HOT PRIVACY ISSUES FOR 2022

Weil

JANUARY 2022

By Barry Fishley, Ruth Fisher and Victoria Dyer

We believe that the privacy issues arising from:

- the increased use of biometric and health data;
- the continuing impact of data subject access requests ("**DSARs**");
- the growing education technology market; and
- the importance of environmental, social, and governance ("**ESG**") considerations

will give rise to significant challenges in 2022 both in terms of privacy compliance but also the privacy aspects of M&A and private equity transactions.

Biometric and health data

Biometric data is personal data relating to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that person such as facial images. Accelerated by the COVID-19 pandemic, a growing number of organisations are processing biometric and health data, either on their own behalf or on behalf of their customers. For example organisations are increasingly using biometric data (such as retina or face scanning) to verify the identity of individuals, whilst many health technology providers are also using biometric data as part of machine learning processes.

Many data protection regimes impose greater obligations on organisations that process biometric and health data. Under the General Data Protection Regulation in the EU and the UK ("**GDPR**"), biometric and health data are categorised as 'special category data'. Organisations that process such data are required to identify a lawful basis for processing under Article 9 of the GDPR (such as explicit consent or necessary within the field of employment), and in many cases must conduct data protection impact assessments ("**DPIAs**") to identify and negate privacy risks prior to processing the data.

In addition, data protection authorities place an increased emphasis on compliance with data protection laws where organisations process biometric and health data. Non-compliance with these laws can result in hefty fines. For example, under the GDPR, data protection authorities can impose fines of up to up to €20 million, or 4 percent of total worldwide turnover for the preceding financial year - whichever is higher. In 2021, the US federal court approved a $650 million settlement in response to a class action lawsuit that was brought under the Illinois Biometric Information Privacy Act ("**BIPA**") for a company's failure to properly inform users that biometric identifiers were being generated, collected and/or stored, or of the specific purpose and length of time of such processing.

As a result of the different ways by which organisations use biometric and health data, there is growing complexity involved in assessing whether the organisation acts as a data processor or data controller in relation to its processing. For example, where an identity verification provider receives retina scan data from a bank which is its client, and processes it for the purpose of providing an identification service to the bank, it is likely to be acting as a data processor. Where the same provider uses the retina scan data for its own purposes, such as developing its machine learning technology, the organisation is likely to be categorised as a data controller.

Correct categorisation of processing activities as those of a data controller or a data processor is crucial as it determines the scope of an organisation's obligations under many data protection regimes. Under the GDPR, for example, controllers are subject to greater obligations than data processors, including an obligation to:

i. maintain more comprehensive records of processing activities than data processors;

ii. comply with Article 13 (which details the information that must be provided where personal data is collected from the data subject) or Article 14 (which outlines the information to be provided where personal data has not been obtained from the data subject) of the GDPR;

iii. conduct DPIAs to identify risks arising out of the intended data processing and to minimise these risks prior to the processing; and

iv. notify the relevant privacy regulator and/or individual data subjects of a personal data breach if the breach is likely to have an impact on the individual's privacy.

Key Takeaways:

- Controller or processor? From a compliance perspective, organisations need to ensure that they correctly categorise themselves as a data processor or a data controller in relation to specific uses of the data. It is also important to ensure that there is sufficient transparency of the purposes of use. For example, by making it clear that data will be used for machine learning or similar purposes. Processing such data for purposes that are outside the individual's reasonable expectation (because they are not mentioned in the organisation's privacy policy and/or terms of business) will increase the risk of complaints and/or regulator action given the heightened sensitivity of such data. Within the context of an M&A transaction, it is important to determine whether the target business is aware of this distinction between controller and processor

and whether the target has the necessary privacy policies and contractual provisions in place that provide the required level of transparency.

- M&A: As mentioned above, the risk profile is increased where the target processes biometric and health data. Accordingly, comprehensive due diligence of the target's privacy compliance will be essential in assessing the likelihood of future enforcement action by data protection authorities. It will also help to identify additional work that may need to be undertaken by the target to improve compliance after closing. Underwriters will also look closely at data protection compliance, particularly where biometric or health data is involved, and will be reluctant to provide warranty and indemnity insurance cover if they feel that privacy due diligence has not been comprehensive.

