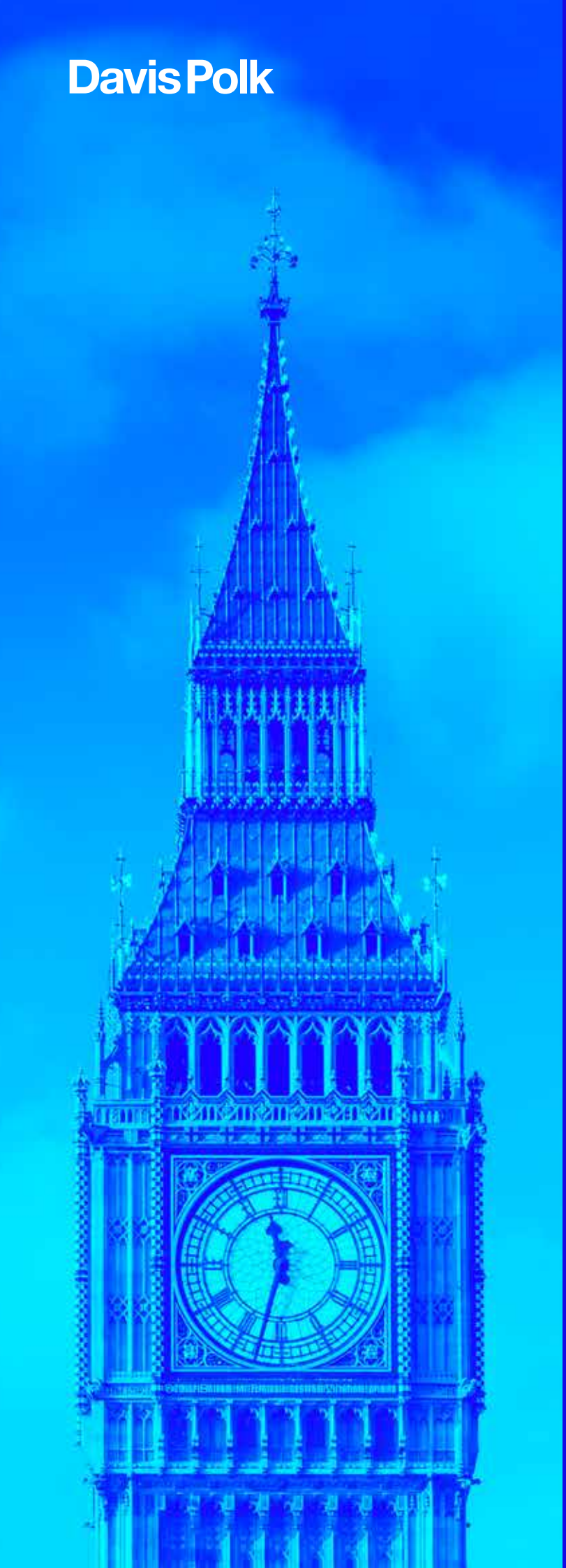
PRIVATE M&A 2023

Contributing editors
Will Pearce and Louis L Goldberg
Davis Polk & Wardwell LLP

LEXOLOGY
Getting the Deal Through

Davis Polk

Davis Polk



Davis Polk is a leader in global M&A. Clients call on our lawyers because of our track record of getting deals done.

With the benefit of our long history of innovation and creative problem-solving, Davis Polk brings strategic and sophisticated judgment, commercial awareness and unsurpassed service to our clients across the full spectrum of M&A transactions.

Our M&A clients rely on the seamless integration of Davis Polk's unparalleled tax, finance, executive compensation and regulatory practices.

Learn more at **davispolk.com**.

davispolk.com

Data privacy and cybersecurity in global dealmaking

Matthew J Bacal, Pritesh P Shah and Mikaela Dealissia

Davis Polk & Wardwell LLP

Since the adoption by the European Union (EU) of the General Data Protection Regulation (GDPR) in 2016, which marked a true watershed moment, data privacy and security concerns have shifted increasingly to the forefront in the minds of consumers, government authorities, business leaders and the media.

This trend has only accelerated year after year as data increasingly becomes a key driver of the modern economy and one of its most valuable asset classes; consumers demand greater protection of their personal data; governments, businesses and security experts seek to keep pace with the increasing sophistication of cyber-criminals, including nation-state and state-sponsored actors, and the increasing frequency and variation of cyberattacks; and legislators and regulators attempt to pass and enforce new laws in this challenging and constantly evolving environment.

Against this backdrop, data privacy and security have transitioned from industry- or deal-specific concerns to broadly relevant issues requiring consideration in nearly every transaction. While sufficiently complicated in any given jurisdiction, increasingly global deals are forcing buyers and sellers to directly confront those issues, commencing at the deal structuring stage, through diligence, ultimate risk allocation and post-closing integration activities.

Legal and regulatory developments

Whether the consequences are primarily reputational or felt immediately at the negotiating table, the upshot remains that all parties to a deal must be cognisant of the implications of an evolving data privacy and security landscape to mitigate short-term disadvantages and long-term risks. A brief tour of the world gives some sense of the breadth of laws and regulations that may require consideration in a global transaction.

