps in the strategy.
- Decide how to apply each of the four dimensions of control over data sharing. Form a clear view about who can access the data, what data they can access, how they access data and what they can use the data for. Decisions regarding each issue should be considered as early as possible in a data-sharing deal. Successful data sharing is most likely to happen where control issues have been considered in advance of engaging with potential data-sharing partners and are informed by the organisation's data strategy.

41 Commission Regulation (EU) No. 316/2014 retained in UK law as a result of Section 3 of the European Union (Withdrawal) Act 2018 and the Competition (Amendment etc.) (EU Exit) Regulations 2019.

- Implement decisions regarding control through technical measures and contractual arrangements that reflect the legal rights in the data. Decisions regarding control of data are implemented through technical and legal means. Contracts should reflect the underlying legal rights in the data and implement decisions regarding the four dimensions of control. Clauses dealing with use limitations, the status of derived data and metadata, audit rights and post-termination obligations will often be key points of control. Contractual terms will also need to be drafted with an eye to restrictions on contractual terms, including the restraint of trade doctrine and competition law.

TOBY BOND
Bird & Bird

Toby Bond is an intellectual property (IP) solicitor in Bird & Bird's London office specialising in high-tech patent, trade secrets and copyright litigation and the practical application of IP rights to data and artificial intelligence systems. He is a member of the International Association for the Protection of Intellectual Property (AIPPI) Standing Committee on Digital Economy and a member of council for AIPPI UK. Toby is also the co-author of the UK chapter of Thompson Reuters' *Trade Secrets Throughout the World* and the author of the UK chapter of Kluwer's *Law of Raw Data*. He is a tutor in patent law for the University of Oxford's postgraduate diploma in intellectual property law and practice and was named one of Global Data Review's '40 under 40' data lawyers in 2021.

Bird & Bird

Bird & Bird is an international law firm with a focus on helping organisations being changed by technology and the digital world. With more than 1,400 lawyers in 30 offices across Europe, Africa, the Middle East, Asia-Pacific and North America, we're ready to help you wherever you are in the world.

12 New Fetter Lane
London, EC4A 1JP
United Kingdom
Tel: +44 20 7415 6000
www.twobirds.com

Toby Bond
toby.bond@twobirds.com

Personal Data Protection in the Context of Mergers and Acquisitions

Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra[1]
Mattos Filho Advogados

Introduction

In today's fast-evolving digital landscape, corporate transactions are increasingly affected by privacy and data protection issues. For this reason, it is essential that purchasers and investors, sellers and corporate lawyers are prepared to deal with the subject and to fully understand their effects on mergers and acquisitions (M&A).

Personal data can be of great value to companies in the context of M&A transactions. Technology companies – including legaltechs, fintechs, healthtechs and many others – whose core business is data itself, are more and more involved in business operations. The value of data goes even further: companies are increasingly facing situations in which data is a central part of the operation: often an M&A transaction only happens because of the data involved. In other words, data can be a major asset within M&A transactions.

Considering the rapid pace of implementation of many data protection regulations around the world, this topic has come to occupy a more prominent place in the context of M&A in recent years, from pre-closing to post-closing phases. After all, these regulations usually provide for relevant sanctions to entities that breach data protection rules (e.g., fines and suspension of data processing operations) and give

1 Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra are partners at Mattos Filho Advogados.*

regulators broad supervisory and sanctioning powers. This is the case, for instance, with Brazil's General Data Protection Law (LGPD) and the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR)) in the European Union.[2]

In view of the potential prominence of data in an M&A transaction, the aim of this article is to provide specific recommendations for identifying some of the aspects of personal data protection that will benefit from special attention in the context of such transactions. The article focuses first on the due diligence phase (both in the preparation and during the due diligence process), which helps the potential buyer to identify opportunities, risks and obstacles concerning personal data and privacy in the context of the target's business. The second part of the article examines how the main findings of the due diligence process in respect of data protection can affect and even dictate M&A negotiations and, in the event of a successful transaction, the post-closing phase.[3]

Due diligence of personal data: relevant aspects to be considered

Roles and responsibilities of main actors

There are usually four parties involved in the due diligence process of an M&A:

- the target company or companies;
- the potential purchaser or investor;
- external auditors; and
- legal counsel.

Each of these parties has a specific role in the due diligence process and their actions may have different implications for the overall transaction. When it comes to privacy and data protection, the parties have a convergence point: as a general rule, each of them is considered controller of personal data. Under the LGPD and the GDPR, controllers are the entities that, alone or jointly with others, determine the purposes and means of the processing of personal data.

It is not difficult to see why the target company and the purchaser or investor are considered controllers of personal data, since they have powers to make decisions about the main elements of the data processing operations involved in the transaction.

---

2 For reference purposes, this article uses both the LGPD and the GDPR as parameters of data protection regulations. All the references to data protection definitions, principles and rules herein are to be interpreted in light of these two regulations, as applicable.

3 The aim of this article is to set forth the main and most common issues to be considered in the context of M&As. However, it is important to bear in mind that the relevance and the category of data protection and privacy issues may vary depending on the nature of the M&A transactions.

For instance, the target company will decide which personal data it will make available in the virtual data room (VDR), while the purchaser can request specific personal data (e.g., employees' data) to assess potential risks relating to the target business.

A more difficult task is to understand why external auditors and legal counsel are considered controllers of personal data in this context. In short, it is because, even if they were hired by one of the parties (the purchaser or the target company), they still will decide in the end, according to their expertise and know-how, which data is to be processed and how that data will be used in the context of their responsibilities.[4]

Therefore, all the parties involved in the transaction will have the responsibilities attributed to controllers of personal data, which may include:

- implementing appropriate technical and organisational measures to protect the security of data;
- ensuring data is processed in a lawful and transparent manner to the data subject;
- ensuring collected data is accurate and up to date;
- conducting privacy impact assessments on any processing activities that are likely to pose relevant risks to the data subject; and
- retaining records of processing activities, among other common obligations that are attributed to controllers of personal data according to each jurisdiction's data protection legislation.

In addition, it is important to note that all parties have to contribute independently and collaboratively to the lawful processing of personal data and that, depending on the applicable privacy laws, none of the parties will be exempted from liability in the event of a data breach or security incident involving personal data in the context of the due diligence process.

To ensure that all the parties will fulfil their data protection obligations and to regulate a possible right to redress in the case of joint liability provided for in law, the parties may put in place data protection clauses or a data processing agreement to establish the roles and responsibilities of each of them in the course of the transaction.

4 The European Data Protection Board specifically examines the role of law firms in the context of data processing activities in its Guidelines 07/2020 on the concepts of controller and processor, available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (page 12) (last accessed on 4 Jan. 2022).

Target's business model and relevant privacy laws

The business model of the target company will be crucial in determining how the due diligence will be conducted. The purchaser and its legal counsel will need to examine the kind of data that is relevant for the target business and the role of this information in the course of the business. Likewise, they will need to analyse whether the business model of the target company brings forth additional challenges or creates unforeseen privacy risks when compared with the existing business model of the purchaser.

For instance, if sectoral rules regarding privacy apply to a certain business (e.g., when the target is a financial institution or insurance company), this will likely change the way the due diligence will be conducted, to ensure that those sectoral rules and obligations are considered by the interested parties in assessing risks and impacts of the transaction.

In addition, in a transaction in which one of the parties is a business that has data processing as its core activity (e.g., an advertising agency or a big data and artificial intelligence company), the importance of the data involved in the operation is even more pronounced. In addition, these types of businesses could be more critical from a data protection perspective and should be looked into more closely to ensure that the purchaser is not assuming a risk that could pose a threat to its own activities in the future. In this situation, besides examining whether the target has a data privacy governance programme in place, it is key to ascertain whether the data processing activities being carried out are lawful.

Companies that develop activities involving relevant processing of sensitive personal data (e.g., health, biometric, racial and religious data) should also be examined carefully in the course of the due diligence, since their activities represent a greater risk from a data protection point of view. Health-related businesses are particularly susceptible since they usually process a huge amount of sensitive data that will probably have to be transferred to the purchaser after the deal is finalised.

Finally, besides the business model, it is also important to analyse (1) the current applicable privacy laws, to determine whether the target company is complying with them, and (2) whether there are new laws that would be applicable when the deal is finalised. As an example, the LGPD and the GDPR could be applicable to the targets even if they are not located in Brazil or in the European Union, respectively. This could be a relevant point of attention during the due diligence process if the target activities have an international connotation.

These are only some of the possible issues that could influence the course of the due diligence process and should therefore be taken into consideration by the parties involved in it. The issues we have discussed are the most common, but many others could arise depending on the particularities of the transaction.

Transparency obligations

Data controllers must be clear with data subjects regarding their activities, according to many of the data protection legislations around the world, such as the LGPD and the GDPR. The obligation to provide transparency prevails even if consent is not the legal basis for the data processing.

Therefore, the data controller must find a way to make data subjects aware of the data processing activities that it carries out in the scope of its business and this should include information about the potential sharing of personal data during the M&A transactions in which it may be involved in the future.

To ensure data subjects are aware of this particular data processing activity, it is common to add a section to a privacy policy or notice informing data subjects that their data may be disclosed in M&A transactions or in the proceedings that lead to a transaction. This information should be available to data subjects before the proceeding is initiated so that it is considered lawful from the outset.

Most common points for review from a privacy perspective

During the due diligence process itself, there are relevant documents and practices of the target to look at from a privacy perspective. To check the level of compliance of the target with the main data protection rules, the first step is to look at the company's documents regarding privacy and cybersecurity. Internal and external privacy policies (data subjects' privacy policies, retention policies, data breach plans, etc.) are a crucial part of any compliance programme and should be looked at as part of due diligence. To the same extent, it is advisable to understand whether the company has internal training programmes in place and whether it reflects a data protection culture.

It is also necessary to detect any possible liability to which the company may be exposed; this means looking at existing or potential legal proceedings relating to data breaches, security incidents, violations of data subject rights or any other type of legal proceeding that involves personal data.

After covering these two basic points, it is time to examine the company's practices regarding data sharing. This necessitates the analysis of the standard contractual clauses or data protection agreements that exist between the target and its main partners and services providers, to verify whether they adhere to the legislation of the

relevant jurisdictions. In this sense, it is important to verify whether the main data sharing operations are lawful and, if not, if it is possible to terminate the relevant contractual relationship between the target and the third party, assessing the potential consequences of the termination for the business operation.

Security of the virtual data room

Considering that most elements of the exchange of personal data happens through VDRs, one of the most important steps to ensure that due diligence is lawful from a privacy perspective is to take care of the VDR's security. The company that provides the VDR must comply with the applicable data protection laws, be trustworthy and adopt high-level security mechanisms.

Furthermore, to ensure that the data shared is minimal and strictly necessary for completion of the due diligence process, whenever possible, personal information should be anonymised or redacted from documents. In addition, sensitive or special categories of personal data should not be made available unless they are a vital part of the process.

Whenever contracts need to be provided, it is recommended that only standard templates are made available in the VDR. Ideally, different levels of access should be given to the individuals involved. Furthermore, only the individuals that need to have access to the data should have it, although they should not be able to edit the documents.

Some other precautions include not making available the names and salaries of employees of the target company, or records of work-related accidents that could be traced to a specific person. Finally, in lawsuit reports, the names of the parties in lawsuits that are under secrecy should be scored out (i.e., rendered illegible).

After the due diligence: M&A negotiations and post-competition phase

Impact on the valuation and other business impacts

As has been mentioned, data has gained a more pronounced role in M&A transactions over time. As a consequence, privacy and data protection are being given an increasing amount of attention within the scope of such transactions. As there are many subjects that can affect a business's valuation (for example, the circumstances of the sale, the economic situation of the relevant jurisdiction, the age of the business age and stability of its management stability, among other things), privacy and data protection risks can also have major significance in estimations of the target's price.

It is crucial for purchasers to take into account the effect of the personal data processing operations on the proposed transaction and on the negotiated valuation. Privacy issues, such as the lawfulness of the processing activities being carried out, the particularities of the data flows, the internal and external privacy policies in place, the level of compliance with applicable laws, the occurrence of data incidents, among other things, can significantly change the target's values. This may depend on the legality of the company's business model, the transaction valuation model (e.g., cash flow valuation, asset valuation, historical earnings valuation or relative valuation method), among other aspects.

This analysis is important to thoroughly identify and formulate a risk mitigation strategy (this can include, for instance, a comprehensive data protection compliance programme, the renegotiation of contracts that involve relevant personal data flows, etc.). It is also important to highlight that the valuation of the target business may be affected even if mitigation measures are taken in the pre-closing and post-closing phases.

An example of the impact that a data protection issue can have on the target's valuation is a situation in which the target has experienced several data breach incidents and has not taken any preventive or remedial actions. In addition to the exposure to administrative sanctions (including high financial penalties), such a company will tends to be less attractive to the market.

In this sense, current and prospective clients are likely to refrain from using the company's services because of the lack of commitment to protecting their personal data. Furthermore, third parties (e.g., commercial partners) are less likely to seek the company to propose marketing deals. Relations with the company's supply chain can potentially be strained, in addition to the reputational damage that this company could suffer. All these aspects have the power to significantly decrease the company's value and have a direct impact on the valuation negotiated by the parties.

Both purchasers and legal counsel must thoroughly investigate privacy gaps within the target business and also consider the costs of implementing measures to comply with the applicable data protection laws, which are usually high. Once these are identified, it is essential to appropriately address the risks and their potential impact on the target's value.

M&A definitive agreements

Regulation of privacy and data protection representations, warranties and indemnities

One of the last and most important phases of an M&A deal is the preparation of the M&A definitive agreement that will set the deal. This can be, for instance, a share purchase agreement (SPA),[5] in the case of a share transfer transaction, or an investment agreement (IA),[6] in the case of an asset transfer agreement (hereinafter referred to as 'definitive agreement').

A relevant section of the vast majority of definitive agreements regulates the representations and warranties (R&Ws). These are given by both the seller and the purchaser or investor and aim to disclose material information. R&Ws are used as an assurance that particular facts are true, especially for topics that are not very easily verifiable. They are also used to allocate the risks between the seller and the purchaser or investor. This is very important, because these are the basis of any future indemnification claim in the event of a breach or inaccuracy post-closing.

R&Ws usually contain standard privacy and data security provisions and it is common to see R&Ws that include general terms (e.g., 'compliance with privacy laws'). However, the best strategy is to refine these provisions to reflect the specific situation and to adjust the relevant topics. This will ensure better protection for the purchaser against specific privacy risks and for the seller in relation to data protection legal provisions that are not yet regulated by the relevant authorities.

More than compliance with the applicable laws, tailored privacy and data protection-related R&Ws can cover compliance with contractual obligations, disclosure requirements, internal data breach recovery procedures or any other measures that are not necessarily required by law or contracts (e.g., industry-standard security measures).

5 A share purchase agreement is a legal document that is used in transactions involving the purchase and sale of equity interests and serves as an instrument for the partners or shareholders of a company to sell their participation to third parties.

6 An investment agreement is a contract between a company and its shareholders and an investor governing a proposed investment in the target company.

Although R&Ws can vary depending on the scale of the transaction and the target's core business, among other aspects, it is important that they contain, at a minimum, specific privacy and data protection provisions that, for example, objectively list the target's data protection main practices and level of compliance with applicable laws. The relevant subjects that R&Ws may address include:

- a history of the target's past data security incidents, legal proceedings and relevant claims (or the lack of breaches), including enforcement actions;
- details of the data flows carried out by the target;
- an indication of the level of compliance with the applicable legislation; and
- an indication of the data sharing practices and retention policies adopted, among other things.

To mitigate risks of M&A, R&Ws insurance is becoming more common. It covers eventual indemnification obligations of the parties in relation to the violation of R&Ws included in the SPA. The main focus is hidden liabilities, although materialised contingencies are not usually covered by this type of insurance. Insurance companies usually analyse the due diligence reports in such cases to assess the main findings and negotiate what will be covered.

This type of risk mitigation may be considered especially relevant since the verification of the level of compliance with the relevant data protection laws usually requires in-depth and detailed analysis, both legal and technical, of the practices adopted by the target, which is not always compatible with the nature of due diligence. Thus, the insurance does not exempt an effective data protection due diligence but can mitigate risks relating to deeper aspects of data protection legal compliance.

Finally, the indemnities section of the definitive agreement is used to regulate the seller or invested company's obligation to indemnify the purchaser or investor for damage and loss caused by facts and circumstances of which the parties are aware. For instance, if a relevant personal data breach occurred before the closing phase and individual lawsuits and an administrative proceeding have been initiated and are still in progress, the parties can agree that the seller or invested company will reimburse the purchaser or investor in respect of any losses that derive from the data breach. In this sense, a common practice when drafting indemnity clauses is to exclude any limitations to indemnify liability (such as caps, *de minimis* and basket amounts) in the case of relevant facts that were disclosed during the due diligence process, such as a critical personal data breach.

Integration of databases and data processing activities

After the deal is completed, depending on the nature of the transaction (e.g., a transfer of control of the target or a merger between two companies), it is time to integrate the companies' databases and processing activities. This means combining and standardising data protection practices and information about clients, commercial prospects, marketing material, payments and supply chain, among many other elements.

The integration phase should start before the deal is finished. Planning is the most important step to assure the success of integration. Therefore, the key is organising the main characteristics of the planned integration in advance, such as the level of integration, the standard of privacy to be reached, priorities, the resources available and the need for IT support.

When the integration itself commences, it is also important to map out the various aspects of organisation, the tools needed to achieve a successful integration and how to coordinate the project to ensure it runs smoothly. Asking questions that can seem obvious at first, but are very commonly overlooked, is a relevant task:

- What is the size of the integration size?
- Is it sufficient to have one individual coordinating the project or is it necessary to put together a privacy team?
- How will the communication between the companies, the internal team and legal counsel work?
- How can other areas (e.g., human resources and marketing) follow the project and provide contributions?
- Do the companies have the necessary IT tools and systems in place?

Privacy components have an important place on the integration agenda. Depending on the issues and risks identified during the due diligence process, the purchaser's priorities and the jurisdiction's legal requirements, the order in which the company addresses these items may differ.

Below are a few examples of data protection matters that may be addressed during the integration phase, depending on the findings of the due diligence and the practices adopted by the target and by the purchaser or investor.

Data protection officer

Some jurisdictions have legal determinations that require companies to formally appoint a data protection officer (DPO). It may therefore be necessary to appoint, or replace, a DPO at the acquired company. This is certainly the case in Brazil and the European Union, as determined by the LGPD and the GDPR.

Structuring or reviewing data breach response plan

Some companies, especially in jurisdictions that do not have detailed data protection regulations, tend not to include privacy issues in their procedures for incident control and restrict them to business sensitive information. At a minimum, a company should include a DPO or a privacy lead on its disaster management team, not least to ensure that the respective country's legal notification deadlines are met. For example, the LGPD determines that notification of the security incident should be made within a 'reasonable period of time'.[7] While further regulation is pending, it is recommended that the Brazilian Data Protection Authority is notified as soon as possible (i.e., the indicative period is two working days from the date of knowledge of the incident).

Preparing or reviewing data privacy governance policy

Data privacy governance policies are documents that establish the main rules, principles and obligations relating to data processing that must be followed by the company (including employees, service providers, etc.). If this document does not yet exist, the best strategy is that the company prepares and puts this policy into practice as soon as possible.

Privacy awareness workshops

One of the most essential parts of integration is internal transparency. All areas should be able to easily follow the integration procedure and provide their input in an organised matter. This practice improves the integration and ensures that all issues are being considered. One of the ways to achieve this goal is to provide privacy and security awareness workshops for employees, sharing the important elements of the integration, the status of the procedure, next steps and explaining the changes in processing personal data within day-to-day activities.

Reviewing privacy statements

Depending on the size, age and activities of the business and the level of integration, it is advisable to review the privacy statements (including data subjects' privacy policies). This can be done according to the template used by the acquiring company, making adjustments to the existing document, or aligning new statements according to the post-closing situation.

---

7 Brazilian General Data Protection Law, Article 48(I).

Sharing human resources data

One of the most sensitive aspects of an integration is the sharing of data held by human resources (HR) departments. Usually, it is necessary for the target employees' data to be shared for the purpose of people management. The transfer of HR data typically requires the drawing up of a contract in advance, in addition to a detailed analysis of the relevant legal obligations of the jurisdiction. In Brazil, the LGPD determines the designation of a legal basis for the processing of personal data and sensitive personal data by the controller. In some situations, a notice to employees is sufficient. In others, specific consent may be required for data processing. It is important to emphasise that, in any event, this data must not be shared beyond what is necessary to fulfil the sharing purpose.

Storing and transferring data

It is advisable to analyse the relevant jurisdiction's transfer restrictions and localisation requirements so as to evaluate the need to prepare customer disclosures or to adopt the required mechanisms for the transfer of data, such as consent or data transfer clauses ensuring the same level of data protection, in case there is a change of location of the target's data.

Sharing personal data

Processing the personal data of clients of the acquired or invested company for different purposes (such as marketing) may trigger the need for separate consent from each of the clients or of notice to data subjects. More often than not, business stakeholders intend to use this personal data for business purposes. As such, it is important that legal and contractual limitations are clear to stakeholders and other parties involved in the transaction and that the measures needed to guarantee the lawfulness of any new sharing of data are put in place.

** The authors acknowledge contributions to this article by Jaqueline Simas de Oliveira, Nuria Bauxali and Beatriz Spalding (associates at Mattos Filho Advogados) and Larissa Teles Nonato (trainee at Mattos Filho Advogados).*

FABIO FERREIRA KUJAWSKI
Mattos Filho Advogados

Fabio Ferreira Kujawski's practice focuses on technology, data protection, telecommunications, intellectual property, media and entertainment, with expertise in transactional and regulatory matters affecting these industries. He advises companies on a wide range of corporate matters, both domestic and cross-border. He is the co-author and editor of the book *Legal Trends in Technology and Intellectual Property in Brazil* (2014). He is an officer of the Brazilian Association of Information Technology and Telecommunications Law (ABDTIC).

PAULO MARCOS RODRIGUES BRANCHER
Mattos Filho Advogados

Paulo Marcos Rodrigues Brancher's practice focuses on technology, financial products, and transactional work concerning innovative industries. He holds a PhD from the São Paulo Catholic University (PUC/SP), where he teaches business law and technology law. Paulo is a former chairman of the Brazilian Association of Information Technology and Communications (ABDTIC). He is a current member of the International Technology Law Association (ITechLaw), having served for six years as a member of the board of directors. He has published several books and is the co-editor of the law journal *Direito Empresarial na Economia Digital* (Business Law in the Digital Economy).

THIAGO LUÍS SOMBRA
Mattos Filho Advogados

Thiago Luís Sombra's practice focuses on technology, compliance and public law, and in particular on anti-corruption investigations handled by public authorities and regulators, data protection, cybersecurity and digital platforms. He has been listed as one of the world's leading young lawyers in anti-corruption investigations by GIR 40 under 40 and in technology by GDR 40 under 40. Based on his experience as a state attorney, he also advises clients in cases relating to state-owned companies, administrative sanctioning procedures, concessions, bids and administrative contracts in general. He served as State Attorney of São Paulo before the Federal Supreme Court and Superior Court of Justice (STJ), and as a clerk at the STJ. He is currently a professor at the University of Brasília (UnB), member of the International Association of Privacy Professionals (IAPP) and the International Committee of Digital Economy of the International Chamber of Commerce (ICC). He is certified by the IAPP with CIPP/Europe. He is also the author of the book *Fundamentals of Privacy Regulation and Personal Data Protection* (Amazon, 2019).

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

Mattos Filho provides services to clients in different legal areas in a coordinated and integrated manner, working in multidisciplinary teams whenever necessary. This work dynamic allows the firm to deliver tailor-made solutions to clients, thereby enhancing the firm's understanding of the clients' businesses and making Mattos Filho a valuable partner.

