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

Editor
Mark Deem

The Guide to Data as a Critical Asset 2022

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

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

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-859-8

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

Contents

Preface

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

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

Global Data Review
London
March 2022

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

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