Europe

One of the most anticipated and influential data privacy and security regulations to date, the GDPR came into effect on 25 May 2018 in the EU and changed the compliance landscape with its extraterritorial scope, weighty obligations and significant penalties. With the exit of the UK from the EU, its own version of the GDPR, as implemented into the domestic laws of the UK, came into effect (the UK GDPR). While the two laws remain very similar for the time being, the UK Parliament is currently considering changes to the UK GDPR, many of which could have significant impacts for both businesses and individuals.

United States

In the United States, holistic data privacy and security regulations have been slow to emerge at the federal level (with Congress considering, but failing to advance, a number of proposals over the past few years, including a comprehensive federal data privacy bill). Apart from the Federal Trade Commission's broad consumer protection mandate and the Securities and Exchange Commission's increasing focus on the data privacy and security practices of publicly traded companies across the spectrum, the federal government has generally continued to rely on a sector-based approach to data privacy and security regulation – focusing on high-risk, regulated industries such as healthcare (eg, the Health Insurance Portability and Accountability Act (HIPAA)) and financial services (eg, the Gramm-Leach-Bliley Act (GLBA)). Most recently, the Biden administration issued executive orders mandating that the federal government create revised cybersecurity standards for all government contractors and requiring the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA.

In the meantime, legislatures at the state level, pushed by consumer protection and privacy advocates, have been at the vanguard of developing comprehensive data privacy and security laws and regulations. California paved the way with its passage of the California Consumer Privacy Act (CCPA) in 2018 and the California Privacy Rights Act (CPRA) in 2020, but states such as Virginia, Colorado, Utah and Connecticut have followed suit, and many other states have passed, or are actively considering, some form of data privacy or security law. Moreover, all 50 states have enacted laws requiring notification of data breaches under varying circumstances.

Other nations

Elsewhere in the world, data privacy and security regulations in other key economies, including Canada, Japan, China, Brazil, Russia, Israel and India, are continuing to evolve and may also impact global dealmaking.

The EU GDPR and UK GDPR

Effective on 25 May 2018, the GDPR governs the processing of personal data by data 'controllers' and 'processors'. A data controller is a person or entity who determines the purposes and means of the processing of personal data. A data processor is a person or entity who processes personal data on behalf of the data controller.

Under the GDPR, the terms 'processing' and 'personal data' are defined broadly enough to capture essentially any activity performed on data related to an individual. Specifically, the definition of personal data covers 'any information relating to an identified or identifiable natural person ("data subject")' and 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that

natural person'. Processing of personal data subject to the GDPR must be done lawfully, fairly and in a transparent manner, and personal data may be collected only for a specified, explicit and legitimate purpose.

Among other operational, contractual, governance and notification obligations on data controllers and processors discussed below, the GDPR provides that controllers must implement 'appropriate technical and organisational [security] measures' for data protection and may use only processors that provide 'sufficient guarantees' to implement those measures. The GDPR also provides data subjects with certain rights in respect of their personal data, including, among other things, the right to demand prompt erasure of any personal data collected (the 'right to be forgotten'), the right to withdraw consent for or object to the processing of personal data, the right to restrict processing of personal data and the right to obtain the identities of third parties to whom their personal data is being disclosed.

Of particular concern to businesses, GDPR violations can result in significant fines of up to the greater of €20 million or 4 per cent of the total worldwide turnover in the preceding fiscal year.

While the GDPR applies to all EU countries, ongoing developments in the UK, including Brexit, have created uncertainty with regard to data protection regulation in the UK and its relationship with the EU. As of 1 January 2021, following the expiry of the transitional arrangements agreed between the UK and EU, data processing in the UK has been governed by the UK GDPR, which combines the GDPR and the UK Data Protection Act of 2018.

This change exposes businesses operating in both the UK and the EU to two parallel regimes, each of which authorises similar fines, such that any violations under the GDPR may also trigger separate regulatory actions and penalties in the UK, and vice versa. At the same time, the two regimes, even in their current, substantially similar form, may be subject to potentially different interpretations and enforcement actions for certain violations.

Over time, either or both laws may be amended in ways that diverge and pose additional compliance challenges for businesses operating in both jurisdictions. While the European Commission (EC) recently adopted an adequacy decision in favour of the UK, which, as discussed further below, enables the continued free flow of personal data between the UK and the European Economic Area (EEA), the decision contains safeguards against future divergence of the laws, including a 'sunset clause', which limits the duration of the adequacy decision to four years.

In August 2021, the UK government announced that it would seek to chart its own path on data protection and reform its relevant laws, including in ways that may differ from the GDPR. The EC responded that it would closely monitor any such changes for impacts on the adequacy of the UK data protection regime. In June 2022, the UK government announced its intention to further reform the UK data protection regime.

The CCPA, CPRA and other US state laws

Unlike the EU, the US has not yet implemented a comprehensive federal data privacy and security regulatory framework. Recent trends, however, have seen states take the lead on enacting significant legislation that affects corporations looking to conduct business within certain jurisdictions or with citizens of those jurisdictions.

One example of recent state legislation is the CCPA. Enacted in 2018, the CCPA came into effect on 1 January 2020, and the California Attorney General's enforcement power came into effect on 1 July 2020.

The CCPA provides many consumer protections and compliance obligations reminiscent of the GDPR and adopts a particularly broad definition of personal information that sweeps in any information that 'identifies, relates to, describes, is reasonably capable of being associated with, or that could reasonably be linked, directly or indirectly, with a particular [California resident] or household'. This definition is limited by certain exclusions, including for publicly available information (subject to certain restrictions), as well as for de-identified or aggregate consumer information that cannot reasonably be linked to the underlying individual or household.