Mattos Filho is a leader in more than 20 different practice areas and works continuously to ensure that all these practices are benchmarks for the market. The firm represents domestic and foreign companies, financial institutions, investors, multilateral agencies, private clients and family offices, investment funds, pension funds, insurers and reinsurers and non-profit organisations.

Alameda Joaquim Eugênio de Lima, 447
Jardim Paulista
São Paulo
Brazil
Tel: +55 11 3147 7600
www.mattosfilho.com.br

Fabio Ferreira Kujawski
kujawski@mattosfilho.com.br

Paulo Marcos Rodrigues Brancher
pbrancher@mattosfilho.com.br

Thiago Luís Sombra
thiago.sombra@mattosfilho.com.br

Successful Data Breach Response: What Organisations Should Look Out For

Rehana C Harasgama, Jan Kleiner and Viviane Berger[1]
Bär & Karrer Ltd

Introduction

With every passing year, the world is becoming more digitalised. The amount of data that is being processed is increasing exponentially and with it the risk of data (as a critical asset) being lost, unlawfully accessed or destroyed and thereby endangering the value of an affected company's value. In 2021, in the United States alone, data breaches increased by about 17 per cent by the third quarter compared to the whole of 2020.[2] Moreover, Cybersecurity Ventures predicts that worldwide annual costs for cybercrime will increase to US$10.5 trillion annually by 2025, compared to US$3 trillion in 2015, which may also lower the value of affected companies' data assets.[3] Both LinkedIn and Facebook were subject to data breaches, affecting about 700 million users and 553 million users, respectively.[4] In the European Union, supervisory authorities issued

1 Rehana C Harasgama is a senior associate, Jan Kleiner is a partner and Viviane Berger is a junior associate at Bär & Karrer Ltd.

2 Maria Henriquez, 'The top data breaches of 2021', at https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021 (last accessed January 2022); ID Agent, '2021 Data Breaches Have Already Exceeded All of 2020', at https://www.idagent.com/blog/2021-data-breaches-have-already-exceeded-all-of-2020/ (last accessed Jan. 2022).

3 Steve Morgan, 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics, at https://cybersecurityventures.com/cybersecurity-almanac-2022/ (last accessed Jan. 2022).

4 Maria Henriquez, op. cit. note 2, above.

fines ranging from a mere €285 to €475,000 in 2021, all essentially triggered by an 'insufficient fulfilment of data breach notification duties' and increasing companies' costs in respective of their data.[5]

To prevent data breaches (and therefore protect data as a critical asset), a minimal standard of data security mechanisms must be implemented according to applicable data protection laws. If these measures fail or a breach occurs despite such measures, the affected organisation has to act in a quick and organised way to avert or at least reduce possible damage. This article provides guidance as to how organisations can react to data breaches, so as to meet applicable data protection law requirements and counteract any damage caused to their data by such breaches.[6] Against this background, this article also compares several jurisdictions to get a sense of global developments with regard to data breaches.

To provide a broad overview and identify similarities regarding the concept of data breaches next to that stated in the General Data Protection Regulation (GDPR) in the European Union,[7] the authors have chosen the (current or soon to be revised) data protection laws of Switzerland, the United Kingdom, Canada, Brazil, China, Australia, South Africa and Japan, as these countries either provide an adequate level of data protection according to the European Commission[8] or have recently introduced a new data protection regime providing similar data breach notification duties as under the GDPR.

---

5 GDPR Enforcement Tracker (tracked by CMS, law tax future), at https://www.enforcementtracker.com/ (last accessed Jan. 2022).

6 The proposals are based on data protection laws only. It must be noted that other, sector-specific legislation may provide for additional requirements (e.g., notification duties) in the event of security incidents.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (last accessed Jan. 2022). The GDPR is retained in UK domestic law as the UK GDPR. (Note the use of '(UK) GDPR' where reference in remaining footnotes is to both Regulations.)

8 An 'adequacy decision' means a decision of the European Commission pursuant to GDPR, Art. 45 on whether a country outside the European Union (EU) offers an adequate level of data protection. If this is the case, personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to these third countries without any further safeguards being necessary; so far the following jurisdictions reviewed have been recognised as adequate by the European Commission: Canada, United Kingdom, Japan and Switzerland. Not recognised but nevertheless examined

This article is divided into three main parts derived from our comparative analysis: first, we describe what constitutes a 'data breach', then we provide an overview of the potential risks a data breach can cause and finally we describe what an appropriate data breach response plan should look like.

What a data breach is

As a general rule, all analysed jurisdictions impose on persons processing or handling personal data a duty to protect that data appropriately from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, while taking into consideration potential risks to the processed data.[9] In other words, companies (or persons) processing personal data are required to ensure the integrity, confidentiality and availability of the data. Although this duty mainly stems from the protection of the individuals whose data is affected, implementing such measures are as important for business continuity and for a company's reputation.

If the implemented data security measures fail or are breached, this can lead to what is known as a data breach. When comparing data protection laws of the countries stated above, there appear to be key similarities regarding the definition of a data breach. In Article 4(12) of the UK GDPR, a (personal) data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[10] Almost identical in wording, this definition is also used under the term 'security incident' in Brazil's General Data Protection Law (LGPD).[11] Similarly, the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada sets forth the concept of breach of security safeguards, which is defined as the 'loss of, unauthorized access to or unauthorized disclosure of personal information'

---

in this article are Australia, Brazil, China and South Africa. European Commission, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed Jan. 2022).

9 See (UK) GDPR, art. 32(2); FADP, art. 7; respectively; revFADP, art. 8; PIPL, art. 9; PIPEDA, clause 4.7 of schedule 1; LGPD, art. 46; Privacy Act 1988, clause 11.1 of pt. 4 of schedule 1; POPIA, sec. 19; and APPI, art. 20.

10 See United Kingdom General Data Protection Regulation, https://www.legislation.gov.uk/eur/2016/679/contents (last accessed Jan. 2022).

11 Brazilian General Data Protection Law (LGPD) (as amended by Law No. 13,853/2019), art. 48 in conjunction with art. 6 VII, translated by the International Association of Privacy Professionals (IAPP), see https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/ (last accessed Jan. 2022).

resulting from a breach of or failure to establish adequate security safeguards.[12] Australia also linked its definition in the Privacy Act 1988 to 'unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity'.[13] Next to the unauthorised access, South Africa's data protection law (Protection of Personal Information Act (POPIA)) additionally includes the acquisition of personal information.[14] Slightly different but following the same idea, under China's Personal Information Protection Law (PIPL), a data breach is described as 'a personal information leak, distortion or loss' that might have occurred.[15] Moreover, several countries have revised or amended their data protection laws and will officially implement data breach reporting duties, for example, as foreseen in the revised Federal Act on Data Protection (revFADP)[16] of Switzerland, which defines a data breach almost identically to the definition under the GDPR and the UK GDPR, or the amendment to the Act on the Protection of Personal Information (APPI)[17] in Japan.

To summarise, the concept of a data breach is characterised by an event affecting the integrity of personal data (e.g., if personal data is altered without authorisation), the data's availability (e.g., if a breach leads to a restriction of access to the data or the

12 Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, sec. 10.1(1), at https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html (last accessed Jan. 2022).

13 Privacy Act 1988 (Cth), pt. IIIC div. 26WA, at https://www.legislation.gov.au/Details/C2021C00452 (last accessed Jan. 2022).

14 Protection of Personal Information Act No. 4 of 2013 (POPIA), sec. 22, at https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (last accessed Jan. 2022).

15 Personal Information Protection Law of the People's Republic of China (PIPL), art. 57, at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (last accessed January 2022).

16 Federal Act on Data Protection of 25 September 2020 (revFADP), art. 24, BBl 2020 7639, 7641, at https://www.fedlex.admin.ch/eli/fga/2020/1998/de (last accessed January 2022).

17 Amended Act on the Protection of Personal Information (APPI), art. 22-2, at https://www.ppc.go.jp/files/pdf/APPI_english.pdf (last accessed January 2022).

deletion of personal data) or confidentiality (e.g., if a breach leads to the disclosure of personal data to unauthorised third parties).[18] Some practical examples for these types of compromises are as follows:[19]

- a targeted attack on credit card data of customers directly linked to the credit card holders can lead to the credit card being used fraudulently;
- a ransomware attack on a hospital's information system that affects health data of thousands of patients. Recovery takes several days, resulting in delays to treatment;
- an unencrypted USB stick containing employees' or customers' private data is lost or stolen on public transportation;
- a dating website is hacked and sensitive user data is published on the internet; or
- owing to a system failure, a staff telephone list is deleted and cannot be restored.

The risks and consequences of a data breach

When a company is affected by a data breach, there are not only grave risks for the company itself but notably also for the affected individuals, whose data has been compromised by the breach. To prevent or minimise damage, all the examined data protection laws require some sort of data breach notification, for which the specifics are discussed below. Finally, we demonstrate applicable consequences in the event of failure to comply with notification obligations.

---

18 Hladjk in Ehmann and Selmayr (eds), *Datenschutz-Grundverordnung, Beck'sche Kurz-Kommentare* (2nd edition, Munich 2018); GDPR, art. 33, no. 5 et seq.; Article-29-WP, Guidelines on Personal data breach notification under Regulation 2016/679 adopted on 3 October 2017, WP250rev.01 (Article-29-WP, Guidelines), p. 7 et seq.; David Rosenthal, 'Das neue Datenschutzgesetz', Jusletter (16 November 2020), no. 161; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7064; Schultze-Melling in Taeger/Gabel (eds), Kommentar DSGVO – BDSG (Frankfurt am Main, 2019); GDPR, art. 33, no. 12; European Union Agency for Network and Information Security (enisa), Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0 (December 2013) (enisa, Recommendations), p. 5.

19 Article-29-WP, Guidelines, p. 30 et seq.; European Data Protection Board (EDPB), Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, adopted on 14 December 2021, Version 2.0, 8 et seq. (EDPB, Examples); enisa, Recommendations, p. 12 et seq.; Information Commissioner's Office (ICO), Personal Data Breaches, at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (last accessed Jan. 2022).

Risks for an organisation affected by a data breach

If affected by a data breach, organisations could face consequences on several levels. On a technical and financial level, data breaches may lead to operational disruptions and failures, the loss of business data and know-how and the financial costs of investigating the breach and restoring the ordinary course of business.[20] The loss of data or loss of access to specific data may also lead to loss of productivity and business continuity issues.[21]

Aside from the technical issues that may arise, data breaches, such as cyberattacks, may cause reputational damage that, in turn, may lead to a loss of consumer trust and a reduction of the company value.[22] The loss of trust may also lead to a higher volume of data protection requests that need to be handled, such as the request of erasure or, in the worst case, civil claims.[23] Finally, data breaches may lead to legal liability (towards either authorities or affected individuals), for example, if a company is in breach of its data security or notification obligations or if affected individuals suffer financial damage as a result of such an incident.[24]

Risks for affected individuals

If not addressed in a timely and appropriate manner, data breaches may result in physical, material or non-material damage to the individual. Examples of such harm may be loss or limitation of control over their personal data, discrimination, identity theft

---

20 Christian Schröder and Tobias Lantwin, 'Cyber-Sicherheitsvorfälle in multinationalen Unternehmen in der EU und den USA', ZD 2021, 614; Tino Gaberthüel, 'Cyber-Security fordert Unternehmen', NZZ no. 201 of 31 August 2017, 9.

21 Embroker Team, 2022 Must-Know Cyber Attack Statistics and Trends, at https://www.embroker.com/blog/cyber-attack-statistics/ (last accessed Jan. 2022).

22 Schröder and Lantwin, op. cit., 614; Gaberthüel, op. cit., 9; others argue that the disclosure of a data breach leads to reputational damages that may be even higher than the reputational damage caused by the data breach itself; see Bernold Nieuwesteeg and Michael Faure, 'An analysis of the effectiveness of the EU data breach notification obligation', *Computer Law & Security Review*, 34 (2018), 1238; Maria Karyda and Lilian Mitrou, 'Data Breach Notification: Issues and Challenges for Security Management', MCIS 2016 Proceedings, Mediterranean Conference on Information Systems (MCIS), 2016, 7.

23 ICO, Personal Data Breaches, at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (last accessed Jan. 2022).

24 Embroker Team, 2022 Must-Know Cyber Attack Statistics and Trends, at https://www.embroker.com/blog/cyber-attack-statistics/ (last accessed Jan. 2022); Nieuwesteeg and Faure, op. cit., 1237 et seq.

or fraud, financial loss, damage to the individual's reputation, loss of confidentiality when data protected by professional secrecy is accessed, or other significant economic or social harm to the individual concerned.[25]

Apart from the evident violations of data protection laws committed by the person causing the data breach, as well as from the perspective of the affected organisation, such an incident almost inevitably leads to a situation in which the organisation will no longer be able to meet the general data protection principles. In particular, the organisation will have difficulties in meeting the principles of proportionality, purpose limitation and transparency. Unauthorised access violates the need-to-know principle and triggers issues concerning the proportionality of processing. Data that has been stolen may not be deleted once it has fulfilled its purposes, as it is unclear who has access to the data. The principle of transparency may be breached because an unknown person gains access to the data. Hence, the personal and fundamental rights of the affected individuals are breached when a data breach occurs, which is why individuals may be able to make civil claims following such an incident.[26]

Notification obligations

Against the background described above, the analysed countries have implemented, or are planning to introduce, data breach notification obligations so that the identified risks for the affected individuals, in particular, can be managed.[27] Under data protection law, the goal of the (new) data breach notification obligations is, on the one hand, to increase transparency and, on the other, to help data subjects regain some of the

25 (UK) GDPR, Recital 85; Hladjk, op. cit.; GDPR, art. 33, no. 3; Dix in Simitis, Hornung and Spiecker also known as Döhmann (eds), Datenschutzrecht, DSGVO mit BDSG, NOMOS Kommentar (Baden-Baden 2019); GDPR, art. 33, no. 2; Reif in Gola (ed), Datenschutz-Grundverordnung, VO (EU) 2016/679, Kommentar (Munich 2018), art. 33 no. 2.

26 (UK) GDPR, Recital 85; Hladjk, op. cit.; GDPR, art. 33, no. 5; BBl 2017 6941, 7064; Bundesamt für Justiz BJ, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (21 December 2016), 62 et seq. (BJ, Erläuternder Bericht); Adrian Bieri and Julian Powell, 'Meldung von Verletzungen der Datensicherheit', AJP 6/2021, 781; Jan Kleiner, 'Meldepflicht bei Datenschutzverletzungen', Zeitschrift für Datenschutz und Informationssicherheit digma 2017, 171; Dix, op. cit.; GDPR, art. 33, no. 2; Article-29-WP, Guidelines, 9.

27 Karyda and Mitrou, op. cit., 9.

control they have lost by taking certain measures themselves to counteract the damage resulting from the breach.[28] From a purely business perspective, the investigation of such a breach is essential to mitigate further damage to the value of the data.

The obligation to notify the supervisory authorities is also intended to give data controllers an incentive to ensure an appropriate level of data security according to applicable data protection laws.[29] Finally, the notification obligations serve the purpose of giving the competent authority the possibility to adopt measures itself to avert or contain the damage or, if necessary, impose sanctions with the purpose of preventing future data breaches.[30]

When looking at the various examined data protection laws, next to the definition of a data breach, another common denominator is a general duty of the person (or persons) processing personal data to investigate and report breaches to the competent authority and, in certain cases, the affected individual, if the threshold to report the incident is reached. However, when closely observing the requirements for these reporting duties, there appear to be differences in some key areas.

First, there seem to be different conditions regarding when to report a suspected data breach to the competent authorities. China's PIPL (Article 57) and South Africa's POPIA (Section 22) stipulate an unconditional duty to notify the breach to the authorities, whereas the other examined data protection laws provide some sort of threshold.

Second, the aforementioned threshold varies between the different jurisdictions depending on whether the obligation is towards the supervisory authority or the affected individuals. As regards the thresholds for notifying the competent supervisory authorities:

- the European Union, the United Kingdom and Brazil require only a 'risk' (UK GDPR/GDPR, Article 33) or 'relevant damage' (LGPD, Article 48) to the rights and freedom of natural persons; and

28 Hladjk, op. cit.; GDPR, art. 33, no. 2 and 3; BBl 2017 6941, 7064; Kleiner, op. cit., 171; Bieri and Powell, op. cit., 782.

29 Jan Kleiner and Lukas Stocker, 'Data Breach Notifications', Zeitschrift für Datenschutz und Informationssicherheit digma 2015, 93; Kleiner, op. cit., 171; Richard J Sullivan and Jesse Leigh Maniff, 'Data Breach Notification Laws', *Economic Review*, 2016; Federal Reserve Bank of Kansas City, 67 et seq.; Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia – Where to now?', *Computer Law & Security Review*, 28 (2012), 297; Nieuwesteeg and Faure, op. cit., 1239; Karyda and Mitrou, op. cit., 7 et seq.

30 Kleiner, op. cit., 171; Bieri and Powell, op. cit., 781; Burdon, Lane and von Nessen, op. cit., 298.

- the (revised) data protection laws of Switzerland, Canada and Australia demand, respectively, a 'high risk' (revFADP, Article 24), 'real risk of significant harm' (PIPEDA, Section 10.1(1)) or 'serious harm' (Privacy Act 1988, Part IIIC Division 26WA).

To clarify these thresholds, several of the data protection laws provide further guidance. For example, the 'significant harm' set out in Section 10.1, Paragraphs (7) and (8) of PIPEDA includes, inter alia, bodily harm, damage to reputation or relationships, loss of employment, financial loss, identity theft, negative effects on a person's credit record and damage to or loss of property, while the factors to determine the risk of such harm include the sensitivity of the personal information involved and the probability of it being misused. Similarly, Part IIIC, Division 26WG of the Privacy Act 1988 provides guidance on what to take into account when assessing the likelihood of 'serious harm', such as the sensitivity of the information, the likelihood that the person who has obtained the information has the intention of causing harm to the individuals and the nature of the harm.

The European Data Protection Board (EDPB) also lists certain factors to consider when assessing the level of harm of a data breach. These factors include the likelihood and risk the data breach could cause the affected individuals, the sensitivity of the affected data, the number of affected data subjects, the type or nature of the breach, the likelihood of identifying the affected individuals, the ability to remedy the data breach as well as other qualifying factors (e.g., a criminal intention behind the breach or systematic approach).[31]

Third, in almost all the examined data protection laws, different exceptions to a general reporting duty exist. Exceptions provided in the jurisdictions reviewed include, among other things, impossibility of notification, protection of higher, important or public interests, low probability of identifying the affected individuals or protection of secrecy obligations.[32]

Finally, the period between the breach and notification to the authority differ between jurisdictions. However, it is generally required that the responsible persons react in a timely fashion. For instance, 'immediate' notification is required under Article 57 of the PIPL. Other jurisdictions are more lenient, for example, in that they

31 Article-29-WP, Guidelines, 24 et seq.; see also enisa, Recommendations, 3 et seq.; Bieri and Powell, op. cit., 782; Kleiner and Stocker, op. cit., 93; Kleiner, op. cit., 174 et seq.

32 e.g., Privacy Act 1988, pt. IIIC div. 26WM-26WQ; (UK) GDPR, art. 34(3); revFADP, art. 24(5); PIPL, art. 57.

require a notification 'as soon as possible' (revFADP, Article 24) or when 'feasible' (PIPEDA, Section 10.1(6)). Moreover, it is noteworthy that of the examined data protection laws, only the GDPR and UK GDPR state a strict deadline of no more than 72 hours after becoming aware of a data breach. Any deviations from this period must be explained to the competent authority (UK GDPR/GDPR, Article 33(1)).

Violations of the notification obligation may be severely fined. By way of illustration, the supervisory authority of the Netherlands imposed a fine of €475,000 on booking.com, because it did not notify the authority within 72 hours of becoming aware of a data breach. However, against this background, both the UK GDPR and the GDPR allow persons who have an obligation to report data breaches to make their notification in phases or steps, if not all required information can be provided to the supervisory authority upon initial notification (UK GDPR/GDPR, Article 33(4)). The draft of the revised ordinance to the revFADP (revOFADP) in Switzerland suggests a similar approach (Article 19(2)). However, the revOFADP has not yet been adopted.

That being said, as far as similarities go, aside from the definition of a data breach, almost all jurisdictions reviewed provide a minimum list of information that needs to be provided when reporting a data breach. This information includes the type of data breach, risks or harm resulting from the data breach, affected data categories and data subjects, remedial measures and, in some instances, a contact person within the affected organisation for follow-up questions.[33]

Consequently, although the analysed countries all require organisations affected by a data breach to report it, there appear to be differences regarding the threshold and deadline to report a data breach as well as the exceptions to the notification obligation.

Risks of non-compliance

Failure to comply with the notification obligations described above may cause harm to the affected individuals, which is why certain data protection laws stipulate fines or other consequences, so as to create an additional incentive to report data breaches and help prevent future data breaches.

33 See (UK) GDPR, art. 33(3); revFADP, art. 24; PIPL, art. 57; Breach of Security Safeguards Regulations, SOR/2018-64, sec. 20, at https://laws-lois.justice.gc.ca/eng/regulations/SOR-2018-64/page-1.html#h-858485 (last accessed January 2022); LGPD, art. 48(1); Privacy Act 1988, pt. IIIC div. 26WK; and POPIA, sec. 22(5).

Fines can be found, among others, in the GDPR, the UK GDPR, PIPL and PIPEDA.[34] Under Section 28 of PIPEDA, to knowingly contravene the notification duty is an offence and may result in fines and penalties up to US$100,000. The GDPR and the UK GDPR, in turn, state in Article 83 the possibility of imposing fines of up to €10 million or up to 2 per cent of the affected organisation's total worldwide annual turnover of the preceding financial year, whichever is higher.

Especially noteworthy regarding sanctions for failing to fulfil data protection duties is Article 66 of the PIPL. First, it stipulates fines of 1 million yuan on the affected organisation and up to 100,000 yuan on the responsible person (or persons) directly in charge, and in severe cases even up to 50 million yuan on the affected organisation. Second, the PIPL states a broad variation of other sanctions in grave cases, such as orders to rectify a data breach or the reporting of affected organisations that can lead to their business licences being cancelled. Also under the PIPL, at an organisational level, the competent authority may decide to prohibit the responsible individual from holding positions of director, supervisor or high-level manager, for a certain period.[35]

Conversely, the revFADP does not levy a fine if a company fails to comply with its notification duties at all. However, the Swiss Federal Data Protection and Information Commissioner (FDPIC) will have the authority to initiate an investigation (revFADP, Article 49(1)) or to order that data processing procedures be adapted if the Commissioner becomes aware of a violation of the revFADP, including data breach notification duties (Article 51(1)). In addition, the FDPIC may order the affected organisation to comply with its reporting obligations (Article 51(1)(f)). If such an order is not complied with, a fine of up to 250,000 Swiss francs may be issued (revFADP, Article 63). Finally, for example, if the data breach is due to the fact that the affected organisation did not comply with the minimum data security standards pursuant to Article 8(3) of the revFADP, a fine of up to 250,000 Swiss francs can be imposed as well (Article 61(c)).

Furthermore, additional criminal or civil liabilities may also be stipulated in the countries' respective data protection laws as well as civil or criminal codes.

34 See also LGPD, art. 52 and POPIA, sec. 109.

35 See, further, 'Guide to China's Personal Information Protection Law (PIPL)', Dentons, 24, at https://www.dentons.com/en/insights/articles/2021/august/30/guide-to-chinas-personal-information-protection-law (last accessed Jan. 2022).

As a result, affected organisations may be subject to sanctions or reputational risks (owing to investigations by the competent supervisory authorities) if they do not comply with their data breach notification obligations.[36] Hence, in the following section, we discuss how organisations processing personal data in the jurisdictions reviewed should prepare for and investigate a data breach to meet their notification duties successfully and protect their data as a critical asset.