Data Subject Access Requests

DSARs give individuals the right to access and receive a copy of their personal data which is held by organisations and the right to know how and for what purposes it is being used. They are becoming increasingly burdensome to organisations in light of the inclusion of these rights within global data protection regimes and increasing public awareness of such rights. Furthermore, a growing number of organisations, located in the US in particular, are seeking to commercially benefit from issuing DSARs, purportedly on behalf of date subjects. We anticipate the trend to spread to the UK and Europe in 2022 - a concern for companies in the region given that research indicates that UK businesses are already spending between £72,000 to £336,000 on DSARs annually.

DSARs can be particularly difficult for organisations to deal with due to the time and effort involved in locating and extracting the relevant personal data, and organisations can often fall short of their obligations. This may expose them to risks such as legal action, monetary penalties and reputational damage. To mitigate these risks, businesses are increasingly employing measures such as the use of template forms, standardised technical processes and employee training to help streamline the process and reduce cost and management time.

In the context of an M&A transaction, the existence of multiple outstanding DSARs will increase the data privacy risk profile of the target business. In addition, a relatively high number of DSARs may indicate wider underlying employee issues as DSARs are often used by disgruntled employees as a tool to obtain evidence from their employers when they have employment law disputes.

Given the cost, time and difficulty involved in responding to DSARs, the UK government recently launched a consultation ('Data: a new direction') which analysed the current regime in the UK in relation to DSARs. The consultation considered whether: (i) the 'manifestly unfounded' threshold for refusing DSARs was too high; (ii) the introduction of a cost limit and the amendment of the time limit for a response (currently one month) would help organisations in responding to DSARs; (iii) the government should reintroduce a nominal fee for processing DSARs; and (iv) there were any alternatives that would benefit organisations in reducing the cost and time taken to respond to DSARs. The consultation has since closed, and the government is expected to publish its response in spring 2022. Depending on the outcome of the consultation, changes to the UK data protection regime in this area may be on the horizon.

Key Takeaways:

- Streamline procedures: From a compliance perspective, businesses should implement procedures, such as the use of templates, technology measures and staff training, to ensure that DSAR processes are efficiently managed.
- M&A: The prospective buyer should determine whether the number of DSARs is out of step for the sector/industry, which may indicate wider systemic issues. This is particularly material for B2C businesses that process high volumes of customer/user personal data.

Education Technology

Interest in the area of education technology (often referred to as "**Edtech**") has been accelerated by the COVID-19 pandemic following government-imposed school closures and the implementation of remote learning methods that pivot around technology. A survey conducted by PwC in 2020 indicated that 83% of 102 venture investors surveyed saw Edtech as the sector with the greatest opportunity for future growth.

Edtech providers whose end users are children will typically be subject to additional obligations under data protection laws. For example, Article 8 of the UK GDPR requires that, where an organisation relies on consent to process the personal data of a child below the age of 13, processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. In such instances, the controller must also make reasonable efforts to verify that the consent has actually been given by the holder of parental responsibility over the child. In the UK, Edtech

providers will also be subject to the UK's Information Commissioner's (being the UK's privacy regulator) 'The Children's Code'.

Key Takeaways:

- Compliance: Where the education technology is used by children, the business will need to comply with additional data protection regulation, and where applicable, ensure appropriate consent has been obtained to process children's personal data.
- M&A: In the context of an M&A transaction, the target's awareness of and compliance with privacy laws concerning children and the sharing of user data (for example where users connect and share information on the target's platform) are areas that should be specifically investigated.

ESG

ESG considerations now have ubiquitous influence in an organisation's governance and long-term value and resilience. ESG considerations commonly include matters such as compliance with data protection laws and within this context, the handling of diversity data and compliance with internal privacy and data policies and practices are key. Ensuring that an individual's data protection rights are upheld is a 'social' concern, whilst ensuring that organisations comply with applicable data protection laws to mitigate their impact on individuals' rights requires appropriate data governance.

As part of an organisation's focus on ESG considerations, diversity data is often collected to allow the organisation to better understand workforce characteristics. Information collected may include ethnic identity, sexual orientation, disability status and gender identity. Such data is classed as special category data under the GDPR, and more onerous obligations will apply to its processing. For example, in the UK and EU, organisations are not able to rely on legitimate interest as a basis for processing special category data.

Key Takeaway:

The key trend we believe will continue this year is the need for organisations to be able to process and share with third parties (such as investors and other stakeholders) the personal data in line with their ESG commitments and aspirations. This may require privacy policies and employee privacy notices to be amended so that this type of personal data can be lawfully collected and shared, even on an anonymised and aggregate basis.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Ruth Fisher	View Bio	ruth.fisher@weil.com	+44 20 7903 1483