In addition, the CCPA provides, among other things, for certain 'rights to be forgotten', including the requirement that businesses delete personal information upon request if the information is not necessary for a specific business purpose, legal compliance or other expected internal uses. The law also establishes a consumer right to request from businesses details about collected information, the purpose for the collection and third parties with whom the information has been shared. A consumer may also request that businesses provide disclosures regarding the sale of consumer data, as well as an opt-out from such sale.

While affording California residents such expanded privacy rights and protections, the CCPA also prohibits covered businesses from discriminating against California residents for exercising any of their rights under the law. It also provides for severe civil penalties and statutory damages for violations and includes a new private right of action for certain data breaches that result in the loss of personal information. This private right of action is expected to increase the likelihood of, and risks associated with, data breach litigation; however, even after more than two years since enforcement began, it remains unclear how various provisions of the CCPA will be interpreted and enforced.

While the CCPA has scope limitations, the breadth of the law reaches large international entities with exposure to California residents as it applies to for-profit businesses that conduct business in California and:

- have a gross annual revenue of over US$25 million;
- buy, receive or sell the personal information of 50,000 of more California residents, households or devices; or
- derive 50 per cent of more of their annual revenue from selling California residents' personal information.

The CCPA provides certain exemptions for entities subject to HIPAA and for data subject to certain other legal regimes, including the GLBA. To provide greater clarity on the CCPA's application and reach, the California Attorney General has issued a series of regulations under the law, the most recent version of which was approved by the California Office of Administrative Law on 15 March 2021.

Further complicating matters, in November 2020, less than a year after the CCPA came into effect and just a few months after enforcement began, California voters passed a new privacy law, the California Privacy Rights Act (CPRA), by ballot initiative. Effective in most material respects from 1 January 2023, the CPRA will significantly modify the CCPA, impose additional data protection obligations on companies doing business in California and grant additional rights to California residents. For example, under the CPRA, California residents may:

- prevent businesses from sharing their personal information under certain circumstances;
- correct inaccurate personal information; and
- limit businesses' use of sensitive personal information (eg, geolocation data, race, ethnicity, religion, genetic data, private communications and sexual orientation) and specific health information.

Non-compliance with the CCPA and the CPRA may present a severe risk to businesses. The CCPA and CPRA provide a private right of action for California residents who have been affected by certain data breaches, whether individually or through class actions, with statutory penalties between US$100 and US$750 per individual per incident and injunctive or declaratory relief without a requirement for the individual to prove actual harm. The California Attorney General is also empowered under the CCPA and the CPRA to pursue enforcement against businesses for penalties of up to US$7,500 for each intentional violation of the law, and penalties of up to US$2,500 may be imposed for any violation of the

CCPA that has not been cured within 30 days of notice of any alleged non-compliance. The CPRA, when it becomes effective, will remove such notice and cure period. The CPRA also establishes a regulatory agency, the California Privacy Protection Agency (CPPA), dedicated to enforcing the CCPA and the CPRA.

The CCPA is not clear regarding whether each violation, as used in calculation of damages for the California Attorney General, is on a per individual per incident basis or simply a per incident basis. On 24 August 2022, the California Attorney General issued its first fine under the CCPA, announcing a settlement with Sephora resolving allegations that Sephora violated the CCPA (including a failure to disclose to consumers that it was selling their personal information). The settlement requires Sephora to pay a US$1.2 million fine and to comply with certain injunctive terms (including to clarify its online disclosures and privacy policy and to provide a mechanism for consumers to opt out of the sale of their personal information). However, the complaint and settlement do not provide any insight into how the amount of the fine was calculated. The CPRA is similarly ambiguous as to the calculation of damages. Instruction based on further civil enforcement actions or an amendment to the law or further regulatory guidance on this distinction will, therefore, be crucial in evaluating a business's risk of non-compliance. For example, the CPPA is still considering proposed rulemaking for the CPRA.

While California has led the way, many other state legislatures have passed, or are currently contemplating and may pass, their own comprehensive data privacy and security laws. For example, in March 2021, Virginia adopted the Virginia Consumer Data Protection Act, which is scheduled to take effect in January 2023; in June 2021, Colorado adopted the Colorado Privacy Act, which is scheduled to take effect in June 2023; in March 2022, Utah adopted the Utah Consumer Data Protection Act, which is scheduled to take effect in December, 2023; and in May 2022, Connecticut adopted the Connecticut Data Privacy Act, which is scheduled to take effect in July 2023.

Other states, such as Illinois, Massachusetts, New York and Nevada, have adopted more narrowly focused privacy or cybersecurity laws but may pass more comprehensive legislation in the future. Compliance with this rapidly evolving patchwork of laws and regulations can be challenging, costly and distracting of management attention, and it will likely require companies to routinely revisit and modify their data processing practices and policies to comply and maintain compliance. As discussed below, it also heightens the need for appropriate data privacy and security due diligence in the context of M&A activity.

Complying with data transfer requirements

While the various regulatory regimes have upped the ante in respect of the physical, technical and administrative measures companies must implement for compliance purposes, as well as the rights afforded to consumers whose data has been collected, one of the most impactful trends when it comes to M&A transactions has been data transfer restrictions, in particular in the EU, China, Russia and certain other jurisdictions. To the extent that a target has activities in those jurisdictions, appropriate consideration must be given in respect of whether personal data in those jurisdictions can be transferred out of the jurisdiction at all, potentially complicating business consolidation goals.