The elements of a successful data breach response plan[37]

Although the comparative analysis of the data breach notification obligations demonstrated that there are certain differences between the requirements in the countries reviewed, they all provide notification obligations in the event of a data

36 Nieuwesteeg and Faure, op. cit., 1239.

37 Although this article reflects the authors' experience and views, see for additional information: Article-29-WP, Guidelines, 40; Bieri and Powell, op. cit., 787; NCSC, Cyberattacke – was tun? Informationen und Checklisten, at https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/vorfall-was-nun/checkliste-ciso.html (last accessed Jan. 2022); NCSC, Cyberattacke – was tun? Checkliste für CISOs für den Fall eines Cyberangriffs, at https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/infos-unternehmen/checkliste-ciso.pdf.download.pdf/checkliste-cisos-de.pdf (last accessed Jan. 2022); ICO, 'Self-assessment for data breaches', at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ (last accessed January 2022); ICO, 'Personal data breaches', at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (last accessed Jan. 2022); Australian government, Office of the Australian Information Commissioner, Data breach response plan, November 2021, at https://www.oaic.gov.au/about-us/our-corporate-information/key-documents/data-breach-response-plan (last accessed Jan. 2022); Australian government, Office of the Australian Information Commissioner, Data breach preparation and response, A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), at https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf (last accessed Jan. 2022); Canadian Centre for Cyber Security, 'Developing your incident response plan', at https://www.cyber.gc.ca/sites/default/files/2021-05/ITSAP.40.003%20Incident%20Response%20Planning.pdf (last accessed Jan. 2022); Office of the Privacy Commissioner of Canada, 'What you need to know about mandatory report of breaches of security safeguards' (October 2018), at https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/ (last accessed Jan. 2022); Office of the Privacy Commissioner of Canada, 'Preventing and responding to a privacy breach' (September 2018), at https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/c-t_201809_pb/ (last accessed Jan. 2022).

breach. Despite some common denominators, organisations should, therefore, keep in mind that they may be subject to multiple notification obligations if they operate in multiple jurisdictions.

In the authors' view, although the deadline and threshold for a notification and the exceptions to the obligation may vary from country to country, the approach in how to successfully identify, report and investigate a data breach can be the same for organisations in all the analysed jurisdictions.

The authors' past experience has shown that although organisations often focus on the implementation of security measures and are aware that they have certain reporting obligations in the event of a data breach, they are often not well-equipped to handle a data breach once it actually occurs.

Generally, a successful data breach response plan is comprised of four key parts:

- the implementation of data security measures to prevent data breaches in the first place;
- the determination of the persons responsible for identifying, investigating and reporting a data breach ('data breach reporting team');
- a policy outlining what employees have to do in the event of a data breach; and
- clear guidelines on how the data breach reporting team should identify, investigate and report a data breach.

Data security measures

As discussed above, organisations are required to implement appropriate measures to protect personal data from data breaches. These measures are both technical and organisational and can include password protection, firewalls, employee training, internal policies on how to treat personal data, access restrictions, encryption and the logging of data processing activities.[38]

To ensure the appropriateness of the security measures, organisations should review their data processing activities carefully by taking into account the types of data that are processed and the potential risks the data processing activity or external factors may pose to the data. It is recommended to work under different scenarios and to run through a worst-case scenario, such as a ransomware attack, where access to data is frozen unless a ransom is paid. Once an organisation has determined and

38 POPIA, sec. 19; LGPD, art. 46; PIPL, art. 51; FADP, art. 7; respectively; revFADP, art. 8; (UK) GDPR, art. 32; Privacy Act 1988, clause 11.1 pt. 4 of schedule 1; APPI, art. 20; and PIPEDA, clause 4.7.2 and 4.7.3 of schedule 1.

implemented the appropriate data security measures, these measures should be periodically tested and reviewed to ensure their robustness (e.g., by conducting stress and business continuity tests as well as simulating attacks).

Responsible persons and team

Once organisations are aware of their data breach notifications duties, they must designate the persons who are in charge of identifying, investigating and reporting data breaches. While ultimately the management or board of an organisation must be informed of a data breach that may need to be reported, the authors' experience has shown that the management often lacks the expertise necessary to actually investigate a data breach and decide on whether the legal requirements are met to report the identified data breach. Hence, an organisation must first designate the direct contact person for employees. Although many companies often define the direct supervisor of its employees as the initial internal point of contact, it is better to keep reporting channels narrow to meet the short deadlines to report breaches. Therefore, generally, it is recommended that organisations designate the data protection officer, the information security officer or the head of human resources as the initial point of contact for employees.

Next, an organisation should define the data breach reporting team who will be in charge of the investigation of the breach and the notification obligations. The team should report back to the management regularly. The data breach reporting team will also be in charge of defining the measures necessary to address the risks stemming from an identified data breach.[39] Therefore, the team should comprised internal and external persons who have the required technical and legal expertise. Against this background, data breach reporting teams often include the data protection officer, the information security officer, the IT department, in-house counsel, public relations and, potentially, external legal advisers, forensics and data protection experts as well as other external technical advisers who have more experience in handling data breaches.

Employee policy

Generally, the employee policy regarding data security breaches should include the following guidelines for all employees to follow:

- what data security entails and how an employee can contribute to it;
- what qualifies as a data breach;

39 Hladjk, op. cit.; GDPR, art. 33, no. 9.

- who an employee needs to inform about a data breach and how the responsible persons can be contacted; and
- how an employee should report a potential data breach.

The policy should be easily accessible, clear and concise, contain examples, not be too technical (there is no need for employees to understand the exact thresholds for a notification), and provide clear guidance on how an organisation's staff should proceed in the event of a data breach. As a general rule, it is recommended that employees report any type of data breach, no matter how serious. Then, during the investigation, the data breach reporting team can determine whether it qualifies as a reportable breach according to applicable data protection laws.

In addition, employees should be provided with a standard form to report the data breach – this is helpful to both the employees and the data breach reporting team. The form should include information such as the date, time and type of data breach, a short description of the data breach, details of the reporting employee, the type of affected data and the affected individuals, if possible, as well as the affected systems and information about the persons the employee has already informed. Finally, employees should be given training regarding data breaches to ensure that they understand what the policies and forms require.

Investigation and report

Once the data breach reporting team becomes aware of a potential data breach, it must initiate the detailed investigation. This is particularly important as the team is responsible for determining what caused the breach, what effects the breach may have, what risk-mitigating measures should be implemented, whether the breach has to be reported and, if so, who needs to be informed (the supervisory authority only or also the affected individuals).

Step 1: Preliminary investigation

The data breach reporting team should review the presented facts, ensure that all necessary internal and external persons are involved and make a high-level determination whether personal data is affected and what risks the data breach may entail. This allows the team to make a decision about whether the supervisory authority should be informed before all the information required by the applicable data protection law has been gathered. Particularly in very complex cases, where it is highly probable that personal data has been affected and the breach may entail high risks to the affected

individuals, organisations may opt to file a preliminary report to ensure that they do not miss their notification deadline. Furthermore, immediate actions such as securing the (potentially) breached data should be taken.

Step 2: Detailed investigation and risk analysis

Next, the focus should be on assessing the cause, nature and extent of the data breach, as well as its severity and consequences. In particular, the data breach reporting team should identify whether personal data has been affected and whether the threshold for a notification is reached. Therefore, this step also entails determining the risks to, and effects of the data breach on, the affected individuals. Although the investigation should be conducted as appropriate to each case, guidelines as to what constitutes a reportable data breach (i.e., explaining when the threshold to report a data breach is reached) should nonetheless be implemented. At this stage, the organisation should also decide whether it wants to file a police report (as this should be done as soon as possible), inform its insurance provider if it has coverage, assess civil claims against third parties, such as service providers, and assess whether the organisation may be subject to civil claims by the affected individuals.

Step 3: Determination of actions and measures

In this phase, the team must determine the required actions to contain the incident and restore control over the affected data. The key objectives are to (1) mitigate the potential consequences, (2) ensure the protection of the affected data from further breaches, and (3) enable the recovery of the systems and personal data to the greatest extent possible. This step also serves to ensure that all information required by law for the notification is compiled and that all evidence is gathered to protect the organisation from potential fines or claims from affected individuals. The main focus, however, should lie in defining the measures to be taken to mitigate the identified risks. Furthermore, the organisation should document any decision not to report an identified data breach if it concludes that the breach does not trigger applicable notification duties. Ultimately, the organisation remains accountable for such decisions if it is investigated by a supervisory authority because of a data breach.

Step 4: Implementation of identified measures and notification

Organisations should now implement all measures that can be taken immediately and define a plan for when the other measures will be executed. Furthermore, at this stage – within the deadline provided by applicable data protection laws – the data breach reporting team or management should notify the supervisory authority or affected

individuals as required by law. For this, the data breach reporting team should determine whether personal data in multiple jurisdictions is affected as this may trigger different reporting duties in several jurisdictions. If no personal data is affected by the data breach or an exception applies, no notification obligation is triggered. If the data breach reporting team concludes that an exception applies, this should be documented too. However, organisations should be aware that they may also be subject to other notification obligations in the event of a security breach based on contractual obligations or other legal provisions not relating to the protection of personal data (e.g., owing to applicable cybersecurity laws).

Step 5: Follow-up and report

As a last step, the remaining measures should be implemented, the affected systems should be tested and reinstated, and the data breach reporting team should write up a detailed report to ensure accountability in case there is an investigation by a supervisory authority. In this context, it is also important to eliminate identified deficiencies in the organisation's data security measures. Once this has been done, the organisation should review and test the implemented measures to ensure that the data breach response was successful. If that is the case, the organisation will have successfully met its investigation and reporting obligations according to applicable data protection laws.

Conclusion

There is a global trend towards an increasing importance afforded to data security and the corresponding reporting obligations if a data breach occurs. Generally, this is triggered by the global trend towards more data protection and accountability but organisations have a general incentive to comply with these obligations to protect the value of their assets – the data. While all jurisdictions reviewed stipulate a duty to implement data security measures and report data breaches, the legal requirements for such a notification differ. However, the necessary approach to successfully respond and react to a data breach is essentially the same.

After an organisation has implemented the required data security measures, it must implement the following steps to be able to successfully handle a data breach:

- determine the initial point of contact and data breach reporting team;
- implement an employee policy; and
- implement a detailed process for the investigation and reporting of the data breach, which should focus on the following topics:
    - dimension of the data breach (e.g., cause, affected persons, affected data, affected regions);

- type and consequences of the data breach;
- detailed investigation and risk analysis;
- mitigating measures and notification duties (data protection law but also other duties, such as contractual or cybersecurity law); and
- documentation, report and review of data breach and implemented measures.

Although the implementation of a successful data breach response plan may at first seem relatively straightforward, organisations should not underestimate the costs and effort it takes to implement a successful process. However, in view of the benefits these processes bring to protect data as a critical asset, the costs seem worthwhile.

Finally, as personal data breach notification obligations are increasing globally, so are cybersecurity requirements. Therefore, organisations should be aware that they may not only have notification obligations under applicable data protection laws but also other legal frameworks that must be accounted for. It will be interesting to see how these two fields develop (and interact) in the future, and, in particular, whether common approaches will be defined by the competent authorities or whether industry-specific guidelines or standards will emerge.

REHANA C HARASGAMA
Bär & Karrer Ltd

Dr Rehana C Harasgama has more than 10 years of experience in data protection law matters and is an expert in domestic and international data law and data protection law. She also advises clients on media and technology law as well as other regulatory topics. She joined Bär & Karrer in June 2019 and is the leading associate of the data protection team, where she is heavily involved in the business development of the practice.

Rehana Harasgama advises clients on complex data protection and privacy questions, such as major cross-border disclosure requests, the implementation of privacy-by-design, data protection due diligences, the implementation of data breach response plans, employee data protection and the sharing of data.

Rehana Harasgama is a lecturer at the Hochschule für Wirtschaft Zurich and at the University of St Gallen (HSG), where she teaches data protection law. She also regularly publishes scientific publications, newsletters and briefings.

Rehana Harasgama obtained her law degree and doctorate (PhD in law) at HSG, where she contributed to the international and interdisciplinary research project 'Remembering and Forgetting in the Digital Age' in collaboration with – among others – the Berkman Klein Center for Internet and Society at Harvard Law School.

JAN KLEINER
Bär & Karrer Ltd

Dr Jan Kleiner co-heads the firm's sport, media and data protection practice groups. His practice covers contentious and non-contentious matters in the fields of national and international sports law as well as media, entertainment and data protection law. He furthermore advises clients on technology and telecommunication law matters.

Jan Kleiner has obtained a doctorate in international sports law from the University of Zurich and holds a Global Executive Master in International Sports Law from the Instituto Superior de Derecho y Economia in Madrid (Spain).

Jan Kleiner regularly publishes on national and international sports law topics and data protection matters. He is a lecturer in international sports law at the University of Zurich and in various other national and international sports law master programmes. He is also a lecturer in data protection law at the University of Applied Sciences of the Canton of Graubünden. He furthermore acts as President of the Sports Law Alumni, an international alumni organisation of sports law graduates.

Jan Kleiner is listed as a Thought Leader in sports law by *Who's Who Legal* and he is a recognised leader in technology, media and telecommunications law.

VIVIANE BERGER
Bär & Karrer Ltd

Viviane Berger is a junior associate at Bär & Karrer and advises clients on EU and Swiss data protection law as well as real estate matters. In particular, she advises on cross-border data disclosures, employee data protection and data protection due diligences and assists in the drafting of data protection policies and processes.

Viviane Berger holds a master's degree in law from the University of Basel.

Bär & Karrer is a leading Swiss law firm with more than 170 lawyers in Zurich, Geneva, Lugano, Zug and Basel. Our core business is advising our clients on innovative and complex transactions and representing them in litigation, arbitration and regulatory proceedings. Our clients range from multinational corporations to private individuals in Switzerland and around the world.

Most of our work has an international component. We have broad experience handling cross-border proceedings and transactions. Our extensive network consists of correspondent law firms that are all market leaders in their jurisdictions.

Bär & Karrer has repeatedly been awarded Switzerland Law Firm of the Year by the most important international legal ranking agencies in recent years: Citywealth Magic Circle Awards Law Firm of the Year (2021, 2022); Euromoney LMG Life Science Firm of the Year (2020); Euromoney LMG European Financial & Corporate Firm of the Year (2020); STEP International Legal Team of the Year (2020); IP Global Awards, Swiss IP-Transactions Firm of the Year (2020); 2020, 2019, 2018 and 2017 Trophées du Droit Silver (2017–2020); *IFLR* Award (2014, 2015, 2019); *IFLR* Debt and Equity-linked Deal of the Year (2019); Mergermarket European M&A Award (Legal Adviser of the Year) (2014–2016, 2018–2019); *IFLR* M&A Deal of the Year (2018); Best in Trusts & Estates by Euromoney LMG (2018); Trophées du Droit Gold (2016); *Chambers* European Awards (2012, 2013, 2016); *The Legal 500* (most recommended law firm in Switzerland) (2014–2016); and *The Lawyer* European Award (2010–2011, 2013–2015).

Brandschenkestrasse 90
8002 Zurich
Switzerland
Tel: +41 58 261 50 00
www.baerkarrer.ch

Rehana C Harasgama
rehana.harasgama@baerkarrer.ch

Jan Kleiner
jan.kleiner@baerkarrer.ch

Viviane Berger
viviane.berger@baerkarrer.ch

The Paper Trail: Data Protection Impact Assessments and Documentation

Felipe Palhares[1]
BMA – Barbosa, Müssnich, Aragão Advogados

Introduction

During the past few years, several data protection laws have been enacted throughout the world. The European Union's General Data Protection Regulation (GDPR)[2] has been viewed as one of the most comprehensive data protection laws in the world and is deemed by many to be the gold standard for laws regulating the processing of personal data. It is no surprise, therefore, that the drafting of data protection laws in many countries has been inspired by the GDPR.[3]

One similarity between the GDPR and the data protection laws in many countries is the idea of accountability, which reflects the obligation of the data controller to be responsible for, and to be able to demonstrate, compliance with the law. In other words, simply complying with the law is not enough: data controllers must be able to effectively show that they are complying with the law.

To do that, creating documentation is fundamental. In some situations, it may also be one of the main obligations of data controllers, such as having records of the processing activities, structuring privacy notices that observe the principle of transparency by providing data subjects with proper information about the processing activities, drafting incident response plans to handle data breaches, and the like.

---

1 Felipe Palhares is a partner at BMA – Barbosa, Müssnich, Aragão Advogados.

2 Regulation (EU) 2016/679.

3 One of those countries is Brazil. In August 2018, legislators enacted Law No. 13.709/2018 – commonly referred to as the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais), which is the first law in Brazil drafted specifically to regulate the processing of personal data. It came into effect on 18 September 2021.

This chapter focuses on one of the most relevant documents for this paper trail: data protection impact assessments (DPIAs). A DPIA is a process that shows that the data controller, having noticed that a project that involves the processing of personal data may result in risks to the fundamental rights and individual freedom of data subjects, has conducted a prior analysis regarding the intended processing activities, identifying the risks arising from the processing and mapping measures that could be implemented to reduce or eliminate those risks.

We begin with a brief overview of how different countries have used DPIAs (or privacy impact assessments (PIAs)) over the years to understand the evolution of this process and the distinct approaches by different laws.

As Brazil is one of the countries that has followed the GDPR stance of making accountability a key element of compliance with its data protection law, in the final section we look at how Brazil's experience can provide a model for accountability and what it may hold for the future.

European Union

The European Union is considered the cradle of identification and standardisation of the social value of modern privacy, raised to a fundamental human right, and the conception of practices in favour of the protection of personal data. Nonetheless, even at the European level, the history of adopting DPIAs is fairly recent.

Regulation (EU) 2016/679 (the GDPR), which was approved on 14 April 2016 and became fully effective on 25 May 2018, was the first law in the European Union that imposed a mandatory requirement on data controllers to conduct DPIAs in some cases, specifically where the processing is likely to result in a high risk to the rights and freedom of natural persons. However, the fact that a requirement for conducting a DPIA has only been set forth by law fairly recently is not to say that PIAs were not a subject of attention by EU Member States prior to 2016.

The United Kingdom was the first (being a Member State at that time) to emphasise the importance of conducting PIAs, when editing, through the Information Commissioner's Office (ICO), a manual on PIAs, released in December 2007 and revised in June 2009.[4]

4 Wright, David; Finn, Rachel; Rodrigues, Rowena, 'A comparative analysis of privacy impact assessment in six countries', *Journal of Contemporary European Research*, Vol. 9, Issue 1 (2013), p. 170.

The manual published by the ICO identified a PIA as a process that helps to visualise the risks arising from the collection, use or disclosure of information about individuals and to anticipate any problems arising from these practices and possible solutions to those difficulties.[5] The responsibility for conducting a PIA would lie with the senior executive level of the organisation, especially someone linked to the areas of audit or risk analysis. Among the reasons listed by the ICO to understand that it was necessary to carry out a PIA were preventing inappropriate solutions and minimising the costs of a project that may have a high probability of privacy risks, causing a loss of trust and damage to the reputation of the organisation with its stakeholders.

The ICO listed 11 questions as a screening to aid in determining whether a large-scale PIA, with an exhaustive analysis of the privacy risks posed by the project, should be undertaken. Depending on the responses to these questions, conducting a PIA could be highly recommended as an appropriate measure to prevent greater risks to data subjects.

In November 2010, the European Commission published a communication entitled 'A comprehensive approach on personal data protection in the European Union', in which it outlined the challenges being faced 15 years after the publication of Directive 95/46/EC (the Data Protection Directive), and stating the profound changes around the world as a result of globalisation and the accelerated development of new technologies, especially those that collect data in ways that are not easily perceptible to individuals.[6]

One of the ways identified by the European Commission to ensure that data controllers adopted more adequate policies to respect the privacy of individuals and more effective data protection mechanisms was precisely the analysis of the possible inclusion of an obligation to carry out DPIAs in certain cases, such as when sensitive personal data is processed. This mandatory requirement, however, would not actually be implemented until much later, with the entry into force of the GDPR.

In December 2010, Ireland was the second EU Member State to publish a guide on carrying out PIAs, specifically for the processing of sensitive data about aspects of the health of patients in hospitals across the country. Among other things, this guide

---

5 Wadhwa, Kush, 'Privacy impact assessment reports: a report card', *Info*, Vol. 14, Issue 3 (2012), p. 40.

6 European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF (last accessed 31 Jan. 2022).

analysed factors that must be taken into account to identify real and potential risks to the privacy of data subjects, indicating the questions that must be asked by health service providers and proposing a step-by-step process for performing a PIA.[7]

The process proposed by the Health Information and Quality Authority of Ireland was divided into four stages: (1) answering an 11-question questionnaire – a positive answer to only one of them would make it necessary to conduct a PIA; (2) identifying potential privacy risks, detailing the project scope, information flows and adopted security measures; (3) analysing the identified risks and defining ways to eliminate or reduce them; and (4) preparation of the report itself, with the documentation of the entire process that had been carried out so far.

One of the relevant points exposed by the Health Information and Quality Authority's guide was the need for the PIA to be regularly updated and to monitor the development process of the respective product or service, so as to ensure that all possible risks to privacy discovered along the way were addressed by the report.[8] Therefore, it was not deemed sufficient to prepare a PIA and keep it for registration only – the report would have to be revisited frequently.

In February 2011, the Article 29 Working Party (WP29) ratified the recommendations issued by the European Commission on the development of a PIA model to be adopted for the development of products or services involving identification methods by radio frequency.[9] This is the first example of using PIAs to address concerns relating to a specific industry sector.[10]

In February 2014, the ICO published a new guide on PIAs entitled 'Conducting privacy impact assessments code of practice'. This code was intended to improve the guidelines formulated in the manual made available in 2007 and revised in 2009, especially to make it clearer how to better integrate PIAs with existing projects and other risk management tools, as well as to make the PIAs more effective and practical tools.

---

7 Wright, David, 'The state of the art in privacy impact assessment', *Computer Law & Security Review*, Vol. 38 (2012), p. 55.

8 Health Information and Quality Authority, 'Guidance on Privacy Impact Assessment in Health and Social Care' (December 2010), p. 14, available at www.hiqa.ie/sites/default/files/2017-03/HI_Privacy_Impact_Assessment.pdf (last accessed 31 Jan. 2022).

9 Article 29 Data Protection Working Party, 'Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (February 2011), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf (last accessed 31 Jan. 2022).

10 Costa, Luiz, 'Privacy and the precautionary principle', *Computer Law & Security Review*, Vol. 28, 2012, p. 19.

The code identifies some projects that possibly warrant a PIA being carried out, such as a new surveillance system or the application of new technologies to existing systems, and explains that it is up to each organisation to define who is better positioned internally to coordinate the process, and emphasising that the data protection officer, when such a position exists in the organisation, is naturally seen as a professional who will have significant influence on the work, even though she or he may not be responsible for carrying out all steps of the process.[11]

In April 2017, WP29 issued a guideline on DPIAs and when a risk should be interpreted as high. In the document, WP29 indicates some criteria that must be taken into account for the analysis, such as whether the processing involves sensitive data, whether personal data will be transferred outside the European Union, whether innovative uses will be adopted, among other things. If two of these criteria are present, the interpretation of WP29 was that it was highly likely that the processing could involve high risks. The guide also advises that a DPIA should be re-evaluated at least every three years, or less, depending on the nature of the processing.[12]

On 25 May 2018, when the GDPR became fully effective, conducting a DPIA was set as a requirement under Article 35(1). It is interesting to note that the text of the GDPR brings a condition regarding the quantification of the level of risk to the rights and freedom of natural persons to assess whether or not there is an obligation to carry out a DPIA.

Although it is stated explicitly that the use of new technologies is considered as an aspect to be observed when assessing the obligation to carry out a DPIA, the criterion that effectively defines whether a previous DPIA should have been conducted is the existence of a high risk to the rights and freedom of individuals. It is not, therefore, any type of risk that triggers the requirement for a DPIA, only those risks that are considered more serious and that may cause greater damage to the privacy of natural persons.