For example, under the GDPR and the UK GDPR, personal data can be freely transferred out of the EEA or the UK, respectively, only if the EC or the appropriate UK regulatory authority, as applicable, has deemed the recipient jurisdiction to provide an adequate level of data protection. Absent such determination (which the US has not obtained from either body), another appropriate safeguard or derogation is required to effect the transfer, which may complicate the data transfer process.

The EU–US Privacy Shield Framework, which was designed to permit transfers of personal data out of the EEA into the US, passed an annual review by the EC in 2019 but was invalidated by the Court of Justice of the European Union (CJEU) in its Schrems II decision on 16 July 2020. The CJEU's judgment also created uncertainty around the continued viability of the use of the EC-approved standard contractual clauses (SCCs) in respect of transfers of personal data from the EEA to the US.

While the CJEU upheld the adequacy of the SCCs generally as an adequate personal data transfer mechanism, the court made clear that reliance on the clauses alone may not necessarily be sufficient in all circumstances; rather, their use must be assessed on a case-by-case basis, taking into account the surveillance laws in, and the privacy rights of individuals afforded by, the destination country. Moreover, the CJEU stated that if the competent supervisory authority believes that the SCCs cannot be complied with in the destination country, and if the required level of protection cannot be secured by other means, the supervisory authority is under an obligation to suspend or prohibit that transfer unless the data exporter has already done so itself.

The EC approved new SCCs in June 2021, which, where applicable, must be used for all new data transfer arrangements involving EU personal data after 27 September 2021 and for all existing data transfer arrangements involving EU personal data by no later than 27 December 2022. While it is currently generally believed that the new SCCs may be used for data transfers from the EEA to the US under most circumstances, some uncertainty remains; the European Data Protection Board (EDPB) or EU member state data protection authorities have or may issue complicating guidance, and the use of the SCCs for transfers to the US or certain other jurisdictions may be subject to further challenge in the future. In March 2022, the European Commission announced an agreement in principle had been reached between EU and US authorities regarding a new transatlantic data privacy framework, however, no formal agreement has been reached, and any such agreement, if formalized, is likely to face challenge at the CJEU.

As discussed above, while the UK currently has an adequacy decision from the EC, the decision may be revoked in the future if the UK GDPR deviates substantially from the GDPR. In March 2022, the UK adopted an International Data Transfer Agreement (IDTA) for transfers of personal data out of the UK, as well as an international data transfer addendum (UK Addendum) that can be used with the EC-approved SCCs for the same purpose, further complicating transatlantic data flows.

Other countries have passed or are considering passing laws requiring local data residency or restricting the international transfer of data – developments that will likely have a significant impact on operations, as well as the expenses and profitability, of many global organisations.

Impact on M&A transactions

For a well-advised purchaser or seller in an M&A transaction, the evolving landscape of data privacy and security necessitates understanding the impact these regulatory regimes have on risk allocation, structure and business flexibility.

In particular, parties to an M&A transaction should be mindful of:

- the extended jurisdictions of the GDPR and the UK GDPR, which encompass companies with establishments in the EU and the UK, respectively, as well as companies, regardless of domicile, that process the personal data related to the offering of goods or services to data subjects in the EU or the UK, as applicable;
- the risk of substantial fines under the GDPR and the UK GDPR based on global revenue that increases the importance of conducting thorough due diligence on a target's compliance with data protection laws; and
- transaction structuring and risk allocation mechanisms that should expressly contemplate data protection to ensure compliance and allocate the risk of non-compliance with the GDPR, the UK GDPR, the CCPA, the CPRA and other data protection regimes, as applicable.

Due diligence

Purchasers and investors should first consider whether the target's data processing is subject to the GDPR, the UK GDPR, the CCPA, the CPRA or any other key data protection regimes.

Under the GDPR and the UK GDPR, processing of personal data is defined broadly to include nearly any act that is performed on personal data, including collection, organisation, storage, use and even the destruction of personal data. The GDPR covers processing of personal data that:

- occurs in the context of the activities of an establishment in the EU;
- relates to the offering of goods or services, regardless of whether payment is required, to individuals in the EU; or
- relates to the monitoring of individuals' behaviour in the EU.

The 'offering of goods or services' may be broadly construed and depends on 'factors such as the use of a language or a currency generally used in one or more member states with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the [European] Union'.

The UK GDPR effectively applies with the same scope in relation to the UK. As a result, the GDPR or the UK GDPR may apply to companies that do not have substantial EU- or UK-based activities and have not previously focused on EU or UK data protection laws.

As discussed above, the CCPA applies to certain businesses that collect personal information from California residents who are defined as 'consumers'. For the purposes of the CCPA, a 'business' is any for-profit legal entity that:

- does business in California; and
- collects, or directs others to collect, consumers' personal information, determines the purposes and means of processing consumers' personal information and:
    - has annual gross revenues in excess of US$25 million (the CPRA clarifies that this refers to US$25 million in the preceding calendar year);
    - annually buys, sells or otherwise commercially processes the personal information of at least 50,000 consumers, households or devices (the CPRA, when it becomes effective, will raise the threshold to 100,000 and remove the reference to devices); or
    - derives 50 per cent or more of its annual revenues from selling consumers' personal information (the CPRA, when it becomes effective, will expressly add sharing for purposes of cross-context behavioural advertising under this prong).

An entity's obligation to comply with the CCPA flows to majority-owned subsidiaries or parent companies with common branding, even if those entities do not independently meet the qualifications of a business under the law. As a result, evaluating whether a particular target is subject to the CCPA may require consideration of the activities of its subsidiaries or parent companies. For example, a business and a consumer do not need to directly engage in a commercial transaction for the business's collection of that consumer's data to come within the purview of the CCPA; rather, the business's data intermediaries, partners and service providers may be subject to the CCPA, rendering it applicable to the business.

Practice tips

- Do not rely on the target's claims that it does not have material EU or UK operations: go beyond diligence questions and investigate the company's online presence, including whether visitors to the target's website from the EU or the UK are provided with local language or shipping options.
- If the target appears to be subject to the GDPR or the UK GDPR, consider whether the purchaser will have access to personal data in the data room or will be provided with such information during the diligence process. If so, the purchaser may be subject to the GDPR or the UK GDPR, or both, and non-disclosure agreements may need to be tailored accordingly. Unless necessary, some purchasers may prefer to affirmatively exclude any personal data from the data room or diligence process to avoid being subject to the GDPR or the UK GDPR.
- Look beyond the target's customer-facing business to consider possible obligations under the CCPA and the CPRA: while the CCPA and the CPRA include an exemption in respect of certain personal information of employees and business-to-business (B2B) contacts, businesses' obligations under the CCPA and the CPRA in respect of personal information of California employees, contractors, candidates and B2B contacts will become effective in January 2023 (absent further action from California's legislature), so prudent businesses may want to consider those requirements now. Additionally, the current exemption does not excuse companies from certain notice obligations or potential liability in the event of certain types of breaches; therefore, even if the target does not commercialise consumer data, it may still be subject to the CCPA and the CPRA if it collects routine human resources data about California employees, contractors or candidates, or personal information of B2B contacts, a target should be prepared to demonstrate its efforts to comply with its CCPA and the CPRA obligations in connection with such data.
- Sellers should anticipate purchaser GDPR, UK GDPR, CCPA and CPRA questions, and consider practicing diligence responses with outside counsel to prepare for calls. As we draw closer to the effectiveness of other major US state data protection laws that have recently passed (eg, the Virginia Consumer Data Protection Act and the Colorado Privacy Act) or that may be passed in the coming months or years, sellers should also be prepared to answer questions about their compliance with those laws, to the extent applicable. Given the uncertainties regarding the interpretation and enforcement of data protection laws, perfect confidence in compliance is unlikely to be expected, but being conversant in those topics will assure purchasers that the issue is being thoughtfully considered.

To the extent that a company may be subject to the GDPR, the UK GDPR, the CCPA or the CPRA, the purchaser may need to re-evaluate and reorient the target's data processing activities after the transaction. The review may look into:

- the process by which the company obtains 'freely given, specific, informed and unambiguous' consent from individuals;
- the company's use of the data and whether it is consistent with the data processing principles of the GDPR or the UK GDPR; and
- the degree to which the company supports data subjects' rights (including the right to access, rectification, erasure – the 'right to be forgotten' – and portability).

Post-closing review also may include consideration of the mechanisms that the company has put in place to respond to consumer requests under the CCPA and the CPRA. Additionally, under the GDPR, the UK GDPR, the CCPA and the CPRA, most covered companies must maintain records of their data collection and processing activities relating to persons protected by the regulations, including the purposes of the processing, a description of the categories of data subjects and personal data, the categories of recipients, the duration of processing, any third-country transfers and general descriptions of the applicable technical and organisational security measures.

Practice tips

- The target's records of processing activities will often be a good starting point to approach key questions, including:
  - Whose personal data is being processed?
  - What kind of personal data is being processed?
  - For what purpose is the data being processed?
  - For how long is the data processed and stored?
  - Is data transferred to other parties?
  - Is data transferred out of the EU?
  - What security measures are in place to safeguard the data?
- If the target is subject to the CCPA and the CPRA, consideration must be given to whether the target has adequate mechanisms to track consumer requests and separate databases of personal information to segregate personal information that cannot be sold. Following the processing of a consumer's opt-out request, a business may not request subsequent authorisation to sell personal information for at least 12 months.

Careful diligence should be conducted on the target's contracts with third parties that are processing data on its behalf. Amendments may be necessary to conform those contracts in respect of requirements under the GDPR, the UK GDPR, the CCPA or the CPRA, including those that add specific provisions relating to the processing of personal data.

As discussed above, the GDPR and the UK GDPR place restrictions on certain cross-border data transfers. Diligence should be conducted with a focus on the existence of such transfers of data outside of the EEA or UK, as applicable (in the case of a US target, local servers may be absent), and the applicable justifications for such transfers.

Under the CCPA and the CPRA, a business that receives a consumer's request to delete personal information may be obliged to direct third-party service providers, including data processors, to delete that consumer's personal information from their records. Consideration should be given to whether the target's contracts with service providers allow it to comply with this obligation.

In addition to heightened obligations regarding the processing of personal data and responding to consumer requests, the GDPR, the UK GDPR, the CCPA and the CPRA also impose affirmative requirements for companies to implement appropriate technical and organisational measures to ensure a level of data security appropriate to the risks presented by the nature, scope, context and purposes of the company's data processing (or penalties for a lack hereof). Under the GDPR and the UK GDPR, companies must ensure such measures are taken by a company's third-party processors as well.