11 Information Commissioner's Office, 'Conducting privacy impact assessments code of practice: Data Protection Act', available at www.pdpjournals.com/docs/88317.pdf (last accessed 31 Jan. 2022).

12 Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 (last accessed 31 Jan. 2022).

The great difficulty, however, is to measure this risk and identify when it would actually be deemed high, compared with the less relevant risks that would not entail the obligation to carry out a DPIA. In this sense, the GDPR text itself includes an exemplifying list of situations in which a DPIA would clearly be necessary, provided for in Article 35(3).

Among the hypotheses therein are (1) in the case of systematic and exhaustive assessments of personal aspects about natural persons, which are based on automated data processing, including profiling, and in which decisions that produce legal effects for these individuals are ruled or similarly affect them, (2) in cases of large-scale processing of sensitive data or data about criminal convictions or criminal offences and (3) in cases of large-scale systematic monitoring of publicly accessible areas.

It is worth remembering that these hypotheses are merely illustrative, not exhaustive. Also, for this very reason, the GDPR has already foreseen that the supervisory authorities of EU Member States should establish and make public lists with specific processing activities that would be subject to the obligation to carry out a DPIA, in accordance with its sole discretion, respecting the consistency mechanism provided for in the Regulation, so that different authorities do not have divergent positions on the same topic that may affect the free flow of personal data within the European Union.

The opinions issued by the European Data Protection Board in the past few years on the lists made available by supervisory authorities of EU Member States bring some interesting points that deserve note, including the following:

- the processing of biometric data does not necessarily represent a high risk; however, when this processing activity is carried out only to identify a natural person and with at least some more criteria, a DPIA would be necessary;[13]
- the use of a new or innovative technology, by itself, does not represent a high risk, so that the requirement for a DPIA in this case would need to be guided in conjunction with some other criterion;[14]

13 European Data Protection Board (EDPB), 'Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)', available at https://edpb.europa.eu/sites/edpb/files/files/file1/201906_edpb_art.64_es_sas_dpia_list_en_0.pdf (last accessed 31 Jan. 2022).

14 EDPB, 'Opinion 21/2018 on the draft list of the competent supervisory authority of Slovakia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' , available at https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_sk_sas_dpia_list_en.pdf (last accessed 31 Jan. 2022).

- the processing of data not relating to health, collected or processed with the aid of a body implant, does not require the carrying out of a DPIA in all cases, but the processing of health data by such an implant does;[15] and
- the processing of location data does not necessarily represent a high risk, and may be carried out without carrying out a DPIA, except in cases where other additional criteria are present that make the performance of a DPIA necessary in accordance with the joint analysis of all the factors involved.[16]

Another relevant aspect about DPIAs under the GDPR regime is the data controller's duty to carry out a prior consultation with the competent supervisory authority when an assessment indicates that the processing would result in a high risk to data subjects in the absence of measures taken to mitigate those risks.

United States

PIAs have been known and used in the United States for several years. In 2002, the E-Government Act was passed, a federal law designed to improve the administration and promotion of electronic services provided by the government and to establish a framework of measures to improve citizens' access to the respective services and to government information.[17]

In Section 208 of the Act, an obligation was created for government agencies to conduct a PIA before developing or acquiring technologies that collect, maintain or disseminate information that is in an identifiable format or before initiating a new collection of information that will be collected, maintained or disseminated using

15 EDPB, 'Opinion 18/2018 on the draft list of the competent supervisory authority of Portugal regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)', available at https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_pt_sas_dpia_list_en.pdf (last accessed 31 Jan. 2022).

16 EDPB, 'Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)', available at https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf (last accessed 31 Jan. 2022).

17 Clarke, Roger, 'An evaluation of privacy impact assessment guidance documents', *International Data Privacy Law*, Vol. 1, Issue 2 (2011), p. 117.

information technologies, and include any information in an identifiable form, allowing physical or digital contact with a particular individual, provided that the collection is imposed on 10 or more people, excluding employees of the federal government.[18]

The PIA must be reviewed and approved by the chief information officer or equivalent position of the respective government agency and, after its approval, must be made public through the agency's website or publication in the official gazette, except when there is a need to protect classified, confidential or private information. A copy of the report must be provided to the agency director, who may edit specifications on the minimum content of a PIA within the respective agency.

In September 2003, the Office of Management and Budget, linked to the Office of the President of the United States of America, issued a memorandum addressed to the heads of government agencies and departments of the Executive Branch with guidance on how to implement the provisions of the E-Government Act regarding the performance of PIAs.

As indicated in that document, PIAs must be carried out and updated whenever necessary, especially when there is any change in systems that creates risks to privacy, such as the conversion of paper support systems to the shared use of digital or new media among government agencies, with the exchange of information in identifiable formats.[19]

Another point made clear by the memorandum was that agencies should identify, in the PIAs, what choices were made in relation to information technology systems and information collection as a result of carrying out the PIA, and that the study should be carried out at the beginning of the development, being later updated before the effective implementation of the system to consider aspects that were not identified at the product design stage.[20]

It is interesting to note that the obligation to carry out PIAs in the United States, at the federal level, is restricted to departments of the Executive Branch, government agencies and any third parties that contract with them, provided that they use

18 Seto, Yoichi, 'Application of privacy impact assessment in the smart city', *Electronics and Communication in Japan*, Vol. 98, Issue 2 (2015), p. 11.

19 Office of Management and Budget, 'M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002' (26 September 2003), available at www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf (last accessed 31 Jan. 2022).

20 Wright, David; Finn, Rachel; Rodrigues, Rowena, op. cit., at p. 171.

information technologies or operate websites with the purpose of interacting with the public. In other words, there is no federal mandate that determines the performance of PIAs by private companies without direct contractual relations with the public administration, demonstrating one of the aspects much discussed in relation to privacy and data protection in North America, that such factors cannot impede or create obstacles to business development.

Canada

The Canadian provinces of Ontario, British Columbia and Alberta were the first to develop specific regulations on PIAs, even before the topic was discussed at the federal level.[21]

In Ontario, conducting a PIA became a mandatory and prior requirement for the approval of any government project involving information and information technologies as of 1998, with the subsequent availability of guidelines in December 1999 in a guide issued by a government agency known at the time as the Management Board Secretariat.[22]

In British Columbia, PIAs became mandatory on the part of government agencies for the implementation of any new system, project or programme as of 2002, owing to changes made to the Freedom of Information and Protection of Privacy Act, even if the provisions contained in that law do not treat PIAs as a comprehensive study of privacy risks, but rather as a checklist verification to ensure that certain legal requirements are being adhered to.

In Alberta, the preparation of PIAs began to be required with the passage of the Health Information Act in 1999, even though the provisions only apply to agencies in the health sector, so that no other sector, whether public or private, is obliged to comply with the rules. In early 2009, the Office of the Information and Privacy Commissioner (OIPC) revised the manuals it had previously published on the performance of PIAs, making it clear that reports would need to be submitted to the OIPC prior to implementing the proposed project. Those reports could be rejected by the OIPC or readjusted in accordance with the OIPC guidelines.[23]

---

21 Bryant, Jennifer, 'Washington Privacy Act fails for second time', International Association of Privacy Professionals (13 March 2020), available at https://iapp.org/news/a/washington-privacy-act-fails-for-second-time/ (last accessed 31 Jan. 2022).

22 Clarke, Roger, op. cit., at p. 127.

23 Wright, David; Finn, Rachel; Rodrigues, Rowena, op. cit., at p. 167.

At the federal level, all government institutions are subject to the obligation to carry out a PIA to ensure that any projects or initiatives to be implemented, and that involve the collection, use or provision of personal information, comply with the provisions set out in the Privacy Act, Library and Archives of Canada Act, and government privacy and data protection policies. Any substantial changes to existing programmes or projects that could pose a risk to privacy should also be subject to a PIA.

The final report of the PIA must be submitted to the Treasury Board of Canada Secretariat (TBS) and the Office of the Privacy Commissioner of Canada. In April 2010, the TBS promulgated a new directive on PIAs, which linked the performance of PIAs to the release of funds for programme approval. This means that when a government agency does not complete a PIA, in cases where it is obliged to do so, it may not receive the necessary resources to implement the respective project.

As is the case in the United States, there is no specific legislation that obliges private companies to carry out PIAs, although they may be viewed favourably by regulators in the event of a data breach.

Suggested model for DPIAs in Brazil

Brazil's General Data Protection Law (LGPD)[24] is the first Brazilian law to address DPIAs. Prior to its enactment, impact assessments regarding privacy or data protection were not something that was considered by local regulators, thus the current lack of guidance on the performance of DPIAs in the country.

Even though the LGPD came into force in September 2021, it is still not clear when a DPIA is actually required under the law. The relevant provisions are open to doubt and, unlike the GDPR, there are no provisions that explicitly state that a DPIA should be carried out where a high risk to the individual rights and freedom of the data subjects is expected.

According to Article 38 of the LGPD, the National Data Protection Authority (ANPD) may request data controllers to carry out a DPIA at any time and shall issue further regulations on carrying out DPIAs, but there is no prior obligation set forth by this provision to carry out a DPIA before any request from the ANPD.

Besides that provision, Article 10, Paragraph 3 of the LGPD also mentions that the ANPD may request a DPIA when the processing is based on the legitimate interests of the data controller. Although some commentators believe that this provision set out a requirement for carrying out a DPIA in every instance where the lawful ground

24 See footnote 3, above.

for the processing is the legitimate interest of the data controller, it seems that this interpretation would create an unnecessary burden that was not intended by the legislator, especially considering that not every processing activity based on the legitimate interest of the controller carries a high risk to the data subjects.

Although there is no guidance from the ANPD, we believe that an appropriate approach for when it would be necessary to carry out a DPIA should be based on an evaluation of the level of risk to the rights and freedom of data subjects resulting from the processing activities, in a similar way to how this is addressed by the GDPR. The recommended approach would be to adopt an assessment method supported by thresholds defined by the data controller, through the response to a previously prepared standard questionnaire, with a checklist of some crucial factors that must be analysed and that might indicate risks involved in a given personal data processing activity. The questions could include the following:

Does the project involve the processing of sensitive personal data?
Does the project involve the processing of personal data of vulnerable individuals?
Does the project involve large-scale processing?
Does the project involve systematic monitoring of data subjects or public areas?
Does the project involve the adoption of decisions based on automated data processing?
Does the project involve new technologies or new applications of current technologies?
Does the project involve profiling, scoring or another form of specific classification attributed to each data subject and decisions based on this classification?
Does the project involve any type of restriction on data subjects in exercising their rights?
Does the project involve combining, comparing or matching data from multiple sources?
Does the project involve the processing of geolocation data from data subjects?
Does the project involve the processing of personal data of children and adolescents?
Does the project involve sharing personal data with third parties?
Does the project involve international transfers of personal data?
Does the project involve contacting data subjects in ways that could be considered intrusive?
Does the project involve the processing of financial data?
Does the project involve the processing of data that, although considered anonymised, may, in combination with other data, from the same source or from multiple sources, allow data subjects to be identified?
Does the project involve the indirect collection of personal data, when it is not possible or feasible to guarantee the right to information to the data subject?
Does the project involve the migration of personal data from one system to another?

Although an isolated positive answer to some of the above questions does not mean, by itself, the existence of a high risk to the rights and freedom of data subjects, these questions serve as a good basis for evaluating the level of risk involved in the project, given that the more affirmative answers given, the greater the risk in the intended operation. When a high risk is observed, it is recommended that a DPIA be carried out, regardless of any request from the ANPD.

Answering such a questionnaire might give the false impression that carrying out a DPIA is only a tick-box exercise, but this is far from what is truly expected from such an assessment. The DPIA should be seen as a process rather than just a report, composed of several steps towards drafting a final report and that are fundamental to the process. Those fundamental steps might include the following:

Describing the proposed project, including its nature, scope, context, purposes and legal bases for data processing
Describing the types of data collected, the volume, the methodology used for collection, with whom the data will be shared, who the data controllers and processors will be, how the data will be stored and for how long the data will be used and retained, the measures of security already in place and who can access the data
Explaining the choices made in the project so that it complies with all the fundamental principles set out in Article 6 of the LGPD
Analysing data flows and identifying possible risks to privacy involved in the project that may violate the fundamental rights and freedom of data subjects, classifying the probability and degree of the respective risks
Identifying and analysing the measures and safeguards that could be implemented to eliminate, or at least reduce, the risks involved
Consulting the stakeholders involved, taking into account any suggestions received and the concerns raised by them
Formulating the necessary recommendations, establishing an action plan for its implementation, and integrating the solutions into the project before it is available to the market
Preparing the report itself and, depending on the case, evaluating its public disclosure for knowledge by the stakeholders involved
Implementing the recommendations set out in the report
Reviewing and updating the DPIA throughout the life of the project, ensuring that the assumptions and descriptions defined in the report remain true and that there are no new identified risks and new protective measures to be implemented

These steps are merely illustrative and serve as a standard threshold to be considered, but others can be added, so that the structure of the DPIA process is in accordance with an organisation's guidelines.

What can never be omitted is a description of the types of data that will be processed, the methods by which they will be collected, the guarantees of information security and the formulation of measures, safeguards and mechanisms that will be implemented to mitigate the highlighted risks, pursuant to the express determination of Article 38, sole paragraph, of the LGPD.

One of the most important points about the steps outlined above is that the DPIA cannot be an end in itself. It is not enough to draw up a report and imagine that the final document, alone, which will be used to record the process carried out, is sufficient to prevent all the risks involved with a given project. On the contrary, as it is a process, the DPIA must be regularly updated and revised, following the project throughout the time it is implemented and adopted by the organisation.

After all, a small change in some aspect of the project, even after it has already been implemented and is being made available to the market, can significantly change the risks to the privacy of data subjects, making it essential to adopt new measures of previously unanticipated mitigation.

This suggested model for a DPIA in Brazil should be reviewed once the ANPD has issued further regulation on this subject. It is expected that the ANPD will provide specific instructions about when and how to conduct DPIAs.

FELIPE PALHARES
BMA – Barbosa, Müssnich, Aragão Advogados

Felipe Palhares heads the data privacy and cybersecurity practice of BMA – Barbosa, Müssnich, Aragão Advogados, a prominent Brazilian full service law firm. Felipe has extensive experience in assisting local and international clients in strategic matters that involve the processing of personal data, in managing the response to data breaches and ransomware attacks, and in dealing with regulators.

He is the only individual in the world to have earned all current certifications and designations issued by the International Association of Privacy Professionals (including CIPP/A, CIPP/C, CIPP/E, CIPP/US, CIPM, CIPT, CDPO/BR, CDPO/FR, FIP and PLS). He holds an LLM from New York University and a Data Protection Officer Professional University Certificate (ECPC-B DPO) from Maastricht University.

Felipe has been recognised by Global Data Review as one of the brightest young data lawyers in the world and profiled in the 2021 edition of its 40 Under 40 list, and is frequently ranked among the top professionals in the field by major directories, including *Chambers and Partners*, *The Legal 500*, *Who's Who Legal* and *Leaders League*. Felipe is admitted to practise law in Brazil and in New York.

Founded in the 1990s, when Brazil was undergoing structural changes, BMA – Barbosa Müssnich Aragão was inspired by a mission to find innovative solutions that are legally viable and sustainable in an environment of rapid development, new regulatory frameworks and new business models in almost all sectors of the economy. Inspired to be a pioneering law firm, ready — and more than able — to take on the big projects and big problems that require sophisticated solutions. An active participant in the privatizations that took place in the 1990s, BMA had achieved a solid reputation and both national and international recognition even before becoming one of the leading firms in Brazil in the mid-2000s, when the Brazilian market experienced a wave of initial public offerings and mergers and acquisitions.

BMA has been present in most of the major M&A transactions in Brazil during the past two decades, participating in the creation of corporate groups that do business around the world. BMA has acquired an impressive stock of know-how in infrastructure projects, especially in the areas of ports, railways, highways, oil and gas, energy and telecommunications. BMA's experienced professionals know that a thorough understanding of the firm's clients' business objectives is essential. BMA works to achieve creative, effective solutions by integrating its specialist teams to ensure a multidisciplinary approach to legal problems.

Av. Presidente Juscelino Kubitschek 1455
10th Floor
São Paulo 04543-011
Brazil
Tel: +55 11 2179 4600
www.bmalaw.com.br

Felipe Palhares
felipe.palhares@bmalaw.com.br

Accountability to Data Subjects and Regulators

Cédric Burton, Laura De Boel, Christopher N Olsen and Lydia B Parnes[1]
Wilson Sonsini Goodrich & Rosati

Introduction

In both the European Union and the United States, governments and data subjects may hold companies accountable for failure to maintain adequate privacy and security protections for their data assets. This article explores the similarities and differences between the EU approach, largely driven by Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), and the US approach, largely driven by the Federal Trade Commission (FTC) and state law. Although the GDPR is theoretically a unifying statute with an express accountability principle, details about what constitute 'appropriate' measures continue to be worked out as the GDPR is applied. The FTC has developed its standards for privacy and data security through case-by-case enforcement over many years. Both the FTC and US state authorities rely on concepts such as 'reasonable' privacy and security measures that are fluid. Thus, companies are regularly held accountable in both jurisdictions, but compliance is no box-checking exercise. Companies that treat data as a critical asset are more likely to have the type of data governance framework in place that is needed to comply with accountability requirements.

---

1 Cédric Burton, Laura De Boel, Christopher N Olsen and Lydia B Parnes are partners at Wilson Sonsini Goodrich & Rosati (WSGR). The authors wish to acknowledge contributions to this article by Roberto Yunquera Sehwani, an associate in the Brussels office of WSGR, and Steve Schultze, an associate in the Washington, DC, office of WSGR.

Accountability under the GDPR

In the European Union, the principle of accountability is codified in Article 5(2) of the GDPR, which states that data controllers shall be 'responsible for, and be able to demonstrate compliance with' the GDPR's core principles. Accountability therefore entails two key elements: (1) the data controller is responsible for complying with the GDPR; and (2) the data controller must be able to demonstrate that it is compliant.[2] Although the principle is stated in simple terms, it is both broad and abstract. It is up to the individual data controller to decipher whether it has 'appropriate' measures in place to comply with all GDPR obligations and sufficient records to demonstrate that compliance.

Pre-GDPR, EU supervisory authorities (SAs) had advocated for the creation of an accountability principle to ensure that companies would take a proactive approach to their compliance with data protection laws.[3] SAs proposed the accountability principle so as to require companies to assess the data privacy and security risks posed by their activities and define the safeguards that would best mitigate those risks.[4] With the GDPR, the accountability principle became part of EU data protection law.

GDPR accountability in practice

Certain accountability measures for data assets are stipulated in the GDPR, such as record-keeping,[5] appointing a data protection officer (DPO)[6] and conducting data protection impact assessments (DPIAs).[7]

---

2 Information Commissioner's Office (ICO), Guide to the GDPR, 'Accountability and Governance', p. 1, at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance-1-1.pdf (last accessed 9 Feb. 2022).

3 Article 29 Data Protection Working Party (WP29), 'Opinion 3/2010 on the principle of accountability' (Opinion 3/2010), para. 25.

4 'A provision on accountability would require data controllers to define and implement the necessary measures to ensure compliance with the principles and obligations of the Directive and to have their effectiveness verified periodically' – WP29 Opinion 3/2010, para. 39.

5 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR), Article 30.

6 ibid., Article 37.

7 ibid., Article 35.

In addition, companies must take certain steps not expressly spelled out in the GDPR to comply with the accountability principle. For instance, large organisations will be expected to develop a comprehensive privacy management framework with dedicated staff, clear reporting lines, internal policies and procedures, and strong privacy safeguards embedded in their products or services.[8]

Organisations are typically expected to take the following measures to comply with the accountability principle.

Risk assessments and DPIAs

The GDPR requires companies to carry out a DPIA before conducting processing activities that may entail a high privacy risk. DPIAs must adhere to the structure set out in the DPIA Guidelines[9] of the European Data Protection Board (EDPB).[10] In addition to carrying out DPIAs for specific processing activities, organisations are expected to assess privacy risks throughout their operations. For instance, when outsourcing data processing to vendors, organisations should assess the privacy risks associated with vendor engagement.

Data protection officer

Although any organisation can choose to appoint a DPO, those that carry out certain privacy-sensitive processing operations on a large scale are required to appoint a DPO (e.g., large-scale profiling for credit scoring purposes). Companies should develop written policies and procedures to ensure the DPO's function is structured in accordance with the EDPB's Guidelines on DPOs.[11] In our experience, SAs often request companies to produce such documentation when they investigate an organisation, in particular to verify the DPO's independence within the organisation. Organisations need to comply with the GDPR's requirements on the designation, position and tasks

8 ICO, Guide to the GDPR, 'Accountability and Governance', p. 3.

9 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', available at https://ec.europa.eu/newsroom/article29/items/611236 (last accessed 9 Feb. 2022).

10 The European Data Protection Board (EDPB) is an EU body that consists of all national supervisory authorities (SAs) in the European Union.

11 'Guidelines on Data Protection Officers ('DPOs')', available at https://ec.europa.eu/newsroom/article29/items/612048 (last accessed 9 Feb. 2022).

of the DPO even when the DPO is voluntarily appointed. Several SAs have already imposed fines on organisations that failed to demonstrate they had set up the DPO function in a compliant manner (see below).

Records of processing

The GDPR requires companies to keep records listing all data processing activities that they undertake. Records should be kept up to date and ready to be shared with SAs at their request. Several SAs have made template records available,[12] and they typically go beyond the information required by the GDPR. For instance, SAs' template records typically require companies to indicate the legal basis for data processing, which is not strictly required by the GDPR.[13] Companies should follow the guidance of the competent SA. SAs have already fined organisations for failure to have records of processing in place (see below).

Internal policies and procedures

Organisations are expected to implement internal policies and procedures regarding their data assets to ensure GDPR compliance in practice. Although the GDPR does not specify the issues that need to be addressed, typical policies and procedures include data handling policy, data breach handling policy, individuals' rights policy, data retention policy, data security policy and data protection audit procedure.

Training

Organisations should ensure that staff receive periodic training on privacy laws and the company's internal policies and procedures. Organisations should keep records of these training sessions to be able to demonstrate that they have implemented a comprehensive GDPR training programme.

---

12 For example, Belgian SA's template records, available at https://www.autoriteprotectiondonnees.be/professionnel/premiere-aide/toolbox; Italian SA's template records, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9047529; French SA's template records, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement (web pages last accessed 9 Feb. 2022).

13 For example, Italian SA's template records, op. cit.; Polish SA's template records, available at https://uodo.gov.pl/pl/383/214 (last accessed 9 Feb. 2022).

Audit and review

The accountability principle also requires organisations to periodically review their approach to privacy compliance, to ensure that the implemented measures and safeguards remain appropriate in light of the privacy risks generated by the organisation's activities.

Codes of conduct and certification

The GDPR allows SAs to approve privacy codes of conduct and certificates to which companies could adhere. Adhering to an approved code of conduct or certification may serve to demonstrate a company's compliance with the accountability principle. However, few codes of conduct and certification schemes are currently available and adhering to a GDPR code of conduct or certification is not yet market practice.[14]

Enforcement of the GDPR accountability principle

Enforcement by supervisory authorities

Violation of the accountability principle is subject to the highest level of fines (i.e., €20 million (about US$24.35 million) or 4 per cent of the total worldwide annual turnover, whichever is higher). Several fines have already been imposed for violation of the accountability principle, albeit much lower. The following are some examples:

- The SA of Baden-Württemberg, Germany, imposed a fine of €300,000 for failure to provide adequate documentation concerning a vendor engagement. The company could not provide documentation identifying the types of personal data disclosed to the vendor, and the safeguards in place to protect the data.[15]

14 For example, the Belgian SA recently approved its first transnational code of conduct intended for cloud service providers (EU Cloud Code of Conduct) – more information available at https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct. The EDPB keeps a public register for codes of conduct and for certification mechanisms, seals and marks, available at https://edpb.europa.eu/accountability-tools_en (web pages last accessed 9 Feb. 2022).