The GDPR and the UK GDPR institute the strictest data breach notification obligations of any generally applicable data protection laws. Companies must notify their competent supervisory authority 'without undue delay and, where feasible, not later than 72 hours' after becoming aware of a data breach. For particularly egregious breaches, the company may also be required to notify the affected individuals. Regardless of whether notification is required, the company must maintain a breach register and document all breaches – the related facts, effects and remedial actions taken – subject to verification by the supervisory authority.

During diligence, it is prudent to request a copy of the target's breach-related documentation. If the target does not maintain a record of breaches, then it may be operating in violation of applicable law, and further diligence may be required to identify whether the target has suffered data breaches that may present future regulatory or litigation risk. Breach-related documentation may also be scrutinised for insight into the target's data breach remediation procedures and approach to risk management and compliance.

While the CCPA and the CPRA do not themselves include any data breach notification obligations, they allow for private actions for damages from certain data breaches, as discussed below, and California maintains a separate breach notification law, which requires companies to notify individuals affected by a breach 'in the most expedient time possible and without unreasonable delay.

Practice tips

- GDPR and UK GDPR compliance will not be satisfied – or considered properly covered by due diligence measures – by a check-the-box approach. Consider requesting a copy of the company's latest data map. The company must be able to provide it to a regulator on short notice, and if it does not have one ready, this may be a sign of an overall lax approach towards compliance.
- Companies outside the EEA or the UK may benefit from building direct relationships, typically through their data protection officer, with appropriate data protection authorities in the EEA and the UK, as applicable. Those relationships can facilitate a smoother notification process as a single data breach may trigger notification obligations in the US, as well as in the EEA and the UK.
- With the rise of remote working practices, particularly in light of the covid-19 pandemic, evaluation should be made in respect of whether the target has evaluated the impacts of a shift in working practices (and any corresponding increase in data security threats) on its data security procedures and practices. A failure to appropriately revise those procedures and practices may expose the target to a higher incidence of data breaches, resulting in additional regulatory scrutiny or private actions under the CCPA and the CPRA.
- Sellers should pre-empt onerous document requests by proactively providing high-level summaries of the target's personal data practices.

If applicable, non-compliance with the GDPR, the UK GDPR, the CCPA and the CPRA presents a serious risk. Each regime provides for regulatory enforcement, as well as certain private rights of action.

Relevant data authorities are empowered under the GDPR and the UK GDPR with broad investigatory and corrective powers. These include the ability to:

- compel companies to provide whatever information may be required to evaluate compliance with the GDPR or the UK GDPR and conduct data protection audits, including obtaining access to a company's premises;
- grant injunctive relief (including modifying a company's data processing processes, forcing a company to provide notice of a data breach to a data subject or imposing a temporary or permanent ban on data processing); and
- impose administrative fines.

Administrative fines under the GDPR and the UK GDPR are not merely compensatory for losses suffered by a data subject; rather, they are structured to be 'effective, proportionate and dissuasive'. The GDPR and the UK GDPR provide limits to administrative fines of up to the greater of €20 million (or, under the UK GDPR, its equivalent in British pounds) or 4 per cent of the total worldwide turnover in the preceding fiscal year for violations of core substantive requirements (including in respect of the GDPR's or the UK GDPR's principles for processing, conditions for consent, data subject's rights and international transfers of data). For more procedural violations, there is a lower threshold of the greater of €10 million (or, under the UK GDPR, its equivalent in British pounds) or 2 per cent of total worldwide turnover.

The CCPA and the CPRA provide for enforcement by the California Attorney General for any violation of the CCPA and the CPRA. The California Attorney General may bring actions for an injunction and civil penalties of up to US$2,500 for each violation or up to US$7,500 for each intentional violation, after a 30-day notice and cure period. However, the CPRA, when it becomes effective, will remove such notice

and cure period. As discussed in more detail above, on 24 August 2022, the California Attorney General issued its first fine under the CCPA, announcing a settlement with Sephora resolving allegations that Sephora violated the CCPA and did not cure such violations within the 30-day notice and cure period. The settlement requires Sephora to pay a US$1.2 million fine and to comply with certain injunctive terms.

The CCPA and the CPRA also provide a private right of action for consumers whose non-encrypted personal information is subject to an unauthorised access or disclosure as a result of a business's failure to implement and maintain reasonable security practices. Among other forms of relief, after a 30-day notice and cure period, a plaintiff may seek to recover damages valued at the greater of actual damages or statutory damages, which range from US$100 to US$750 per consumer per incident, depending on the nature of the violation and the defendant's assets, liabilities and net worth.

Four years after the GDPR's implementation, and two years since CCPA enforcement began, observers have been watching for regulatory and private enforcement under those laws as businesses and legal communities continue to evaluate trends in global enforcement actions. While not all fines levied in the first four years of the GDPR reached a substantial size, perhaps the most newsworthy penalty determined in the first year of GDPR enforcement was the €50 million fine imposed by the French National Commission on Informatics and Liberty against Google in January 2019.

This penalty was followed by a series of fines from October 2020, including the €35 million fine imposed by the Hamburg Commissioner for Data Protection and Freedom of Information against H&M, and €22.4 million and €18.4 million fines imposed by the UK Information Commissioner's Office against British Airways and Marriott International, respectively. The Luxembourg National Commission for Data Protection issued the largest GDPR fine recorded to date on 16 July 2021 against Amazon in the amount of €746 million (which Amazon is appealing). Most recently, the French Commission Nationale Informatique & Libertés issued a GDPR fine on 31 December 2021 against Google in the amount of €150 million. In the aggregate, these fines demonstrate the possible magnitude of the penalties under the GDPR.

While active cases for violations of the CCPA have already been brought, including those against well-known corporations such as Amazon, Zoom and TikTok, it remains to be seen how penalties under the CCPA and the CPRA will be implemented in private and public enforcement actions.

Practice tips

- Investigate the company's history of cooperation with data privacy regulators in the EU and the UK and its past handling of data breaches. A company history of regulator cooperation may help mitigate future fines.
- Carefully probe the company's personal data retention practices with an eye towards confirming that the company only retains personal data as necessary.
- Investigate the target's mechanisms to process data subject requests. Additionally, consider the target's past handling of data breaches as an indication of the level of risk that the target presents.

Valuation considerations

If the GDPR, the UK GDPR, the CCPA or the CPRA regimes apply, the purchaser or seller in an M&A transaction should consider:

- how consistent the valuation model is with the scope of the company's ability to use its personal data;
- the potential costs to bring the business into compliance with legal obligations from an operational, contractual and governance perspective; and
- the reputational and financial risks associated with non-compliance with the GDPR, the UK GDPR, the CCPA or the CPRA (while the GDPR, the UK GDPR, the CCPA and the CPRA provide for the use of personal information, the laws' constraints may impact a target in different ways).

Considering first the GDPR, one of the law's core principles is the purpose limitation, which binds companies to the specified, explicit and legitimate purposes communicated to data subjects when their personal data is collected. Further processing beyond the original communicated purposes is allowed only to the extent that the processing is not incompatible with the original purpose.

If the purchaser's or the investor's valuation model relies on different or expanded uses of the target's database of personal data, the purchaser may need to communicate a new privacy statement to each data subject and, in certain instances, obtain affirmative consent to be compliant. The cost and time associated with this exercise may impact the purchaser's business plan as the GDPR may require affirmative consents that may not be satisfied by, for example, simply updating a privacy policy on a website. The same considerations apply to the UK GDPR.

The CCPA does not contain a purpose limitation in line with that of the GDPR or the UK GDPR; however, the CPRA (when it becomes effective) will include a purpose limitation similar to that of the GDPR. Additionally, the CCPA and the CPRA do provide consumers with a right to opt out of the sale of their personal information and a right to be forgotten through the deletion of personal information previously collected or shared with service providers. If the purchaser's or the investor's valuation model relies on the continued use of existing databases of personal information, the model should reflect the risk that a portion of California consumers may request the deletion of their personal information or may opt out of future collection. Purchasers and investors should also consider whether a target's operational model feasibly allows the business to stop selling or sharing data upon a consumer's request.

Practice tips

- Financial modellers should be pushed on their models and assumptions, and personal data-related assumptions that legal and business teams should focus on during diligence should be identified.
- Sellers should update privacy policies or obtain appropriate consents before the transaction is consummated to ensure that the company's database of personal data may be transferred in connection with a merger or similar transaction.

The implementation of certain operational, governance and contractual measures prescribed by the GDPR, the UK GDPR, the CCPA and the CPRA, including those described above, may impose additional financial costs.

For instance, in a scenario where an acquisition expands the data processing activities of the target to constitute large-scale, regular and systematic monitoring of data subjects, the appointment of a data protection officer may be required under the GDPR or the UK GDPR. Under the GDPR and the UK GDPR, the company may also need to implement extensive documentation processes and conduct data protection impact assessments.

The CCPA and the CPRA require the implementation of California-facing privacy notices and mechanisms through which consumers can submit requests to the company. These requirements are in addition to the obligation to amend the company's existing contractual arrangements with third parties (which, beyond the diversion of resources, may require additional consideration) and the implementation of appropriate

data protection measures. The total costs of such measures could be significant.

Practice tip

- The diligence gap analysis should include a review of technical cybersecurity and physical security operations, as well as a headcount of the company's data privacy compliance function. IT upgrades can be a significant expense and, if the compliance function is understaffed, additional resources may be required.

Non-compliance with the GDPR, the UK GDPR, the CCPA and the CPRA risks severe financial and reputational harm. As discussed above, administrative fines for non-compliance with both laws can be punitive, and the indirect costs of dealing with a data breach may also be significant. For example, data breaches can involve potentially huge damages awarded to private plaintiffs under the CCPA and the CPRA, as well as third-party costs of investigation and remediation (and may involve notifications and credit monitoring, where applicable). Furthermore, reputational harm associated with a data breach can be even more problematic for companies that rely heavily on consumer trust.

Practice tips

- Nearly every company regularly faces actual or attempted data security breaches, and the Federal Bureau of Investigation has reported an increase of 300 per cent in reported cybercrimes since the onset of the covid-19 pandemic and the accompanying increase in remote work; therefore, it is critical that the target is aware of the ever-present threat of breach attempts and is implementing measures to ensure its data is as secure as reasonably possible.
    - Do not limit diligence to the target's legal staff; also speak with the chief information officer regarding penetration testing, patch and logging procedures, and the target's information security and breach response plans.
    - Consider whether the target has received any notices for CCPA violations that were subsequently cured.
- Sellers should determine if the company has a history of data breaches and carefully summarise the scope of the breaches, the company's responses and any material impacts on the business.