15 See FAQs at https://www.vfb.de/de/vfb/aktuell/neues/club/2021/fragen-und-antworten-zur-datenaffaere/ and press release of the data protection authority at https://www.baden-wuerttemberg.datenschutz.de/vfb-stuttgart-bussgeld-erlassen/ (web pages last accessed 9 Feb. 2022).

- The Greek SA imposed a fine of €150,000 on a company for failure to document its choice of legal basis for its processing activities. The SA determined that the company was not able to demonstrate how it complied with the GDPR's provisions concerning the legal basis for processing, which constituted a breach of the accountability principle.[16]
- The Italian SA imposed a fine of €30,000 for various violations, including failure to keep records of processing activities.[17]
- The Spanish SA imposed two fines of €50,000[18] and of €25,000[19] for failure to designate a DPO.
- The Belgian SA imposed a fine of €50,000 for failure to set up the DPO function in accordance with GDPR requirements.[20]

Compliance with the accountability principle does not prevent SAs from imposing fines for breach of other provisions of the GDPR.[21] However, SAs are likely to mitigate GDPR fines if an organisation keeps appropriate documentation, has strong privacy safeguards embedded in its products and services, and maintains clear privacy governance procedures.

Accountability and the one-stop shop mechanism

The accountability principle is a key part of the overall enforcement of the GDPR, especially in the context of the GDPR's one-stop shop mechanism (OSS). Under the OSS, a company's activities involving the processing of personal data across the European Union are subject to enforcement by the SA in the country where the company has its main EU establishment (e.g., the EU regional headquarters of a US multinational). That SA will be considered the 'Lead SA' and act as 'the sole interlocutor' of the

16 Greek SA, Decision 26/2019, summary available at https://edpb.europa.eu/sites/default/files/files/news/summary_of_decision_26_2019_en_2.pdf (last accessed 9 Feb. 2022).
17 Italian SA, Decision of 25 March 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9577323 (last accessed 9 Feb. 2022).
18 Spanish SA, Decision PS/00251/2020, available at https://www.aepd.es/es/documento/ps-00251-2020.pdf (last accessed 9 Feb. 2022).
19 Spanish SA, Decision PS/00417/2019, available at https://www.aepd.es/es/documento/ps-00417-2019.pdf (last accessed 9 Feb. 2022).
20 Belgian SA, Decision of 20 April 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf (last accessed 9 Feb. 2022).
21 WP29 Opinion 3/2010, para. 38.

company.[22] SAs often rely on the documentation kept to comply with accountability rules to determine which SA should be the Lead SA. For instance, SAs will check the location in which the DPO is based, or the office in which most policies and procedures relevant to privacy are adopted.[23] Companies should consider their approach towards the OSS when drafting their accountability documentation, to ensure that the documentation adequately reflects and justifies the company's approach.

Private enforcement: collective action lawsuits

The GDPR allows individuals and organisations to enforce the GDPR through the courts in EU Member States, using the accountability principle as a tool for litigation. The GDPR expressly grants individuals the 'right to an effective judicial remedy' before the courts of the Member State where the individual resides, in addition to any right to file complaints before SAs.[24] To facilitate the exercise of the right to an effective judicial remedy, the GDPR also allows non-profit organisations to submit complaints, including filing lawsuits in court, on behalf of multiple individuals.[25] The GDPR therefore provides for collective action lawsuits to be filed by non-profit organisations against companies.

Several private litigants (including collective action organisations) have argued that the accountability principle requires companies to proactively disclose information in court to demonstrate that the company is compliant with the GDPR. These litigants take the position that, under the accountability principle, individuals are not required to demonstrate that a company has breached the GDPR; rather that the company has to proactively demonstrate its compliance with the rules. The accountability principle, under this interpretation, reverses the burden of proof in court proceedings.

This approach has thus far been endorsed by courts only in a limited number of cases,[26] and it is not yet part of the case law of the European Court of Justice. In the cases where the accountability principle served to reverse the burden of proof, courts

22 GDPR, Article 56(6).

23 For instance, SAs will question a company's statement that their main EU establishment is in one country, if their data protection officer is located in another country and all the relevant policies governing data protection are drafted and adopted by employees based in another country.

24 GDPR, Article 79.

25 ibid., Article 80.

26 See, for instance, the judgment of Stuttgart Higher Regional Court in 'German court reverses GDPR burden of proof', *Global Data Review* (27 September 2021), at https://globaldatareview.com/data-privacy/german-court-reverses-gdpr-burden-of-proof (last accessed 9 Feb. 2022).

did not require plaintiffs to demonstrate that the defendant had breached the GDPR. Rather, they awarded damages to plaintiffs on the basis that the defendant companies had not been able to demonstrate that they complied with the GDPR. It is still unclear whether this will be the standard approach across the European Union. If so, this would constitute a significant change for litigants in continental Europe, where civil laws do not usually require defendants to disclose a vast amount of information, contrary to common law jurisdictions such as the United Kingdom or the United States, which have strict discovery rules.

Accountability in the United States

There is no uniform principle of accountability in the United States akin to the GDPR's Article 5(2). That is not to say that data controllers – in GDPR parlance – are unaccountable. On the contrary, companies are accountable to an overlapping patchwork of federal regulators, states and the data subjects themselves for proper handling of their data assets. The substantial accountability to each is discussed in the subsections below.

Accountability under EU and US law is not as different as it might first seem. Both jurisdictions leave much undefined. As described above, the broad and abstract language of the GDPR affords generous room for interpretation. Because the United States lacks any uniform legal code in this area, companies and data professionals have similarly improvised from the bottom up. As in the European Union, best practices are a surer lodestar of what companies may be held accountable for than any statute's text. More than a decade ago, leading academics explained that US privacy was governed far more by practices 'on the ground' than 'on the books'.[27] Little has changed in that regard. Although there have been perennial calls for unified data security and privacy legislation, none has emerged.[28] The result is an accretion of conventional wisdom endorsed by regulators or courts in the course of individual enforcement efforts.

---

27 Kenneth A Bamberger and Deirdre K Mulligan (2011), 'Privacy on the Books and on the Ground', *Stanford Law Review* 63: 247–315.

28 This article does not address the specialist statutes codifying liability for data protection failures in specific fields such as the Health Insurance Portability and Accountability Act for healthcare, Gramm Leach Bliley Act for financial services, and the Federal Information Security Management Act for federal agencies. Although those also incorporate reasonableness and other broad principles, they have considerably more detailed implementing regulations better suited for specialised review and have no applicability to entities outside their narrow spheres.

In the United States, 'reasonable' is a key term. For example, companies may represent in privacy policies or elsewhere that they 'take reasonable precautions and follow industry best practices' to ensure that data is not inappropriately 'lost, misused, accessed, disclosed, altered or destroyed'.[29] The US Federal Trade Commission (FTC) frequently holds companies accountable for failure to take reasonable measures, relying on industry practice to argue that their practice was unreasonable.[30] A growing number of state laws also require 'reasonable' measures to protect personal information independent of the company's representations. Under California law (a bellwether regime that applies broadly to many businesses that happen to serve California users), unreasonable practices are actionable by both the state attorney general and by individuals affected.[31] Such state laws generally do not define what is reasonable. Practitioners, regulators and enforcers have filled the void with case-by-case interpretations that become persuasive in future actions. There has thereby emerged a rough sense of which privacy and data security practices a company can be held accountable for to federal enforcers, state enforcers and individuals.

The federal government, through the FTC, has historically been the most active enforcer. But legal actions by state regulators and attorneys general also make up a substantial portion of enforcement activity, while actions by individuals through both traditional common law means and new state-level statutory grants of authority are common.[32] Unlike EU law, US law has no concept of a one-stop shop. Nor is there statutory federal pre-emption, generally. Thus, companies can be held accountable by each type of enforcer independently.

---

29 See, e.g., *Tapplock, Inc.*, File No. 1923011 (F.T.C. May 18, 2020) (complaint), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockcomplaint.pdf (last accessed 9 Feb. 2022).

30 See, e.g., *Tapplock, Inc.*, File No. 1923011 (F.T.C. May 18, 2020) (decision and order), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf (last accessed 9 Feb. 2022).

31 See Cal. Civ. Code § 1798.81.5 (requirement to implement and maintain reasonable security procedures, enforceable by the attorney general) and § 1798.150 (consumers may sue for breaches that result from unreasonable practices).

32 See, e.g., the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq.

Accountability to the US Federal Trade Commission

The FTC is the most prominent US enforcer of data protection practices. It holds companies accountable even though it has no express statutory grant of sweeping authority over data security and privacy.[33] Instead, the FTC usually relies on its broad authority to police 'unfair or deceptive acts or practices in or affecting commerce' granted in Section 5 of the FTC Act.[34] It can do so (1) through an administrative proceeding directly under Section 5 or (2) as a lawsuit in federal district court under Section 13 as an actual or imminent violation of a 'provision of law enforced by the Federal Trade Commission'.[35] Some academics have described the FTC's case-by-case elaboration of its authority as a 'common law of privacy',[36] but that view is not universal. Much of this 'common law' consists of consent orders that are the result of negotiated settlements between the FTC and companies, as opposed to a court's legal determination after an adversarial process. The FTC's 'deception' authority is generally the most straightforward: a company that makes a privacy or data security commitment must honour it. These commitments are often made in privacy policies or in statements required by regulators but can also take the form of voluntary assertions. The FTC's authority over 'unfair' privacy or data security practices is more nuanced. And courts themselves have not been consistent with respect to the scope of the FTC's authority in this area. But in practice, those court decisions have not slowed the FTC's enforcement efforts.

---

33 Although the Federal Trade Commission (FTC) does not have an express statutory grant to enforce data protection or privacy writ large, some statutes do grant specific authority over narrow areas, such as children's privacy under the Children's Online Privacy Protection Act. 15 U.S.C. § 6501 et seq. The FTC recently announced that it will be embarking on a privacy rulemaking; as a result, we may see more specific privacy requirements in the future.

34 15 U.S.C. § 45(a).

35 15 U.S.C. § 53(b). Until recently, the FTC could seek monetary damages under Section 13(b) that were not available under Section 5(b). However, the United States Supreme Court held in *AMG Capital Management, LLC v. FTC*, 141 S. Ct. 1341 (U.S. 2021), that monetary damages were not available under Section 13(b) either. Unless the US Congress expressly grants this authority under one of the statutory provisions, first-time violators may be able to escape monetary relief. See Christopher Olsen and Stephen Schultze, 'FTC Authority Under Siege: Monetary and Injunctive Relief at Risk in Courts as Congress Contemplates a Response', 1, *Antitrust Source* (April 2021).

36 See Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 *Columbia Law Review* 583 (2014).

The first important decision regarding FTC authority for data security accountability came in 2015 from the United States Court of Appeals for the Third Circuit. In *FTC v. Wyndham Worldwide Corporation*, the Court held that the FTC could proceed against Wyndham under its 'unfairness' authority for failure to encrypt customer information, to enforce strong passwords or to employ reasonable measures to detect and prevent unauthorised access, among other things.[37] Wyndham had suffered multiple security breaches and the FTC's list of alleged failures was long. The FTC argued that each of the specific failures was unfair under the terms of the statute. The Court noted that the FTC might also have the authority to pursue a claim that Wyndham had acted deceptively by violating its general promise to use commercially reasonable measures that, according to its privacy policy, included vague 'appropriate safeguards'. The Court ultimately concluded that Wyndham's alleged failures were plainly 'unfair' under the statute.[38] It also rejected Wyndham's argument that without notice of what specific practices were required, the company lacked fair notice of what it must do to comply with the statute.[39]

The second important decision appeared to cut the other way, although it did not directly conflict with *Wyndham*. In 2018, the United States Court of Appeals for the Eleventh Circuit held in *FTC v. LabMD* that an FTC order requiring the company to implement 'reasonable safeguards' was too vague to be enforceable under the statute.[40] The FTC's order, according to the court, 'command[ed] LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness'.[41] Commentators noted that if, according to the Eleventh Circuit, a court cannot determine what constitutes a reasonable data security or privacy regime for the purpose of enforcing an injunctive order, then a court should likewise be unable to determine whether a regime is reasonable from the perspective of the statute itself. But the *LabMD* decision did not cite the *Wyndham* decision and instead avoided addressing the issue, so there was no clear procedural path for the United States Supreme Court to resolve the apparent split between the Third and Eleventh circuits. For its part, the FTC revised its subsequent data security orders to add more specific requirements.[42]

---

37 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240–41 (3d Cir. 2015).

38 ibid., at 244–47.

39 ibid., at 255–59.

40 *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1237, 1241 (11th Cir. 2018).

41 ibid., at 1246.

42 https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance (last accessed 9 Feb. 2022).

The practical effect is that companies must assume that the FTC has broad authority to bring enforcement actions for allegedly unreasonable privacy or data security practices – whether directly under the statute's 'unfair or deceptive' prohibition, as violation of a privacy policy's 'reasonableness' promise, or as a violation of an existing order requiring 'reasonable' measures. Facebook experienced this dynamic in 2019 when the FTC alleged that the company had been giving third parties access to certain user data, contrary to the company's public statements and contrary to a 2012 consent order that required both specific safeguards and implementation of a 'comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information'.[43] The FTC's US$5 billion settlement, while subject to much debate, was at least a demonstration of the FTC's practical authority to hold companies accountable for maintaining 'reasonable' privacy and data security protections.

Zoom found itself in a similar position in November 2020 when the FTC alleged that the company deceptively failed to implement several encryption measures that it claimed existed.[44] Above and beyond the company's failure to live up to its express promises about encryption, the FTC alleged that the company's software unfairly 'circumvent[ed] a security and privacy safeguard' built into the Safari web browser. Notably, the FTC explicitly alleged that this unfair security and privacy practice harmed consumers and it identified no countervailing consumer benefit.[45]

The Sedona Conference, an influential collection of judges, practitioners and academics, has surveyed the standards that courts, regulators and practitioners might use to determine what constitutes reasonable data security.[46] The Sedona Conference authors first observed that *Wyndham* quoted the FTC's statutory authority to hold an act or practice unfair when it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'.[47] That formulation, the authors noted, is akin to the classic cost/benefit reasonableness test for tort liability

43 See *In re Facebook, Inc.*, Dkt. No. C-4365, 2012 FTC LEXIS 135, *9 (F.T.C, Jul. 27, 2012), *In re Facebook, Inc.*, 2020, Dkt. No. C-4365, FTC LEXIS 80, *16–19 (F.T.C., Apr. 27, 2020).

44 *In re Zoom Video Comm'cns, Inc.*, 2020 WL 6589816 (F.T.C., Nov. 9, 2020) (complaint).

45 ibid., at ¶ 38.

46 See The Sedona Conference, 'Commentary on a Reasonable Security Test', 22 *Sedona Conference Journal* 345 (2021).

47 ibid., at 376 (quoting *Wyndham*, 799 F.3d at 255–59).

articulated by Judge Learned Hand in *United States v. Carroll Towing Co*.[48] Further extending their common law analogy, the authors also highlighted the role of industry custom and cost/benefit calculations in determining whether an actionable products liability tort occurred. This way of defining reasonableness in the privacy and data security context likely resonates with common law practitioners. Absent a prescriptive statute, it may be the closest thing to a general legal standard that exists.

In practice, companies that wish to avoid being held accountable to the FTC must digest prior FTC cases and consent decrees, FTC guidance and industry standards to determine what measures to implement. For example, *Wyndham* highlighted encryption of stored data, network monitoring for malware, password complexity, proper use of firewalls and intrusion detection.[49] The initial 2012 Facebook consent order is an example of a privacy regime that the FTC considered appropriate for a large company that was a first-time violator: implementation of a comprehensive privacy programme with 'reasonable' safeguards, biennial assessment by an independent third party and reporting to the FTC, and changes tailored to the specific failure. The 2019/2020 Facebook consent order is an example of a privacy regime that the FTC considers reasonable for a recidivist: appointment of board-level privacy compliance officers, enhanced transparency measures, pre-launch product functionality privacy review, proactive breach reporting and a substantial monetary penalty.[50] The FTC also provides high-level guides for protecting personal information and implementing security protections.[51] Overviews such as the Sedona Conference commentary catalogue some of the most salient industry standards, including the Center for Internet Security Critical Survey Controls (CIS Controls)[52] and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).[53]

---

48 159 F.2d 169, 173 (2d Cir. 1947.

49 *Wyndham*, 799 F.3d at 258–59.

50 *In re Facebook, Inc*., 2020, Dkt. No. C-4365, FTC LEXIS 80, (F.T.C., Apr. 27, 2020).

51 FTC, 'Protecting Personal Information: A Guide for Business' (2016), at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FTC, 'Start with Security: A Guide for Business' (2015), at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (web pages last accessed 9 Feb. 2022).

52 Center for Internet Security, CIS Critical Security Controls, at https://www.cisecurity.org/controls/ (last accessed 9 Feb. 2022).

53 National Institute of Standards and Technology, Cybersecurity Framework, https://www.nist.gov/cyberframework (last accessed 9 Feb. 2022).

Accountability to the states

Many states have laws that give state regulators or the state authority to hold companies accountable for privacy and data protection. These laws are diverse but fall into two broad categories. The first type of law requires businesses to notify consumers or regulators (or both) of data breaches. The definition of 'breach' (or even whether the state's law uses the term 'breach') differs by state. Lawyers advising a company that has suffered a breach will typically first gather the facts about the nature of the breach and the population affected, then analyse those facts against a complex matrix of state laws. There are basic matrices published by the National Conference of State Legislatures and the International Association of Privacy Professionals.[54] The second type of law requires businesses to maintain reasonable privacy and data protection practices. These laws are even more diverse and range from specific privacy and security statutes with implementing regulations to general consumer protection statutes.

New York and California are good examples. Section 899-AA of the New York General Business Law governs breach notification, and Section 899-BB governs data security protections. Section 899-AA requires notification when defined 'private information' is breached, and lays out several factors that a business may consider when determining whether the information has been 'acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization' (i.e., breached). Section 899-BB requires 'reasonable safeguards to protect the security, confidentiality and integrity of the private information'. The provisions are enforceable by the state, and do not create a private right of action. Section 1798.82, and related sections, of the California Civil Code requires breach notification in a specific format and creates a private right of action for failure to notify. Section 1798.81.5 of the Code requires companies to 'implement and maintain reasonable security procedures' and is enforceable by the California Attorney General.

In 2016, California's then Attorney General, Kamala Harris, published a data breach report that included a series of recommendations. Like the FTC guides, these recommendations indicate what a state might consider to be reasonable privacy and data security protections. The Attorney General described 'reasonable security' as 'the

54 See National Conference of State Legislatures, 'Security Breach Notification Laws', https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; International Association of Privacy Professionals, 'State Data Breach Notification Chart', https://iapp.org/resources/article/state-data-breach-notification-chart/ (web pages last accessed 9 Feb. 2022).

standard of care for personal information'.[55] This first suggests that the CIS Controls are the baseline minimum standard of care.[56] The report also recommend multi-factor authentication,[57] encryption of data in transit[58] and fraud alerts.[59] The report concludes by acknowledging that state laws differ, but calls for increased efforts to harmonise state laws rather than pre-empting them through a uniform federal law.[60]

Notwithstanding the Attorney General's call for harmonisation, state laws have only become more diverse. California itself has been promulgating new statutes and regulations at a rapid pace, with much still unsettled in practice. The 2018 California Consumer Privacy Act added a host of new requirements, including Civil Code Section 1798.150, which gives consumers the right to sue directly for breaches arising from unreasonable security practices. The 2020 California Privacy Rights Act created a new state regulatory agency, the California Privacy Protection Agency, with rule-making authority and independent power to investigate and prosecute violations. Many of the details about what the Agency will do and how it will work remain to be determined before and after it becomes operational in 2023. The Act itself outlines seven high-level responsibilities of businesses that cover data collection, notice, deletion, correction and a requirement to 'take reasonable precautions to protect consumers' personal information from a security breach'.

Thus, the trend at the state level is to increase accountability to states by both promulgating more requirements and creating additional – and sometimes indeterminate frameworks – premised on what is 'reasonable'. Although the states may not be focused on harmonisation and the federal government may not pass unifying privacy and data security statutes in the foreseeable future, businesses that follow prior state enforcement actions, written guidance and generally accepted industry practice can best satisfy diverse state accountability standards.

55 Kamala D Harris, California Dep't of Justice, 'California Data Breach Report' (February 2016), *27, at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (last accessed 9 Feb. 2022).

56 ibid., at 30.

57 ibid., at 34.

58 ibid., at 36.

59 ibid., at 37.

60 ibid., at 38.

Accountability to data subjects in the United States

Data subjects may bring an action in the United States either as an individual or as a class. They may do so under express state causes of action or common law tort. Any privacy or data breach action of this sort is likely to face several early procedural and jurisdictional hurdles, including removal to federal court or remand to state court, class certification objections, attempts to consolidate via multi-district litigation and challenges to standing. There are few cases that have proceeded to the merits and defined the specific practices for which data subjects can hold companies accountable.

Individual and class suits typically require highly specialised plaintiffs' and defendants' lawyers. The myriad procedural and jurisdictional questions generally make them large and complex undertakings that are frequently structured as multistate class actions in federal court. Much of the dispute in these cases involves whether the action qualifies as a 'case or controversy' under the Article III of the US Constitution.[61] In a string of cases, the US Supreme Court has held that for data inaccuracies or disclosures to constitute a case or controversy, plaintiffs must plead an 'injury in fact' that is sufficiently specific to show that they were harmed or faced imminent harm.[62] This is a complex and fact-specific area of law. Most suits are either dismissed at or before a standing challenge; otherwise they generally survive and are settled.

The 2017 Equifax data breach provides a case study of all modes of US accountability operating simultaneously. Indeed, had the breach occurred after the GDPR came into effect, the company might have faced EU accountability as well. The plaintiffs' bar seized upon the opportunity to sue Equifax even before regulators became publicly involved. In typical fashion, many class actions were initiated nationwide, consolidated in multi-district litigation and challenged together in a motion to dismiss.[63] The plaintiffs' theories included negligence, violation of state consumer protection and fraud laws, and violation of state data breach notification laws.[64] All survived the motion to dismiss, at least in part.[65] Shortly thereafter, Equifax settled with the consumer class

61 U.S. Const. art. III, § 1, cl. 1.

62 See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2211–13 (2021).

63 *In re Equifax, Inc.*, 362 F. Supp. 3d 1295, 1308–11 (N.D. Ga. 2019). Somewhat uncharacteristically, Equifax did not contest standing. ibid., at n. 70.

64 ibid., at 1321–43.

65 ibid., at 1345.

for about US$380 million.[66] During the same period, the FTC, the federal Consumer Financial Protection Bureau and state attorneys general conducted their own investigations under their own authorities.[67] These culminated in a coordinated settlement for about US$575 million independent of the consumer class action.[68] Although few privacy and data security failures will garner as much attention as the Equifax data breach, the incident serves as a reminder that accountability in the United States can come from all enforcers at once.

66 See Order Granting Final Approval of Settlement, Certifying Settlement Class, and Awarding Attorney's Fees, Expenses and Service Awards, *In re: Equifax Inc. Customer Data Security Breach Litigation*, No. 1:17-md-02800-TWT (N.D. Ga. Jan. 13, 2020), ECF No. 956.

67 See 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach', FTC (Jul. 22, 2019), at https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related (last accessed 9 Feb. 2022).

68 id.

CÉDRIC BURTON
Wilson Sonsini Goodrich & Rosati

Cédric Burton is a leader in Wilson Sonsini's Brussels office, where he co-leads the firm's global privacy and cybersecurity practice and leads the EU data protection team. He assists clients of all sizes with regard to privacy and data protection, information technology, data security, advertising and marketing, and e-commerce laws.

Cédric has developed substantial experience in advising companies on all facets of global, European and Belgian privacy and data protection law. His privacy and data protection practice covers all sectors and includes a wide range of activities, such as defining global pan-European strategies for compliance, developing creative and practical advice on unsettled topics, such as online profiling and behavioural advertising, counselling clients on how to resolve or mitigate risks relating to conflicts between EU data protection law and foreign requirements, and representing clients in their dealings with the European Commission and other major regulatory bodies.

Cédric has authored many articles on privacy and data protection law and speaks regularly on data protection-related topics. Prior to Wilson Sonsini, he worked as a research fellow in privacy and data protection law at the Research Center on IT and Law (CRID) of the University of Namur (Belgium) and at the Center on Law and Information Policy at Fordham University (New York).

LAURA DE BOEL
Wilson Sonsini Goodrich & Rosati

Laura De Boel is a partner in the Brussels office of Wilson Sonsini Goodrich & Rosati. Her practice is focused on all aspects of European data protection law, including data breaches, international data transfers and online profiling. She has extensive experience in advising clients on pan-European data protection compliance across a range of sectors. She also assists clients in their dealings with privacy and data protection authorities, such as the Belgian Privacy Commission.

Laura has been quoted in leading industry and legal publications, including Bloomberg BNA. She is a native Dutch speaker and is fluent in English and French.

CHRISTOPHER N OLSEN
Wilson Sonsini Goodrich & Rosati

Christopher Olsen advises clients on all aspects of privacy and cybersecurity matters and represents companies under investigation by the Federal Trade Commission and state attorneys general. He has an established track record of success in resolving investigations without enforcement action and clients regularly seek his guidance when facing high-stakes regulatory scrutiny.

Chris is a former deputy director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC), where he directed the international work of the Division of Privacy and Identity Protection and acted as the agency's co-lead negotiator in discussions with the European Commission regarding improvements to and renewal of the US–EU Safe Harbor Framework.

Prior to joining the bureau director's office, Chris was the assistant director of the Division of Privacy and Identity Protection at the FTC. In this role, he managed a number of significant privacy and security enforcement actions, as well as several of the most important privacy initiatives in recent FTC history, including a seminal 2012 FTC report on consumer privacy that formulated important recommendations for businesses.

LYDIA B PARNES
Wilson Sonsini Goodrich & Rosati

Lydia Parnes is a partner in the Washington, DC, office of Wilson Sonsini Goodrich & Rosati, where she is co-leader of the firm's privacy and cybersecurity practice. She regularly represents companies in complex regulatory investigations and provides advice on complying with federal, state, and global privacy and data protection laws.

The former director of the Bureau of Consumer Protection (BCP) at the Federal Trade Commission (FTC), Lydia is a highly regarded privacy expert. As director of the BCP, Lydia oversaw privacy and data security enforcement efforts and the development of the FTC's approach to online advertising. She testified on numerous occasions on the benefits of a uniform nationwide data breach law and the risks of legislating in the technology area.

Lydia advises companies on how to navigate global privacy and data security requirements while pursuing their business goals. She helps them develop and implement comprehensive privacy compliance programmes and understand the nuances of regulation and self-regulation in the privacy arena. Lydia regularly represents clients before the FTC and other federal and state agencies.

Lydia is regularly recognised among the country's top privacy and data security attorneys in *Chambers USA*, *Chambers Global* and *Who's Who Legal: Business Lawyers*.

WILSON SONSINI

As the premier legal adviser to technology, life sciences and growth enterprises worldwide, Wilson Sonsini is at the forefront of privacy and cybersecurity law in the United States and throughout the world. Our cross-disciplinary team of highly experienced professionals helps companies navigate the complex and ever-changing set of laws, regulations and industry standards that govern the collection, storage and use of information.

Our privacy and cybersecurity team includes former senior officials who served in the Federal Trade Commission's Bureau of Consumer Protection, the US Department of Justice's National Security Division and the Department of Homeland Security. The team also includes some of the nation's leading litigators and veteran trial attorneys who have litigated complex data disputes involving novel issues of law. Rounding out the team are compliance and transactional attorneys, as well as legislative and regulatory strategists.

Rue Montoyer 47
Brussels, 1000
Belgium
Tel: +32 2 274 57 00

1700 K Street NW
Fifth Floor
Washington, DC 20006
United States
Tel: +1 202 973 8800

www.wsgr.com

Cédric Burton
cburton@wsgr.com

Laura De Boel
ldeboel@wsgr.com

Christopher N Olsen
colsen@wsgr.com

Lydia B Parnes
lparnes@wsgr.com

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

Cybersecurity Compliance

Burcu Tuzcu Ersin, Burcu Güray and Ceylan Necipoğlu[1]
Moroğlu Arseven

Introduction

During the past decade, the regulation of cybersecurity has become a very hot topic in the world as a result of an increase in the level of importance attributed to data and privacy as well as the digitalisation of services, including government services. As the value of information systems and the data they contain increase, the security of these information systems and data becomes more and more important. Also, with the use of the internet of things (also known as IoT) in homes and workplaces, the cost of cybersecurity events has become more concrete and visible. Therefore, efforts to draw up a legal framework to ensure an adequate level of security have accelerated.

Data breaches are costly. During 2021, the average cost of data breaches rose from US$3.86 million to US$4.24 million.[2] According to a report by Verizon,[3] the financial impact of 95 per cent of a business email compromise is between US$250,000 and US$984,855, that of a computer data breach is between US$148,000 and US$1,594,648, and that of a ransomware attack is between US$69,000 and US$1,155,775. These figures do not take account of legal costs, liabilities and secondary costs, and on top of that is the associated loss of reputation and trust. According to research, companies that suffered a data breach were underperforming on the NASDAQ stock exchange after six months.[4]

---

1 Burcu Tuzcu Ersin is a partner and Burcu Güray and Ceylan Necipoğlu are senior associates at Moroğlu Arseven.

2 IBM, Cost of a Data Breach Report 2021, available at https://www.ibm.com/uk-en/security/data-breach (last accessed 21 Feb. 2022).

3 Verizon, 2021 Data Breach Investigations Report, available at https://www.verizon.com/business/resources/reports/dbir/ (last accessed 21 Feb. 2022).

4 id.

Data breaches are also costly for data owners and data subjects. A data breach may lead to exposure of a person's private information. With the increase in the importance attributed to personal data, especially in the electronic environment created by the level of digitalisation and popularity of smart devices, there is now a new aspect of cybersecurity and the awareness for protection of data has entered a new phase. However, cybersecurity is not limited to protection of personal data, but has the purpose of protecting any data – or more accurately, the system and network as a whole.

In this article, we examine the general framework for data security in the European Union and the United States to gain a better understanding of the latest trends. Then, as a more specific example, the current outlook in Turkey is explained.

Regulating cybersecurity

In the European Union, Directive (EU) 2016/1148 (the NIS Directive)[5] was the first legal document setting out the regulation of cybersecurity across the Union. Being in the form of a directive, EU Member States have been able to adopt its requirements with a certain level of flexibility. Regulation (EU) 2019/881[6] was enacted to complement the NIS Directive to establish a framework for cybersecurity certification.

The NIS Directive requires Member States to ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks to the security of the network and information systems that they use in their operations. The term 'operator of essential services' is defined as a public or private entity carrying out business in the field of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, or digital infrastructure and that meet the following criteria:

- an entity providing a service that is essential for the maintenance of critical societal or economic activities;
- provision of the service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

5 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

6 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

The NIS Directive also requires Member States to adopt a national strategy on the security of network and information systems to define the strategic objectives and appropriate policy and regulatory measures.

As explained, the NIS Directive does not provide an EU-wide standard that applies to every and each entity, but instead requires the Member States to ensure the security of network and information systems in certain sectors by means of incident notification measures. A proposal presented to the European Commission on 16 December 2020 will repeal and replace the NIS Directive, and extends the scope to include new sectors such as telecommunications, social media platforms and public administration.

Most current legislation does not provide a sufficient standard for cybersecurity. To plug this gap, other frameworks and standards have been developed and published. In this respect, the European Union Agency for Cybersecurity (ENISA) has collaborated with the Standard Developing Organisations (namely ISO SC27, ETSI and CEN CENELEC).[7]

In the United States, there is no single legal document that determines a nationwide cybersecurity framework. However, the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999 and the Federal Information Security Management Act, which is part of the 2002 Homeland Security Act, are the main pieces of legislation that set out certain cybersecurity requirements.

Under Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, issued in February 2013, the National Institute of Standards and Technologies was assigned to develop a cybersecurity framework. Furthermore, the Cybersecurity and Infrastructure Security Agency has determined 16 critical infrastructure sectors that require an enhanced level of protection against cyberattacks, namely chemical, commercial facilities, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems.

In addition, in 2014, the Securities and Exchange Commission's Examination Priorities included a focus on technology controls and cybersecurity.

In Turkey, although cybersecurity is not an old concept, there is no specific law or regulation that governs cybersecurity standards. Nevertheless, since the enactment of the Personal Data Protection Law No. 6698 (the DP Law), cybersecurity has become an even more important concept for any data controller as data breaches can now

7 See https://www.enisa.europa.eu/topics/standards/standards (last accessed 21 Feb. 2022).

lead to administrative fines as well as civil and criminal liability. The Personal Data Protection Board (the Board) has published guidelines regarding technical security measures to be taken by all data controllers, but this is limited to the protection of personal data. The DP Law introduced a new aspect to cybersecurity, namely that it is not limited to the protection of personal data but also the information system and network, including the data within it.

The minimum cybersecurity measures to be undertaken by public institutions and certain key sectors, such as telecommunications and banking, are also determined by a series of circulars and guidelines. Furthermore, cybersecurity standards adopted by the Turkish Armed Forces comply with the standards required by the North Atlantic Treaty Organization. There are also specific regulations for the protection of data in regulated sectors, including banking and capital markets.

In recent years, the establishment of the Digital Transformation Office of the Presidency of the Republic of Turkey (DTO) and National Cyber Incidents Response Center (NCIRC) were big steps towards establishing a more solid foundation for cybersecurity across Turkey. Both the NCIRC and the DTO publish guidelines regarding information security measures.

Following the steps taken by the European Union regarding cybersecurity, Turkey's Information and Communication Technologies Authority has initiated efforts to prepare a draft code regarding cybersecurity-related matters. This draft is expected to echo the NIS Directive and Regulation (EU) 2019/881 and establish a national cybersecurity standard. Additional legislation was planned as part of Turkey's National Cybersecurity Strategy for 2013–2014[8] and 2016–2019,[9] but no drafts have yet been published. Similar plans were included in the National Cybersecurity Strategy and the 2015–2016 Action Plan, but no draft has yet been made public. However, it was mentioned verbally by the Information and Communication Technologies Authority that work on cybersecurity legislation had been carried out.

Regulating cybersecurity with regard to the protection of personal data

Cybersecurity is a concept of security of information systems and the information they contain, regardless of the types of data. That being said, personal data protection regulation has made cybersecurity an important aspect of data protection regimes. In

8 See https://www.btk.gov.tr/uploads/pages/2-0-1-cyber-security-strategy-and-action-plan-2013-2014-5a3412df707ab.pdf (last accessed 21 Feb. 2022).

9 See https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (in Turkish only) (last accessed 21 Feb. 2022).

most jurisdictions, including Turkey, the most severe data breaches have been caused by a lack of cybersecurity measures. The scope of data protection regulations is limited to the protection of personal data; but as they require an adequate level of cybersecurity, they can be a guide for cybersecurity in jurisdictions where no specific universal cybersecurity regulation is in place.

Article 24 of Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR)) requires data controllers to implement appropriate technical and organisational measures to ensure their processing complies with the GDPR. Moreover, pursuant to Article 32, taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of variations in likelihood and severity for the rights and freedom of natural persons, data controllers and data processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, among other things:

- the pseudonymisation and encryption of personal data;
- the ability to ensure continuing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to personal data in Turkey in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

Article 12 of Turkey's DP Law requires data controllers to take all necessary technical and administrative measures to provide a sufficient level of security to prevent unlawful processing, prevent unlawful access, and ensure the retention of personal data. However, the DP Law does not set out the minimum requirements for complying with this rule. The Turkish parliament, preferring to refrain from limiting the measures to be taken by data controllers, instead required data controllers to take all necessary measures to protect data, without any limitation.

Nevertheless, the Board has published a Guideline on Personal Data Security (Technical and Organisational Measures)[10] (the DP Guideline) to guide data controllers on technical measures for the protection of personal data.

10 See https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (in Turkish only) (last accessed 21 Feb. 2022).

In the United States, the California Consumer Privacy Act allows any consumer whose non-encrypted and non-redacted personal information is subject to unauthorised access and exfiltration, theft or disclosure as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect personal information, to institute a civil action for:

- recovery of damages in an amount not less than US$100 and not greater than US$750 per consumer per incident, or actual damages, whichever is greater;
- injunctive or declaratory relief; and
- any other relief the court deems proper.

In summary, personal data protection regimes require a certain level of protection for systems that contain personal data.

Cybersecurity for public offices and critical infrastructure

The protection of state information systems as well as critical infrastructure has been regarded as a matter of national security for a while now. In fact, protection of critical infrastructure has been the main reason why several jurisdictions have adopted cybersecurity regulations. For instance, the NIS Directive and Regulation (EU) 2019/881 establish the protection of critical infrastructure. However, they do not include any requirements for information systems that are not considered as critical.

Turkey has adopted a similar path and regulates certain cybersecurity requirements to which public entities and critical infrastructure operators must adhere. A Presidential Circular on Information and Communication Security Measures,[11] published in Official Gazette No. 30823 of 6 July 2019, governs security measures that should be taken by public institutions and operators providing critical infrastructure services so as to mitigate and eliminate the security risks faced in information systems and to secure the critical data that could jeopardise national security or cause destruction of public order when their privacy, integrity and accessibility have been compromised.

11 See https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures (last accessed 21 Feb. 2022).

Sector-specific cybersecurity regulations

Owing to the importance attributed to their data, there are specific regulations regarding cybersecurity within the banking, insurance, e-commerce, telecommunications and health sectors. Apart from being considered as critical infrastructure, in many jurisdictions specific regulations have been adopted to protect the integrity and continuity of the information systems.

In Turkey for instance, the Regulation on Information Systems of Banks and Electronic Banking Services, published in Official Gazette No. 31069 of 15 March 2021, which is fully effective as of 1 January 2021, is the main legal document governing banks' information systems.[12] This Regulation aims to regulate the minimum procedures and principles required as a basis for the management of information systems in the performance of banking activities, the provision of electronic banking services, and the management of the risks related thereto, and the information systems controls that must be established.

Electronic communications is another sector in which information systems are heavily regulated. In Turkey, the Regulation on Electronic Communication Infrastructure and Information System (the Infrastructure Regulation), the Network and Information Security Regulation in the Electronic Communications Industry (the Network Regulation) and Electronic Communication Law No. 5809 are the main pieces of legislation that govern the security of information systems of electronic communication institutions. The Infrastructure Regulation envisages the establishment of an Electronic Communication Infrastructure Information System in which the information regarding the infrastructure of operators within the electronic communication sector is recorded.

The Network Regulation regulates the procedures and principles to be followed by operators to ensure network and information security. The operators are obliged to establish an information system management system (ISMS), which is defined as all activities that are systematic, regulated, planned, manageable, sustainable, documented, accepted by the management of the operator, and based on international security standards (TS ISO/IEC 27001 or ISO/IEC 27001 standards), to ensure the confidentiality, integrity and accessibility of information. Operators must also implement an ISMS policy, an asset inventory and classification. The Network Regulation envisages certain security measures, including preparing risk management and evaluation,

12 See https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (in Turkish) (last accessed 21 Feb. 2022).

business continuity measures, management of information security breach and vulnerabilities, internal audits, employment, discipline procedures, physical access, protection against environmental threats, equipment security, electronic environment management, network security, separation of duties and environments, backing up, logging, user access management, password management, maintenance, and other measures.

The regime applicable to the health sector is relatively strict as regards processing of sensitive health data. The Regulation on Personal Health Data, Circular No. 2015/17 on Health Information Systems Applications and Information Security Policies Directive and Guideline are important legal documents that set out security measures to be adopted within the sector.

BURCU TUZCU ERSİN
Moroğlu Arseven

Burcu Tuzcu Ersin, LLM, leads Moroğlu Arseven's IT and telecommunications practice area. Within her IT and telecommunications work, Burcu focuses on mergers and acquisitions, venture capital, growth and start-up financing, data protection, privacy, e-commerce, cloud services, gaming, cybercrime and e-money issues. Her experience with complex compliance issues, anti-corruption and anti-money laundering matters means Burcu provides a full range of support to IT and telecommunications clients, often involving cross-border elements and multi-jurisdiction liability considerations.

Burcu is known for being a strong negotiator, as well as providing clients with clear, high-quality and concentrated legal advice within the rapidly developing and expanding Turkish IT and telecommunications market.

Burcu has experience in all segments of IT and telecommunications, including regulatory support, software development, mobile services (such as mobile platform development), web services, e-commerce and hardware manufacturing, as well as related financing and investment. She works closely with clients of all sizes and development stages, providing strategic guidance on the legal aspects of creating, acquiring, transferring, using and protecting technology.

She has a strong track record of guiding and training clients on the legal and practical aspects of the local IT and telecommunications sector. She is particularly active in venture capital, growth and start-up financing. A significant proportion of her time is spent assisting clients in related areas.

BURCU GÜRAY
Moroğlu Arseven

Burcu Güray is a senior member in the firm's fintech and IT teams, with particular expertise in local and EU data protection, e-commerce and internet services, digital assets, crowdfunding and compliance issues.

Burcu helps clients to deal with circumstances where commercial issues intersect with regulatory considerations and has particular experience assisting clients to deal with complicated compliance issues in Turkey. She supports clients with complicated regulatory compliance questions and programs, covering topics such as data protection and privacy, data security matters, capital markets instruments, crypto assets, insurance matters, corporate governance, anti-corruption and business crimes.

She advises clients on a large quantity of technology matters, including IT procurement, outsourcing, cloud and licensing. She also assists clients on financial services and products in the fintech sector and helps them to establish their market strategy by understanding their commercial needs and objectives.

CEYLAN NECİPOĞLU
Moroğlu Arseven

Dr Ceylan Necipoğlu, LLM, is a senior associate who specialises in IT law, particularly in e-commerce, internet law, fintech, emerging technologies, cryptocurrencies, privacy and data protection, cybersecurity, compliance and telecommunications law.

She assists clients in the establishment of their market strategies on complex ICT projects, and the drafting and negotiation of complex IT contracts, including outsourcing, licensing, procurement and service agreements.

She deals with businesses on the assessment and strategic management of their privacy, security, electronic workplace, and e-business legal risks both domestically and globally. She has been lecturing at universities as a guest lecturer and has articles published in international academic journals on subjects ranging from cybersecurity to fintech technologies.

Ceylan is a member of ITechLaw and the International Association of Privacy Professionals. She has been a mentor and adviser for a range of technology-related working group meetings organised by İtü Çekirdek and Work-Up. She is ranked as a global ambassador by WomanTech. She is also working for Maltepe University Technology and Intellectual Property Law Research Center as a research assistant.

MOROĞLU
ARSEVEN

Moroğlu Arseven is an independent full-service law firm established in 2000, with broadly demonstrated expertise and experience in business law. It has a dynamic and dedicated team of lawyers who are experts in their respective fields and who offer outstanding client service with the support of distinguished independent of counsels. The firm's primary guiding principles are universal and national ethical values, independence of legal practice and the indivisibility of legal science and legal practice. Moroğlu Arseven is known as a detail-oriented, well-connected, hands-on and focused law firm that is expert at handling complex tasks, whether these relate to transactions, disputes or settlements. Its clients include national, foreign and multinational commercial, industrial and financial enterprises, which it advises on complex issues and high-profile matters that require multidisciplinary legal support. The firm's primary goal in representing and advising clients is to provide and implement clear, applicable and pragmatic solutions that focus on each client's specific needs, transactions, legal questions or disputes. Its attorneys adopt a holistic approach to the broader legal and commercial situation and offer expertise in individual topics, while also collaborating with topic experts from other practices.

Harbiye Mahallesi
Abdi İpekçi Caddesi, No. 19/1
İç Kapı No. 11
Nişantaşı
Şişli
İstanbul 34367
Turkey
Tel: +90 212 377 47 00
www.morogluarseven.com

Burcu Tuzcu Ersin
btuzcu@morogluarseven.com

Burcu Güray
bguray@morogluarseven.com

Ceylan Necipoğlu
cnecipoglu@morogluarseven.com

Embedding Good Data Governance across the Business

Sarah Pearce and Ashley Webber[1]
Paul Hastings (Europe) LLP

As is identified in the title and elsewhere in this publication, data has become a critical asset of the majority of organisations operating in today's world – beyond simply data-rich or data-driven businesses. It is vital, therefore, that the data is well managed and protected, arguably in a more sophisticated way but at least to the level of protection given to other critical assets of a business.

What is data governance and why is it important?

The Collins dictionary defines 'governance' with respect to a company as 'the way in which it is managed'. 'Data governance' and 'privacy governance' and other similar broad terms are used frequently, and sometimes interchangeably, to describe an organisation's management or control of privacy, data protection and data security. From a practical perspective, this is most commonly achieved by way of a compliance programme. While themes emerge between approaches to data governance, several of which are discussed below, no one size fits all: governance models vary according to the size of the organisation in question, the processing activities it undertakes, its industry sector, and indeed the organisation's posture and risk appetite as regards data privacy and security.

Effective governance generally requires some form of structure and a set of rules, and this applies equally in the context of data management. This is most commonly achieved by way of processes, procedures and internal policy documents that are prepared in line with applicable laws and industry practice.

1 Sarah Pearce is a partner and Ashley Webber is an associate at Paul Hastings (Europe) LLP.

Good data governance is crucial in facilitating an organisation's compliance with applicable privacy and security laws. Indeed, in certain jurisdictions it is actually a legal requirement. However, with successful implementation, good data governance can provide much more than a simple compliance tool; it can allow organisations to make use of its data as an asset in an effective and efficient way that can, in turn, benefit the business and lead to valuable outcomes both operationally and financially. In short, embedding good data management practices and tools can enhance the value of data as a critical asset and, ultimately, the value of the business.

What good governance looks like and how it is achieved

Governance models vary and, consequently, what amounts to good governance also varies. There is no one defined set of requirements: certain styles or measures that work effectively for one organisation could, quite simply, be wrong for another. That said, there are common themes that flow through good governance models, certain of which we discuss in detail below. Organisations that are considered as demonstrating good governance have probably approached and applied to their organisation all the areas we discuss.

Plan of action

Before any steps are made towards implementing some form of governance structure, an organisation needs to develop a clear plan of action as to approach; this is paramount for success. Without a sound plan, gaps in good governance are inevitable and potential efficacy and efficiency gains will be missed.

A solid plan will include at least the following.

- *Goals*: The first question to be asked is: 'What do we as an organisation wish to achieve by undertaking this initiative?' The answer will be very different depending on the organisation asking it but all will generally be geared towards ensuring the data retains its value. Common goals include compliance with a new regulatory requirement or related guidance, expansion of the business into new sectors or jurisdictions, or increased, new or different processing activities. Some organisations tailor their goals for governance around compliance with a particular accreditation, for example, ISO 27001.[2]

2 ISO/IEC 27001:2013 (issued by the Information Organization for Standardization) specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.

- *Strategy*: The second question is: 'How do we as an organisation intend to achieve these goals?' The answer will again differ depending on the organisation asking it but strategies will very often include several of the topics discussed below. Time frame is also important here; it should be realistic, while also endeavouring to maintain momentum with the project because the time required to implement a governance programme is often underestimated.
- *Team*: The third question that should be asked is: 'Who will be suitable for helping us achieve these goals and implementing this strategy?' Note that at this stage, the team being established does not have to be the team who will manage the programme once implemented, and most likely will not be, in its entirety. For example, given the potential size of a project of this nature, having a project manager on the team can be very useful but a project manager is unlikely to be involved in the day-to-day governance matters once implemented. It is also very common for organisations to consult, or even rely on, third parties for assistance at this stage, such as external legal counsel. Further, the implementation of good governance will often require new additional resources, for example, a data protection officer (as discussed below) or a chief privacy officer.