Acquisition agreements

Prudent purchasers and investors are factoring GDPR, UK GDPR and CCPA compliance into their acquisition agreement structuring and risk allocation mechanisms.

If the transaction is structured as an asset purchase, particular care will be needed to determine whether the transfer of the target's databases itself may violate the GDPR or the UK GDPR (eg, by exceeding the scope of the applicable consent or by transferring data outside of the EU or the UK to a jurisdiction that has not been deemed adequate by the European Commission or the applicable UK regulatory authorities, as applicable).

If the target is subject to the CCPA and the CPRA, particular care should be exercised to determine whether the transfer of any personal information qualifies as a merger or acquisition that is exempt from the definition of a 'sale' of personal information under the CCPA and the CPRA to ensure that consumer opt-out requests do not prevent wholesale transfers of personal information. Covenants may be appropriate to ensure continued compliance (or development of a compliance programme) or notification of any new breaches between signing and closing the transaction.

Risk allocation provisions should also be thoughtfully negotiated to ensure appropriate excluded liability, representation and indemnity coverage. Representations regarding compliance with law are insufficient to fully address data privacy risks and should be expanded to cover data privacy-related contract provisions, industry standards and practices, and the existence and handling of data breaches.

Among the representations that purchasers should consider are:

- operation in accordance with the company's written privacy policy;
- the provision of all applicable privacy and cybersecurity policies;
- the absence of written notices regarding related claims, investigations or complaints;
- the existence of a commercially reasonable information security programme;
- the absence of restrictions in respect of the target's successors' rights to use, sell, license, distribute and disclose personal data;
- the absence of breach notification obligations or notifications; and
- the absence of data security breaches, loss of data and unauthorised disclosures of personal sensitive information.

Practice tips

- In an asset deal, consider making GDPR, UK GDPR, CCPA and CPRA non-compliance, as applicable, an excluded liability. Include not only pre-closing operations, but also a reasonable period post-closing so that the purchaser has a covered window to bring the business into compliance.
- Depending on the duration between signing and closing, consider adding a covenant for the target to bring itself into compliance with the GDPR, the UK GDPR, the CCPA and the CPRA, as applicable, before closing. Purchasers that are operating companies with their own robust privacy programmes may prefer to simply onboard the target as part of post-closing integration.
- To the extent possible, as part of the larger deal dynamic, indemnities backing the related representations should be uncapped or subject to limitations of liability sufficiently high to cover the GDPR's and the UK GDPR's global revenue-based fines and the risk of significant private damages under the CCPA and the CPRA.
- If the purchaser is planning to rely on representation and warranty insurance, ensure that data privacy is not on the list of exclusions and carefully discuss with outside counsel the extent to which data privacy diligence should be conducted (as known liabilities are typically excluded from the scope of coverage, regardless of whether they are ultimately disclosed as part of the transaction agreement).
- Keep in mind that representation and warranty insurance, which is often capped at 10 per cent of the purchase price in the US, may be insufficient to cover fines under the GDPR or the UK GDPR. Purchasers should also be wary of material adverse effect definitions that exclude cyberattacks.

Post-closing

The post-closing process of transferring and integrating data can last up to several years, especially if the acquisition involves a business carve-out with related transitional services arrangements. During this period, either the seller or the purchaser may be required to continue data processing for the other. In those cases, the GDPR, the UK GDPR, the CCPA or the CPRA may require the incorporation of specific contractual provisions between the parties in the applicable transitional services agreement, whether structured as a controller–processor or controller–controller relationship.

After the transaction, the purchaser may wish to consolidate the target's data at the purchaser's existing data centres. If the transfers involve the movement of data outside the EEA or the UK, specific measures must be complied with if the recipient country has not been deemed adequate in respect of the protection of personal data by the EC or the applicable UK regulatory authorities, as applicable. The EC is in the process of negotiating additional adequacy determinations.

Purchasers should monitor regulatory determinations regarding transfers of personal data out of the EEA or the UK into the US, as well

as the relationship between the EU and the UK, to ensure that such transfers remain compliant with the GDPR's and the UK GDPR's obligations, as applicable.

Conclusion

Although they may have different geographic scopes, the GDPR, the UK GDPR, the CCPA and the CPRA represent major and impactful developments in a broader global trend towards stricter and more comprehensive data privacy and security regulation. As the implications of these regulations may impact all phases of a deal, a well-advised party would do well to keep in mind such considerations starting from the deal structuring stage through diligence, ultimate risk allocation and post-closing integration activities.

With the passing of the fourth anniversary of the GDPR's effectiveness, the EDPB, EU member state data protection authorities and the UK Information Commissioner's Office, among other agencies, continue to produce guidance and monitor the impact of the GDPR (and the UK GDPR) on businesses, organisations and individuals. Companies should continue to monitor developments in the field as interpretation and enforcement trends in respect of these existing data protection laws, and any additional data privacy and security regimes on the horizon, continue to evolve.

Davis Polk

Clients turn to us for exceptional service, sophisticated advice and creative, practical solutions.

Davis Polk is an elite global law firm with world-class practices across the board. Industry-leading companies and global financial institutions know they can rely on us for their most challenging legal and business matters.

Learn more at **davispolk.com**.

davispolk.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-550-4