One thing to note about preparing a plan in this context (and indeed any plan) is that it should always be adaptable to change. Many things could arise that directly affect the original plan. Privacy and security are areas that are particularly vulnerable to change, whether this is because of the release of new guidance or enforcement action taken by a regulator, so organisations should be prepared to adapt to such changes. Further, data governance as a concept and how it is implemented is also evolving with new methods or tools for governance emerging regularly. It is important, during all stages of a compliance programme, from the planning to implementation to maintenance, that the organisation be as agile and proactive as possible as opposed to rigid and reactive. Although the latter cannot always be avoided, a flexible, proactive approach generally puts the organisation in a stronger position to deal with potential curveballs that affect the plan or otherwise, such as the discovery of a large and previously unknown data processing activity, an unknown data set of significant value or a historic security incident.

Global programme and the GDPR

In recent years, the world of data privacy and security has seen a massive shift into focus with new laws and legal regimes being enacted globally. Arguably the most influential and far-reaching of these laws is Regulation (EU) 2016/679 (the General

Data Protection Regulation (GDPR)). The GDPR came into effect in May 2018 and overhauled privacy and security compliance globally. Although this publication is not intended to focus on the GDPR and its requirements, it is worth highlighting that the it has global reach, applying to any organisation located in the European Union processing personal data of an individual and to any organisation located outside the European Union processing personal data of an individual located in the European Union (subject to meeting certain criteria). As such, the GDPR is probably a fundamental core element to any good data governance programme and, in turn, any good data governance – seeking to ensure the protection of such a critical asset.

Since the GDPR came into effect, many other new laws have appeared, for example in Brazil, South Africa and in certain US states such as California, with many other countries either in the process of finalising draft laws or preparing to announce new laws. When analysing any of the new and emerging laws, it is evident that they have been inspired and influenced by the GDPR as they contain many of the same or similar principles and obligations. That said, no single piece of legislation globally has had as significant and far-reaching an effect, nor do any of the later laws require any higher level of compliance, as the GDPR. Therefore, it is generally recommended that any governance programme be built around and geared towards compliance with the GDPR. In this respect, compliance with the GDPR is often referred to as the 'gold standard' for privacy and security. To the extent that any new laws are enacted to which the organisation will be subject, it is recommended that the new law be compared against the GDPR to identify whether there are any nuances in the new law that may require actions or measures in addition to the existing governance programme to comply with those nuances. Certain requirements may be limited to local matters but others may need to be rolled out globally. From a compliance perspective, these requirements may include registration of an entity with a public register, appointment of a privacy- and security-focused role (e.g., similar to a data protection officer (DPO, as discussed further below), or the translation of a particular policy into the local language.

In addition to benchmarking governance against the GDPR, for an organisation's compliance programme to amount to good governance and to ensure sufficient protection is given to the valuable data, it is crucial that the programme be rolled out across the entire organisation, globally if applicable. The programme remains subject to any local law requirements, of course, but from a general principles perspective, policies and procedures should be applicable to all employees, and the reporting structure should take into account persons and teams located in offices that are not the organisation's headquarters or where, for example, the legal team are largely based. As noted above, the GDPR is considered the 'gold standard' of privacy and security compliance

and, therefore, by implementing a governance programme that is built on the GDPR globally, the organisation is prepared and in a better position should any new privacy laws or requirements be implemented. Global implementation also leads to be better understanding by personnel of the principles and requirements, and a stronger privacy and security culture across the organisation, which ultimately helps enhance the value of the data as one of its assets.

Mapping

One of the most time-consuming, but arguably most important, action items when implementing a governance programme is data mapping. This stage is sometimes overlooked, partly because it and its value are often misunderstood. Data mapping is a process that records or 'maps' details about an organisation's processing activities, including types of personal data, categories of individuals (e.g., employees, customers), locations of processing activities (both geographically and by team or business line), and purposes of the activities. This exercise should also track other key considerations, such as with whom the personal data is shared (whether this be with another team or business line within the same organisation or a third party), where data is stored and what security measures are in place to protect the data. A common approach, depending on the resources available, is to distribute an initial questionnaire to key stakeholders across the business that aims to capture, at a high level, information regarding a team's processing activities. Following this, those performing the mapping (whether internal or external advisers) will ordinarily analyse the initial findings and determine how to best delve deeper; this may involve live interviews or additional written requests (or both). The information is then gathered and documented in the organisation's chosen 'map': for some organisations, this is an Excel spreadsheet and may incorporate sophisticated PowerPoint diagrams; for others the information is collated by way of a purpose-built off-the-shelf piece of software.

Completing a comprehensive mapping exercise well will be critical to the success of global governance within an organisation as it can highlight key considerations that shape the governance programme. For example, it may identify countries or offices where higher risk or simply more processing is taking place, or laws to which the organisation is subject of which it was not previously aware. Such an exercise also helps identify gaps in knowledge and understanding of data privacy and security concepts across the organisation that can influence policies, procedures and training.

As noted, a data mapping exercise can be time-consuming, particularly if the organisation is a large global cooperation. It is often difficult in such instances to identify who is the best person (or persons) on the ground to assist with the process

and drive it forward. Given the time and complexity involved, this is often the stage at which implementation of a data governance programme falls down. However, from experience, governance will never be fully successful and reflective of an organisation's needs, including its legal obligations, if at least some mapping is not completed.

Establishing the team and identifying key stakeholders

As noted above, the team overseeing the implementation of a compliance programme and other measures around governance does not, and likely will not, be entirely the same team operationalising, managing and maintaining governance once implemented (the Privacy Team); however, there is likely to be some overlap. A task for the team overseeing the implementation of a compliance programme and other measures for governance is to determine the best model for the Privacy Team and, ultimately, to create the Privacy Team.

There are several ways to do this and points to consider when doing so:

- looking at existing privacy-related roles and seeking to structure and maintain governance around those roles (e.g., chief privacy officer, general counsel, compliance officer or privacy lawyers). This is common if said roles already take on a level of the governance responsibility without it having been expressly defined as governance, such as completing data protection impact assessments;
- whether any new roles are required, for example a DPO (see further discussion below) or whether additional personnel are required;
- where best in the organisation the Privacy Team should sit. A key question here is often whether it should form part of an existing team (e.g., legal, IT or compliance) or whether it should be a stand-alone team that supports and engages with other teams if and when required. This often depends on manpower and resources but, for instance, larger organisations are more likely to find that a stand-alone Privacy Team with fewer reporting lines is more effective;
- how best to structure the reporting lines both within the Privacy Team and outside. This will be partly driven by where it is determined the Privacy Team will sit; and
- whether there would be benefit in having Privacy Team members located in specific countries or jurisdictions, or whether the Team can be located in one or a small number of countries while relying on a local network of persons who have a sufficient understanding of privacy to allow them to assist the Privacy Team when needed. Considering the discussion above regarding benchmarking compliance against the GDPR, if an organisation is subject to the GDPR in a significant way (e.g., it has key employee or customer operations in the European Union), it would be useful to have one or more team members located there.

Once the structure has been determined, it is crucial to define the roles of the members and consider how they will influence governance, to ensure that it is embedded within the culture of the organisation. For example, one person's role may focus on security incidents whereas another may focus more on policy preparation. The Privacy Team is likely to be fairly well known in the organisation and, therefore, it is much more efficient and easier to manage requests from the business if there are clearly defined responsibilities.

After the Privacy Team has been established, it is important to identify key stakeholders across the organisation. In this respect, a stakeholder is person, or a team, who is not an expert in privacy but whose engagement will be pivotal to the success of the governance programme given their role, purpose or location. These persons or teams will probably be in areas such as IT, legal, HR, operations and product, but will depend largely on the nature of the organisation's business. The more data the organisation processes, the more stakeholders it is likely to have.

Data protection officer

Although the role and the idea of a DPO has existed for some time, it was given new weight and meaning by express provisions in the GDPR. A DPO is mandated in certain instances (e.g., where an organisation's activities involve large-scale systematic monitoring of personal data) and the appointed individual should be a person with expert knowledge of data protection law and practices whose role is mainly to assist the organisation to monitor internal compliance with the GDPR, including informing and advising the organisation and its personnel about its obligations with regard to privacy and security. The DPO should act independently to the extent possible to avoid being conflicted as the role is more focused on compliance than the commercial business. For example, a DPO should report to the highest management level of the organisation, probably the board, whereas members of the Privacy Team are likely to have more corporate reporting lines.

When determining whether a DPO should be appointed and have a role in governance, there are a few factors to consider, including the following:

- An organisation should first assess whether it is required by law to appoint a DPO. Although it is recommended to structure governance around GDPR requirements, note that if the organisation is not actually subject to the GDPR, appointing a DPO should not be considered. As an alternative, appointing a specialist with a different title but similar responsibilities could be useful to ensure good governance throughout the organisation.

- The role of a DPO is regulated by the GDPR so if an organisation appoints a DPO (as that role is defined in the GDPR), it is subject to the relevant obligations under the legislation.
- As noted above, the DPO should not be conflicted. Conflict is most likely to arise when the individual also performs a more commercial role, such as chief financial officer.

Even where not strictly required by data privacy laws or regulations, appointing a data protection specialist can be very useful within an organisation that is seeking to implement a compliance programme and protecting its data assets.

Policies and procedures

One of the most important tools, if not the most important, for implementing a compliance programme and embedding a cultural governance within an organisation is to have written policies and procedures. Policies and procedures can take many forms and cover many topics. It is for the organisation to determine what exactly should be documented and how, although it is worth highlighting that the GDPR does require the 'implementation of appropriate data protection policies' when seeking to demonstrate compliance, and other privacy laws have similar requirements. Common policies and procedures include the following:

- *Data protection*: This usually sets out the principles to which the organisation adheres in respect of data privacy (largely reflective of the GDPR or other applicable privacy and security law principles) and how it administers its compliance according to those principles;
- *Data breach or incident response*: The purpose of this document is explain to personnel what a security incident is, how to identify one and what to do if one has, or potentially has, occurred. Such a document may also go further and detail the internal process that will follow, such as the teams and persons involved in investigating, how reporting would be assessed, and so on, whereas some organisations opt to have this latter information in a policy only applicable to the teams and persons it governs;
- *Data subject rights*: The purpose of this document to explain what data subject rights are, how to identify when a person is making a request to exercise a right (this is particularly useful for a consumer-facing business), and what steps personnel should take if they receive a request. Such a document may also go further and detail the internal process that will follow once a request has been received, such as how to respond to the request (template responses are always helpful in this

respect), the time frames for responding, among other things, whereas some organisations opt to have this latter information in a policy only applicable to the teams and persons it governs; and

- *Document retention*: The purpose of this document is to explain when, why and how documents should be retained and deleted. This may also incorporate a retention schedule with specific periods for retaining documents; how detailed this is will depend on the nature of the organisation. When determining a retention period for any document or data type, several laws may have an impact, including local laws and market practice on the subject matter, such as a statute of limitations requirement for a contract.

These are fairly standard policies and procedures that are generally recommended at a very basic level and their existence is indicative of an organisation having good data hygiene, which is vital bearing in mind its value as a critical asset for most organisations currently, as previously described. However, there will are likely to be several other policies and procedures that are suitable and, indeed, advisable for the relevant organisation.

Privacy by design

Privacy by design is a principle that has been around for some time, and now forms part of an integral principle of many data privacy laws, including the GDPR. 'The 7 Foundational Principles'[3] is a leading guide in this respect, which is intended to apply to an organisation's entire ecosystem and highlights that to be able to enjoy the benefits of innovation, such as new technology, organisations must also ensure that the protection of data, including controlling data flows, is preserved. Privacy by design essentially requires organisations to put privacy and protection of personal data first. It requires organisations, at the time of determining the relevant processing activity and during the processing itself, to implement appropriate technical and organisational measures that are designed to implement data protection principles in an effective manner and integrate necessary safeguards that meet the requirements of applicable law and protect the rights of individuals.

3 Privacy by Design – The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices (Information and Privacy Commissioner of Ontario), at https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. See also the chapter on Privacy by Design in this guide.

As discussed previously, good governance should be proactive and not reactive. If an organisation deploys a policy of privacy by design such that it can identify potential privacy risks early and implement mitigating measures, it will be in a position to reduce the risk profile of the organisation and be in a significantly better position with regard to compliance generally.

Assessments

Several privacy laws require organisations to be active in assessing their own activities to identify and mitigate risks, or determine that a particular data processing activity should simply not be undertaken because the risks are too high.

Laws that include assessment requirements often either have a threshold for completing the assessment (e.g., type of processing activity) or they are optional. That said, when an organisation is about to begin a new processing activity, such as launching a new product or implementing a new security measure, the completion of such an assessment remains good practice, even where the threshold is not met or its completion is not otherwise compulsory. From a governance perspective, assessments should be undertaken, of course, when required by law but completing them when not required is also good practice and should be encouraged when there is a potential risk to data, security and individuals, such as in the collection of sensitive personal data. It can be the case that risks will not be clear on the face of it and that an assessment actually helps to highlight them. Alternatively, an assessment is a way to assess a potential or known risk, to weigh up the pros and cons, and to determine whether the risk can be mitigated sufficiently.

As with privacy by design, assessments of this nature allow organisations to be proactive rather than reactive when it comes to assessing and preventing harm to privacy and security. Documented assessments are also a great compliance tool in that they can easily demonstrate an organisation's commitment to privacy and security, should a third party (e.g., customer) or indeed a regulator request it.

How good governance is maintained

We have discussed ways in which good governance can be implemented and demonstrated; the next hurdle, and often one that organisations neglect, is maintaining it – and maintaining it to a consistent standard, reflective of the value and level of criticality of the data in question for the organisation. Below are some common examples of how organisations can ensure good data governance be truly embedded and maintained.

Operationalise the programme

Operationalisation of any programme, particularly one that involves new policies and procedures, is vital to its success. This may seem obvious but it is surprising how many organisations put significant hours of work and resource into preparing a compliance programme that is then placed in a drawer and left untouched and forgotten. Others will only operationalise to a degree, resulting in an inconsistent approach across the organisation. These failures could be for several reasons, such as lack of senior leadership buy-in or approval, lack of appropriate communication channels to spread the word, or the organisation is not receptive to change.

So how does an organisation ensure this does not happen? There are many ways in which an organisation can operationalise a compliance programme, including:

- ensuring from an early stage that senior leadership and key stakeholders are on board with the programme and are willing to support and discuss it when the time comes. Referring back to the discussion above regarding developing the Privacy Team, the clearer the structure and the reporting lines, the easier this task will be and the more support the programme will be given;
- getting approval to send organisation-wide communications about the programme, or at least relevant policies and procedures, and deploying technologies to administer where appropriate or necessary;
- identifying appropriate communication channels at an early stage. This will begin the process of increasing awareness, which is vital to the success of the programme. If mass communication is not appropriate or not an option, there should be an appropriate and effective way to spread the message about the programme and any new policies and procedures;
- launching a central privacy repository of documents and information, possibly in the form of a portal, which is a great way to ensure all personnel can access the documents and information relevant to them easily; and
- audit, or threaten to audit, employees' compliance with policies and procedures. Depending on the nature of the relevant employee's violation, consider disciplinary recourse or other remediation actions, such as additional training.

Training

Training employees at all levels on governance is of the utmost importance to the success of a compliance programme as it will assist in truly embedding privacy and security governance into the culture of the organisation; providing employees with

clear examples and situations they can relate to is often a very successful way of achieving this. When considering what training to provide and how, an organisation should consider the following:

- Structure the training programme so that it is continual and not just undertaken at the beginning of an employee's enrolment with the organisation.
- Tailor training to specific roles and levels within the organisation. For example, any employees involved in investigating and handling security breaches should be trained in this area. Key stakeholders should also be given more advanced and additional training if they are to effectively assist the Privacy Team, as discussed above.
- As new policies and procedures are introduced, consider which areas of the business require specific training and which can be provided with a written overview.

Vigilance

In line with the theme of being proactive and not reactive, privacy and security laws and related guidance are evolving with speed and we expect to see multiple new and updated laws and related guidance appearing globally during the coming months and years. Although compliance with the GDPR will position an organisation well to tackle new and emerging laws and guidance, it does not necessarily amount to absolute compliance with each and every one. The Privacy Team or lead data specialist within an organisation needs to remain alert and vigilant to the introduction of new laws and guidance and proactively seek to identify potential gaps in advance of them coming into effect.

Monitor and learn

Good data governance should be seen as a living programme, and not simply a compliance programme that is implemented and left to run on its own. It needs to be regularly monitored and analysed to see where it is working, and where it is not. For example, organisations should diarise the provision of regular updates to employees on governance, by way of a newsletter for example, undertake regular audits, and seek feedback from employees to see if policies and procedures can be improved, as they will be the ones using them regularly.

Further, another source of learning comes from any incidents suffered by the organisation. Although not something an organisation wishes to suffer, it does assist with identifying compliance and operational gaps, provided lessons are learnt. Mock incidents, also referred to as 'table-top exercises', are also a fairly common tool for assessing how an organisation would respond to an incident; these can be undertaken however best suits the organisation, for example, by a team or an entire organisation

– or perhaps even both. At the very least, those responsible for privacy and security should be well versed in how to handle an incident in a rapidly responsive manner, allowing for regulatory notification requirements where appropriate.

Conclusion

There is no perfect model of data governance, nor is there a perfect method for embedding a good culture of governance within an organisation. That said, we have outlined several key features that can be useful in developing a successful and sustainable compliance programme and achieving recognisably good governance models. As explained earlier, the implementation and maintenance of a good governance model is highly advisable for any organisation that processes data or is affected in some way by data privacy and security issues, which, in today's world, is almost all organisations. Where that data represents a critical asset – as it does for many organisations at the current time – it will be vital.

With this in mind, and the fact that data privacy and security has shifted into focus on a global scale of late, a culture of good governance is something all organisations should be working towards: not only can it assist in demonstrating compliance with applicable data privacy and security laws but it can also help to foster safer and more effective data processing, which, in turn can, help to drive efficiencies and, ultimately, the success of the business.

SARAH PEARCE
Paul Hastings (Europe) LLP

Sarah Pearce is a partner in the privacy and cybersecurity practice of Paul Hastings and heads our UK/EU team from the firm's London and Paris offices.

Ms Pearce's practice covers data privacy and security issues in the United Kingdom and across Europe, including the impact of Brexit and the aftermath of the United Kingdom leaving the European Union. She assists clients in identifying, evaluating and managing global privacy and information security risks and compliance issues and regularly navigates clients through data breach response and associated regulatory investigations and enforcement proceedings. Her experience includes conducting privacy impact assessments and advising on risk management associated with data collection and use, international data transfer and marketing issues together with the drafting of privacy notices, policies, standards and processes. Ms Pearce routinely advises on the privacy and data security provisions of complex commercial and technology-related contracts, as well as those arising in the context of corporate transactions.

While her focus is data privacy, security and information management matters, Ms Pearce has a background in technology transactions and her practice encompasses a broad range of commercial and IT/IP issues, including supply, distribution, licensing and outsourcing arrangements, consumer rights and e-commerce-related matters.

ASHLEY WEBBER
Paul Hastings (Europe) LLP

Ashley Webber is an associate in the privacy and cybersecurity practice of Paul Hastings and is based in the firm's London office.

Ms Webber assists clients in managing global privacy compliance projects, identifying and evaluating information security risks, and assists clients in handling data breach responses. Her experience includes advising on the use of data, international data transfers and marketing issues together with the drafting of privacy notices, policies, standards and processes. In addition, Ms Webber advises clients on the privacy and cybersecurity provisions of commercial and technology-related contracts while also assisting them with the privacy and cybersecurity issues in corporate transactions.

Ms Webber also has experience in advising on wider commercial contracts, including technology contracts, and in doing so routinely advises on a range of commercial and IT/IP issues, including supply, distribution, licensing and outsourcing arrangements, and consumer rights.

PAUL HASTINGS

In today's world of transformative change, our purpose is clear – to help our clients and people navigate new paths to growth.

Founded in 1951, Paul Hastings has grown strategically to anticipate and respond to our clients' needs in markets across the globe. Our innovative approach and unmatched client service has helped guide our journey to becoming one of the world's leading global law firms in such a short time.

We have a strong presence throughout Europe, Asia, Latin America and the United States. We offer a complete portfolio of services to support our clients' complex, often mission-critical needs – from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

Our data privacy and cybersecurity practice brings together industry chief counsels, privacy officers, former government officials, and regulatory and consulting experts who are skilled in solving today's emerging privacy and security challenges. Our legal guidance and recommendations are based on our real-world experiences of working closely with clients to advise and implement actual solutions that are grounded in a deep understanding of global privacy, cybersecurity and data protection laws.

32, rue Monceau
Paris 75008
France
Tel: +33 1 42 99 04 50

100 Bishopsgate
London, EC2N 4AG
United Kingdom
Tel: +44 20 3023 5100

www.paulhastings.com

Sarah Pearce
sarahpearce@paulhastings.com

Ashley Webber
ashleywebber@paulhastings.com

Threat Awareness: The Spectre of Ransomware

René Holt[1]
ESET

Introduction

Twenty-first-century businesses rely on data to run their operations; data is their lifeblood and any interference can be deadly – a risk identified by criminals.

The task of defending information technology (IT) networks, therefore, is all about the data moving across them; inactive data is a risk or potential threat at worst. The challenge when data is moving is knowing what it is doing.

Ideally a company would want to know what happens to every piece of data in transit on its network and set rules about its use. However, this is a potentially technically challenging solution and an inflexible method requiring significant amounts of data storage.

Furthermore, such a system would present serious problems for the move to home working popularised by the covid-19 pandemic because it would mean that each device would need to authenticate via insecure, public networks to access a corporate network. The virtual private network (VPN) method that most companies currently use to achieve this is designed for flexibility, which means that it is open to all internet protocol addresses, apart from those that are blacklisted.

1 René Holt is a security writer at ESET. The author acknowledges that the main source of the information in this chapter is a white paper, updated by ESET Security Awareness Specialist Ondrej Kubovič in August 2021, that includes contributions by Stephen Cobb, former senior security researcher at ESET, and current ESET colleagues Research Fellow Bruce P Burrell and Chief Security Evangelist Tony Anscombe. See https://www.welivesecurity.com/wp-content/uploads/2021/08/ransomware_paper.pdf (last accessed 10 Mar. 2022).

The freedom this gives to employees reflects the risks to data from a potential attacker. Data can be stolen, it can be put out of reach or it can be destroyed. This means each organisation must decide several security issues, such as the perceived value of data, the capability of tracking its movement and the balance that can be struck between the employees' freedom and the threats to that data.

There are a number of cybercrime threats to data, ranging from data breaches that focus on the theft of passwords, usernames and financial information to threats to networks, such as distributed denial of service attacks (DDoS), which attempt to overload a network or computer (in most cases, a web server hosting a website) with automated junk traffic to make it unavailable for its intended users for a certain period.

The most reported form of attack is ransomware, which has refined most cybercrime techniques and has become the most effective method of making money using modern developments in technology. Ransomware relies on an attacker gaining access to a company network, encrypting the data on it and denying the company access to either data or devices unless a ransom is paid.

Although not a new threat – in the 1990s there were several cases of disgruntled employees encrypting data and demanding ransoms for access – the advent of cryptocurrencies and the internet have generated a huge increase in the activity. In the 20th century, the ransom had to be picked up either in cash or by bank transfer, which left the extortioner very vulnerable to arrest. That risk no longer exists.

As a result, the sheer scale of the attacks is forcing businesses to factor a response to a ransomware attack into their business models, which could expose a business to legal issues over whether to pay.

What is even more problematic is that, often, even if a ransom is paid, a company may not regain access to all its data.

Another factor is that the payment of a ransom not only confirms to the criminals that their crime pays, it also has reputational issues: first, regarding the business's cybersecurity and second, regarding the future integrity of the business's data.

A final factor is the legality of payment as cybercriminals are often either sanctioned or operating from sanctioned states.

This issue received stark emphasis in November 2021 from the US Department of Treasury's Office of Foreign Asset Control (OFAC), which updated the Sanction List with a number of cryptocurrency wallets specifically concerning individuals associated with cybercrime, who were the alleged perpetrators of ransomware attacks. The update also included for the second time a crypto exchange known as Chatex, which is suspected of facilitating financial transactions for hackers.

The regulatory landscape has also changed. The US Federal Deposit Insurance Corporation, a US regulator of the financial industry, announced on 18 November 2021[2] that banking organisations will be required, from 1 April 2022, to report computer security incidents within 36 hours. The new regulations, which other industry sectors are likely to adopt, mean that organisations will find it more difficult to hide an incident.

The Ransomware Disclosure Act proposed by Senators Elizabeth Warren and Deborah Ross[3] is likely to make payment even more problematic. The Act, if passed, will require companies that are the victims of ransomware attacks to report ransom payment information to the Department of Homeland Security, which will provide the US government with critical data on cybercrime activity. It may also have the effect of reducing a company's or its insurer's willingness to pay, knowing that they may face government scrutiny when they disclose the payment, which is likely to include how payment was made, how much was paid and to whom. Similar legislation is being proposed in other parts of the world, such as Australia.[4]

So, perhaps a business's first step in developing a response should be to seek legal advice regarding a ransomware insurance policy.

Ransomware is big business

Although no exact figures exist for the annual criminal proceeds of ransomware, the activities of law enforcement in arresting gang members and recovering stolen funds do give an indication of the scale of the activity. This policing activity has led to seizures of millions of dollars in cash and expensive assets, as well as the freezing of criminal cryptocurrency accounts.

2 https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html (last accessed 8 Mar. 2022).

3 https://www.warren.senate.gov/newsroom/press-releases/warren-and-ross-introduce-bill-to-require-disclosures-of-ransomware-payments (last accessed 8 Mar. 2022).

4 'New Australian bill would force companies to disclose ransomware payments', The Record (21 Jun. 2021), https://therecord.media/new-australian-bill-would-force-companies-to-disclose-ransomware-payments/ (last accessed 8 Mar. 2022).

To gain an insight into the scale of the issue, in one notable event on 14 January 2022, Russian Federal Security Service (FSB) agents arrested 14 members of one of the most notorious ransomware gangs – Sodinokibi (aka REvil)[5] – and confiscated US$6.6 million worth of cash assets, 20 luxury cars and a parcel of cryptocurrency wallets used to run its affiliate business.

Before the Russian raid, law enforcement agencies had already arrested seven affiliates of the gang, and even recovered US$6.1 million from another affiliate still at large.

In a business model often used in computer crime, the Sodinokibi gang runs ransomware-as-a-service (RaaS) affiliate operations, and takes a cut of 30 to 40 per cent from ransom payouts made to their affiliates around the world.

According to the US Department of Justice,[6] in November 2021, the Sodinokibi ransomware operation collected more than US$200 million in ransom payouts and encrypted no fewer than 175,000 computers.

The impact of ransomware on global business and its data has been severe. This trend has been reflected in media headlines, most notably the 2021 attack on the US company Colonial Pipeline.[7] This incident resulted in petrol shortages because of panic buying of fuel and a US$4.4 million ransom demand.

An idea of the scale of the problem can be gauged from analysis carried out by the European Union's cybersecurity agency ENISA, which in 2019 put the cost of ransomware payouts at €10 billion, and the US Financial Crimes Enforcement Network, which, in the first part of 2021, estimated bitcoin payments it associated with ransomware to be in the region of US$5.2 billion.

These figures also mask one other often overlooked factor, which is that the success of ransomware is only possible because of the criticality of data to run modern businesses. Lose access to your data and you lose your business.

---

5 'Russia arrests REvil ransomware gang members, seize $6.6 million', Bleeping Computer (14 Jan. 2022)), https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/ (last accessed 8 Mar. 2022).

6 'DOJ charges 2 men allegedly behind REvil ransomware attacks', ABC News (8 No. 2021), https://abcnews.go.com/Politics/doj-charges-men-men-allegedly-revil-ransomware-attacks/story?id=81037690 (last accessed 8 Mar. 2022).

7 https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (last accessed 8 Mar. 2022).

The psychological pressure ransomware generates for critical data

Ransomware generates huge psychological pressure because organisations are conscious of potential reputational damage, service outages and legal and financial penalties, to which is added the obvious knowledge of losing control of core data. It is a mark of the importance of critical data that the ransomware trend has reached such levels as its specific purpose is to take advantage of how dependent businesses are on their computer networks.

In November 2019, the Maze ransomware gang started a trend called doxing (taking valuable or sensitive data from victims' systems before encrypting it). The gang then threatens to either publicly release the data or sell it to other malicious actors unless they are paid an additional fee on top of the ransom – a type of double extortion.

To increase the pressure still further on their victims, some ransomware operators take the step of directly contacting business partners or customers of victim organisations that have not paid a ransom demand. They will imply that sensitive data has been accessed in the attack and suggest that the business partners or customers also put pressure on the victim organisation to pay the ransom, or even demand payment directly from the business partners or customers.[8]

What is also particularly interesting about the crime trend is the acute awareness that criminals have developed regarding the value and use of information in the internet age.

In a final brazen twist, they have begun to offer insider information to short the stock of publicly traded companies in tandem with a public announcement of a ransomware attack. The DarkSide ransomware gang used this technique in April 2021[9] when it released a notice on its dark web portal offering information about companies listed on NASDAQ and other stock exchanges that had fallen victim to the gang. The group's ruse was that the combination of bad publicity, a dip in stock prices and the sale of insider information might put pressure on some companies to pay the ransom.

Gangs have homed in on market pressure in the wake of Verizon's 2017 acquisition of Yahoo. Following news of two data breaches, Verizon reduced its original offer for Yahoo by US$350 million, which was noted by the cyber gangs. This was a development

8 'Ransomware gang urges victims' customers to demand a ransom payment', Bleeping Computer (26 Mar. 2022), https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/ (last accessed 8 Mar. 2022).

9 'Ransomware gang wants to short the stock price of their victims', The Record (22 Apr. 2022)), https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/ (last accessed 8 Mar. 2022).

the US Federal Bureau of Investigation (FBI) highlighted in November 2021[10] when it released a private industry notification warning that ransomware actors now coordinate their attacks with current mergers and acquisitions to maximise extortion bids.

Acutely conscious of the value of the data it is denying to the company, the gangs' modus operandi is usually to keep ratcheting up the pressure with a range of other attacks. Furthermore, if victims refuse to pay, ransomware gangs will often threaten multiple follow-up disruptions. These range from DDoS attacks on victims' websites[11] to personal threats against company executives[12] using data found on their devices.

Sometimes, the criminals advertise their presence on a network using shock tactics such as print bombing, in which multiple printers on a network are commanded to print a ransom note – threatening management's ability to control internal and external communication about an incident.[13] Some gangs have also taken to cold calling executives using data on companies' databases to further increase the sense of being under siege.

In a 2020 attack, the Ragnar Locker ransomware gang even used funds from a US man's hacked Facebook account to run a Facebook Ads campaign[14] against Campari, in a bid to coerce it to pay for a ransomware attack. The campaign failed when Facebook detected the advertisements and quickly capped the campaign spend at US$35.

Preamble to a ransomware attack and other threats to data

A corporate ransomware attack is typically preceded by a two-stage preparation process that begins with initial access and is followed by reconnaissance, possibly accompanied by the theft of data.

---

10 'Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims', Federal Bureau of Investigation (1 Nov. 2021), https://www.ic3.gov/Media/News/2021/211101.pdf (last accessed 8 Mar. 2022).

11 'Another ransomware now uses DDoS attacks to force victims to pay', Bleeping Computer (24 Jan. 2021), https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/ (last accessed 8 Mar. 2022).

12 'Some ransomware gangs are going after top execs to pressure companies into paying', ZDNet (9 Jan. 2021), https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/ (last accessed 8 Mar. 2022).

13 This is highlighted by ESET in its 2020 Q4 Threat Report, at https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf (last accessed 8 Mar. 2022).

14 'Ransomware Group Turns to Facebook Ads', Krebs on Security (10 Nov. 2020), https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/ (last accessed 8 Mar. 2022).

Typically, ransomware operators rely on access brokers who specialise in gaining initial access to a network. To gain entry, these attackers probe networks for insecure system configurations, especially in remote access software tools such as remote desktop protocol (RDP, a tool that allows a device to be accessed via a network), or look for vulnerable software to exploit. Other lines of attack involve spearphishing (i.e., targeting individuals with an email they are likely to reply to because it appears to come from someone they trust) or bulk phishing emails. Both types of email contain malicious attachments or links that aim to trick unwary recipients into unwittingly giving up their credentials or allowing malware to be downloaded and installed.

For these access brokers, often hired via the dark net, the coronavirus pandemic was a godsend because of the number of office employees forced to work from home who suddenly became dependent on remote access tools. As a result, RDP became an essential requirement for people working from home. It works both ways, also enabling support staff to remotely manage employees' machines.

Unfortunately, RDP can be a significant risk, and to expose it to the internet – especially at scale – is a decision that should not be taken without some thought.[15]

Although gaining access from the internet to devices running RDP may require more effort than ransomware delivered via other channels, such as email, RDP does offer attackers significant benefits, such as misuse of legitimate access, the potential to evade protections and the ability to compromise multiple systems, or whole networks within a single organisation, especially if attackers successfully elevate their privileges to 'admin' or compromise an administrator's machine. Since RDP is a legitimate service – unlike malware – attacks via RDP can also fly under the radar of many detection methods, meaning fewer records and less threat awareness.

Full-on search for vulnerabilities

The quest for vulnerable companies by access brokers is relentless. Once one avenue has been exhausted, they switch to another, taking advantage of unpatched vulnerabilities in legitimate system software both to gain initial access and, once inside, to extend access to additional connected systems. It is a process like that used in the

15 Data collected by ESET security products deployed around the world shows that attackers have been making billions of attempts to brute force RDP logins by guessing passwords and usernames. The data revealed 29 billion malicious password guesses in 2020 alone. This number exploded in 2021, closing the year with 288 billion attacks, an almost tenfold increase in absolute numbers (897 per cent increase year-on-year).

animal world by predators on herds – they search for weaknesses and the target is pursued because of its weakness. It is only afterwards, once identified, that it is examined for its potential exploitation value.

Another method of attack used as part of this pattern of victim identification is the use of 'zero days'. A vulnerability is a mistake in the coding of some software of which a cyber criminal can take advantage to conduct an attack. A zero-day vulnerability occurs when there is no yet a patch in place to mitigate it, there being 'zero days' since a patch has been made available to the public. Discovering zero-day vulnerabilities can be an expensive process that generally involves well-funded and sophisticated threat actors such as advanced persistent threat (APT) groups and nation state-sponsored actors.

In one example in March 2021, a spate of attacks occurred when Microsoft rushed out emergency updates to address a chain of four 'zero-day' flaws – subsequently named ProxyLogon[16] – that affected versions of Microsoft Exchange, a server software used by organisations to deliver email via Outlook.

The speed and scale of the attack on Exchange servers around the world by more than 10 APT groups was striking. Companies that were too slow to patch or had not protected their systems sufficiently saw threat actors accessing their Exchange servers and attempting to steal email, download data and compromise machines with stealth malware to obtain long-term access to their networks.[17]

When coupled with ransomware, the automated exploitation of a vulnerability can become devastating. One of the best examples of this was WannaCry ransomware,[18] one of whose victims was the United Kingdom National Health Service in 2017. That attack came about because of the misuse of a high-severity vulnerability in Microsoft's Server Message Block (SMB) protocol, which is used for file and printer sharing in

16 'Exchange servers under siege from at least 10 APT groups', We Live Security (10 Mar. 2021), https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/ (last accessed 8 Mar. 2022).

17 ESET's detection data for 2021 showed the ProxyLogon vulnerability chain to be the second most frequently used attack avenue, at 14 per cent, beaten only by password guessing at 47 per cent.

18 'WannaCryptor remains a global threat three years on', We Live Security (12 May 2020), https://www.welivesecurity.com/2020/05/12/wannacryptor-remains-global-threat-three-years-on/ (last accessed 8 Mar. 2022).

large company networks. Despite patches having been available for two months before the WannaCry outbreak on 12 May 2017, attackers still found and encrypted more than 200,000 vulnerable machines.[19]

That ransomware gangs do their homework is obvious as is their attention to detail, aware that some companies have managed to avoid paying them by backing up their data. It is therefore not surprising that the network-attached storage (NAS) devices commonly used to share files and make backups have also attracted their attention. This was confirmed in 2021, when the NAS appliance maker QNAP alerted its customers that a ransomware called eCh0raix was attacking its NAS devices, most successfully with those with weak passwords.[20]

In January 2022, the DeadBolt group kicked off a ransomware campaign targeting internet-connected QNAP NAS devices. The attackers claimed to be exploiting a zero-day vulnerability that they would disclose to QNAP in return for US$1.85 million.

If such a device is connected to the internet and vulnerable, the best advice is to disconnect it right away. Considering that NAS devices are commonly used to store backups that can help organisations recover from a ransomware attack, this can be a particularly damaging type of attack.

As mentioned earlier, many criminals still use email attachments to deliver the malign code that installs ransomware. The attachments will either deliver downloaders that install malware on the email recipient's machine or establish a foothold on a machine within an organisation's network.

Email is one of the primary routes for botnets (such as Trickbot, Qbot and Dridex), one of the blights of the internet. Botnets are software programs that link a huge number of infected computers to form a usually automated 'robot network' – hence 'botnet', one of the core criminal internet entities. They are available for hire on a metered basis (often for as little as 15 minutes) to take down websites and online computer systems by sending a stream of automated requests for information that overloads the computers and forces them to crash. They provide the essential delivery mechanism for junk email campaigns, the DDoS attacks discussed earlier, and for ransomware.

---

19 'Microsoft Exchange exploits – step one in ransomware chain', ESET (29 Mar. 2021), https://www.eset.com/blog/enterprise/microsoft-exchange-exploits-step-one-in-ransomware-chain/ (last accessed 8 Mar. 2022).

20 ESET research from Q4 2020 showed that eCh0raix was the most prominent ransomware targeting NAS devices.

The criminals scan the internet looking for vulnerable computers to infest while simultaneously sending out junk email to catch the unwary. Once installed, the software harvests and sends data about the victims' machines to the attackers' server. The attackers then take control of the machine and link it with others they have infected to form a botnet, a network of computers that can be used in large-scale attacks, such as malicious email campaigns, DDoS attacks on websites and ransomware. For the owner of the computer, the only sign of the infection may be that it begins to run slowly.

Botnets such as Trickbot commonly attach Microsoft Office documents tainted with malicious code in email campaigns for initial intrusion that can later lead to ransomware as the final payload. In these cases, the botnet operators usually act as initial access brokers who sell or rent their access to compromised networks to the ransomware operators. It is because of this that there are often direct links between botnet and ransomware software.[21]

Criminals have also managed to pollute the legitimate software supply chain. People commonly acquire software by downloading it from websites and then, over the lifetime of using that software, receiving updates directly from the update servers of the software company. These servers routinely push updates that include bug fixes, security patches and new features.

In 2017, for example, it was found that an accounting software suite named M.E.Doc was being used by criminals to push the DiskCoder.C (aka NotPetya) malware as part of its cyberwar against Ukraine,[22] where M.E.Doc is widely used. The attackers penetrated the software company's update servers and added their own code to legitimate application update files. When users of the accounting software clicked to install program updates, they were also installing a malware backdoor, opening the way for what became the most devastating cyberattack in history.[23]

---

21 Some of the many known relationships between botnet and ransomware families include Emotet with Qbot, and Trickbot and Ryuk.

22 'TeleBots are back: Supply-chain attacks against Ukraine', We Live Security (30 Jun. 2017), https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ (last accessed 8 Mar. 2022).

23 'New TeleBots backdoor: First evidence linking Industroyer to NotPetya', We Live Security (11 Oct. 2018), https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/ (last accessed 8 Mar. 2022).

Kaseya VSA became another target of a supply-chain attack in July 2021. Kaseya is an IT management software provider whose main clients are managed service providers (MSPs). Its VSA product delivers automated software patching, remote monitoring and other capabilities so that MSPs can manage their customers' IT infrastructure.

The attackers compromised scores of MSPs using VSA and sent a fake update to the MSPs' customers that contained Sodinokibi ransomware.

Definitive proof that crime gangs were attempting to suborn employees to obtain access to their employers' networks came in July 2020 when the FBI arrested a Russian who tried to recruit a Tesla employee into a ransom scheme against the company. The employee was offered US$1 million in return for details about Tesla's network that would be used to develop custom malware to steal the company's data, which the employee would install during a diversionary DDoS attack.

The risk of insider threats is a continuing problem. According to a survey of IT firms in the United States conducted in December 2021, 65 per cent of employees revealed that hackers had offered them bribes to hand over access to their corporate networks. These campaigns used email, social media and even phone calls to reach out to employees.

Once inside a network, attackers will move on to the second stage and begin to explore, often with the aim of increasing their level of access. Modern operating systems typically assign a set of privileges to specific processes and users, which allows them to perform certain actions. This increases the security of a system because attackers that compromise systems as low-level users are limited in what they can do – having the highest level of privilege would allow attackers to do almost anything they want on the computer. So the attackers' first task is to check whether the operating system or any installed applications allow them to elevate their privilege level, ideally to that of administrator. The second objective is to maintain access for future intrusions.

This task becomes easier if the attackers are on a computer storing information about the people using the network, as one option is to look for people who have not used their accounts in a long time and to assume their identities. This is a very good reason for network administrators to disable and remove the accounts of former employees, lest a ghost of them should reappear in the network. Although an attacker could create a new user account, this would likely be noticed by the IT administrator. This is why maintaining an inventory of internet-facing assets, users and software is a basic step in preventing attacks.

Another approach used by attackers to achieve future access is to introduce 'back-door' software into a system that allows them to come and go at will, but ideally, an attacker will try to introduce as little malicious code as possible to minimise the

chances of detection. This is a strategy known as 'living off the land' because it uses legitimate software, often used by the system's actual administrators, and standard tools installed with the base operating system, to extend network penetration. There are valid reasons for these programs to be executed and so detecting abuse by an attacker can be difficult, although not impossible.

If endpoint protection is installed on the system and it can be turned off by a user with administrator privileges, the attacker will want to turn it off; therefore checking that all security solutions are protected with strong, unique passwords should be the first item in a security software audit.

How to protect your critical data

A basic step in defending against RDP attacks is to make an inventory of internet-facing accounts, listing those that have remote access enabled and deciding whether that access is necessary. Those accounts should have long and unique passwords – or passphrases, which are easier to remember.

Knowing you are under attack is useful. Some security products have brute-force attack protection that detects groups of failed external login attempts and blocks further attempts. In a brute-force attack, typically an attacker uses automated software tools to attempt to log in with standard administrator account names, such as 'admin', and lists of default or leaked passwords, sometimes making millions of attempts.

This can also be stopped by setting an account login threshold. For example, after three invalid login attempts, further login attempts could be blocked for a set period or still allow subsequent attempts but require longer intervals to flag the failed login.

Even better than relying on passwords is to use multi-factor authentication, which requires another piece of information in addition to the usual username and password.

Hardening and patching should be performed for all remotely accessible devices. All non-essential services and components should be removed or disabled and all system settings configured for maximum security.

Companies should adopt an email strategy. Many already have basic spam filtering and phishing detection in place but they can go further and block unused attachment types.

Organisations should protect all their endpoints and servers with endpoint protection software that stops employees going to web pages blacklisted by the software for hosting malware or deemed inappropriate for work use. The software also allows central management and updating and can control access to external devices, such as removable USB sticks, that are connected to a system.

Providing cybersecurity training for employees that reflects the latest trends significantly reduces cybersecurity incidents. Employees should report suspicious messages and attachments to the help desk or security team immediately.

Organisations should also have a comprehensive, properly managed and well thought out backup program. For example, when backup storage is 'always on', it can be compromised by ransomware in exactly the same way as local and other network-connected storage. This risk can be prevented by:

- ensuring that backups are not routinely and permanently online;
- protecting backed-up data from automatic and silent modification or overwriting by malware whenever online;
- protecting earlier generations of backed-up data from compromise, to provide a fallback;
- examining the organisation's legal liability to its customers; and
- carrying out regular testing, validation of readiness and optimisation of the backup process.

Conclusion: To pay or not to pay?

The threat of cybercrime has raised the costs of the internet-enabled computer systems that are essential to modern businesses and forces three choices on organisations: invest in cybersecurity, pay for cyber insurance or foot the cost of an attack – sometimes a combination of the three.

From a technical viewpoint, there are several potential points where a ransom payment made in the hope of receiving a decryption key can go wrong:

- some of the data might have been corrupted in the encryption process and is not recoverable;
- the process for delivering the decryption key fails;
- the decryption tool might be bundled with other malware, might not work properly, or is much slower than backup recovery; or
- if the ransomware has been removed, the encrypted data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is often part of the malware.

Paying a ransom also has its risks: the criminals may not keep their word, although this is not 'good' business. It is also an acknowledgement of weakness. According to a survey carried out in 2021, almost half of the organisations that paid ransoms were attacked a second time, apparently by the same gang.

Cyber insurers now play an important part in protecting companies from cyber incidents but the increase in attacks is driving up premiums. Potentially large payments also encourage the growth of ransomware – there have already been cases of gangs digging through an attacked company's files to discover whether it has a cyber-security policy and how much it is covered for, suggesting the role of cyber insurers may need to change to providing insurance against the cost of recovery, rather than paying a ransom.

Regulatory attention is also beginning to be focused on ransomware gangs. This has led to a requirement in some jurisdictions to disclose incidents, and to add groups and individuals known to be associated to them to sanctions lists. A pushback is also occurring against the practice of ransom payment. It is possible governments may insist on mandatory disclosure before paying and limit the circumstances in which it can occur. As the FBI makes clear: 'Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity.'[24]

However, taking the moral high ground by not paying is not always the cheaper option. When WannaCryptor hit the UK's National Health Service, experts estimated the rebuilding costs at £92 million in costs to rebuild.

When critical services such as healthcare are hit, some point out the potential harm to human life by not paying the ransom. There have already been two cases,[25] in 2019 and 2020, in which a ransomware attack was named as one of the possible contributory causes of the death of a patient.

Paying ransoms also masks another issue, which is that perhaps companies should legally be obliged to protect their systems, particularly in certain industries.

In fact, the long-term costs of taking the easy path of paying now seem to be sparking new impetus among insurers to push organisations right back to the basic cybersecurity practices and tools in which they should have been investing all along.

---

24 FBI Cyber Division Assistant Director James Trainor quoted in 'Incidents of Ransomware on the Rise – Protect Yourself and Your Organization', FBI News (29 Apr. 2016), https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise (last accessed 8 Mar. 2022).

25 The first was in connection with a baby's death (30 Sep. 2021), https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116; the second with a woman's death (17 Sep. 2020), https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/; and a third clarifying the impact of ransomware (12 Nov. 2020), https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/ (web pages last accessed 8 Mar. 2022).

RENÉ HOLT
ESET

René Holt is a security writer with ESET's global public relations team based in Bratislava, Slovakia. He works with malware researchers, detection engineers and product development teams to better understand and raise awareness of the modern cyber threats that are endangering the security of businesses today. His particular areas of interest are ransomware, vulnerability research and threat hunting tools.

Aupark Tower, 16th Floor
Einsteinova 24
Bratislava 851 01
Slovakia
Tel: +421 2 322 44 111
Fax: +421 2 322 44 109
www.eset.com

René Holt
rene.holt@eset.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