DATA USE
PROTECTING A CRITICAL RESOURCE

Nick Pantlin, Andrew Moir, Christine Young, Miriam Everett and Claire Wiseman of Herbert Smith Freehills LLP consider the key issues for businesses in the use and protection of data.

Described by some as the "new oil" for the digital economy, there is no doubt that data are now seen as critical for organisations to succeed. Data are a powerful and lucrative fuel for productivity. If not adequately protected, data are vulnerable to leaks that can cause widespread damage, and their true value is only realised once they have been processed and refined. They are, however, an almost infinite resource when compared with the finite supply of oil.

Data affect all businesses and industries, and dealing with data is an issue for the whole business as it affects every team within an organisation. This article examines:

- Market trends in the ballooning use of data worldwide.
- Some of the legal implications of dealing with data, particularly in light of the General Data Protection Regulation (*679/2016/EU*) (GDPR) which will apply from 25 May 2018, including in particular, GDPR compliance, cyber security and employee monitoring.

DATA AS A CORE ASSET

There has been a real shift in the market regarding data over the last few years. Data have always existed but, in our current digital age, the use of data has now become the core lubricant of global trade.

The rapid emergence of new innovative technologies and the digitisation of businesses have enabled the greater collection of data and, crucially, the ability for organisations to better interrogate and analyse that data in order to drive business and extract value.

According to an IBM report, 90% of the world's data were collected in the last two years and a staggering amount of data is produced on a daily basis (*www-01.ibm.com/software/in/data/bigdata/*). As more connected devices are becoming sources of data, from thermostats to cars, the majority of activities and communications leave a data trail from which organisations can amass an enormous pool of information, including behavioural patterns and preferences. In turn, the commercial value attributed to data has increased dramatically as organisations strive to use that data to predict and respond to customers and market influences in ways that were not previously thought possible.

It is therefore no surprise that data are starting to become the cornerstone of an organisation's strategy and one of the most effective tools with which to build a new information-driven business model, and through which to help a business grow. By cementing data analytics in all aspects of their business, organisations have the

potential to differentiate themselves from competitors that are less astute in their use of data. The ongoing analysis of that data in real time enables a far more agile business which, in turn, transforms business processes and supply chain models, aids innovation, saves time and money, manages risk and assists with making smarter, more strategic decisions.

When data from existing customers are used to tailor and improve a service, the service itself improves, which attracts more customers. This, in turn, generates more data to help further improve the service and, over time, the service continues to become more intelligent through the use of automated machine-learning technology. This so-called "data-network effect" can give organisations a further advantage over competitors.

DISRUPTIVE DATA

According to The Economist, data are to this century what oil was to the last one; that is, a driver of growth and change (*www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy*). In the same way as digitisation, no sector is immune from data's disruptive effect.

Organisations, particularly in consumer-facing retail sectors, have been able to engage better with their customer base through novel, more targeted offerings across all aspects of a consumer's retail experience. Even more traditional sectors, such as energy, mining and real estate, have been able to reap the benefits of data, from the use of big data analytics technology to speed up extraction or screen huge geoscience data sets, to the rise of smart meters and smart buildings (*see feature article "Big data: protecting rights and extracting value", www.practicallaw.com/1-595-7246*).

Commentators have suggested that data are giving rise to a new economy. Initially described as a "new asset class" at the World Economic Forum in a report published in 2011, the EU Commissioner for Competition, Margrethe Vestager, also referred to data as a "new currency" in 2016 (*www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf; https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en*). However, attributing a value to that currency is less clear cut for a number of reasons. Individuals are willing to trade their data for free access to a service, product or website in a way that they have never done before. Data tend to generate value indirectly, with their power harnessed by the technological tools through which they are processed. There is also not necessarily a correlation between the volume of data and their value. The disruptive effect of data therefore forces reassessments of traditional notions of trade and economic exchange.

The recognition of data as a core asset has sparked new global trends in mergers and acquisitions as companies look to buy other companies simply to ensure access to this valuable asset or to the underlying technology to realise that value. Determining the control and ownership of rights in data is also not without its challenges as it is not possible to own data under English law. Instead, organisations rely on protections under intellectual property rights, database rights (particularly for more structured systematically arranged data sets), confidentiality, and strategic contractual arrangements on matters such as access and usage rights. The purchase of a company often allows organisations to take advantage of an established legal framework, rather than venturing into the complexities of separating out a data asset and buying it in its own right.

Data also form an integral part of the UK government's current Brexit negotiations with the EU (*see Briefing "Brexit and data protection: between a rock and a hard place", www.practicallaw.com/2-628-4586*). The government has reiterated the crucial economic importance of the uninterrupted cross-border flow of data to any future partnership with the EU. According to the government's position paper on personal data, the European Commission (the Commission) valued the EU data economy at an estimated €272 billion in 2015, with the figure forecasted to rise to €643 billion by 2020 (*www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf*).

REGULATORY BALANCING ACT

There is, however, a sting in the tail. Just because technology unlocks new opportunities for organisations to innovate with data, it does not mean that the law will allow it. The use of data introduces significant new risks and challenges for a business to navigate within the relevant regulatory landscape. These are amplified by the scale of big data-related activity and the potential harm to individuals. It is therefore unsurprising that data have caught the attention of various regulators.

The digital economy relies on the trust of consumers to engage with it. Alongside the benefits of convenience and better alignment of products with consumer needs, individuals have a growing expectation of privacy. This expectation is no doubt compounded further by the high-profile and damaging data breaches coming to the fore. A prime example is the Equifax data breach reported in September 2017, where the credit reporting agency disclosed that cyber attackers gained unauthorised access to the personal information, and in some cases the credit card details, of 143 million US individuals.

The tension between innovation and regulation, including the competing fundamental human rights of privacy and freedom of expression, is not easily resolved. Balancing the two concurrently is something that regulators have been grappling with and will continue to do so. As ever, technology and innovation are evolving faster than the frameworks to regulate them. The increasing pervasiveness of technology is mapped by a corresponding rise in the relevance of data protection, privacy and cyber security regulation in particular.

EU reform

Given that the Data Protection Directive (the Directive) (*95/46/EC*) was first established in 1995, long before the internet became a feature of our everyday lives, the existing regime was certainly ripe for reform and the GDPR is the tool to tackle it (*see feature article "General Data Protection: a game-changer", www.practicallaw.com/2-632-5285*). Reportedly the most heavily lobbied piece of legislation in European Parliament history, from 25 May 2018 the GDPR will apply to all organisations established in the EU or offering goods or services to individuals in the EU or monitoring their behaviour.

It will replace the Data Protection Act 1998 (DPA) in the UK and GDPR standards are expected to continue to apply to the UK following Brexit through a combination of the new Data Protection Bill and the European Union (Withdrawal) Bill 2017-19 (*see News briefs "Data Protection Bill:*

aspiring to equivalence", www.practicallaw.com/w-011-0503 and "EU (Withdrawal) Bill: the first step down a long road", www.practicallaw.com/w-009-3199).

The GDPR provides an enhanced compliance framework and seeks to give individuals genuine choice and ongoing control over how their data are used. This is twinned with a technology-neutral approach and the legislation expressly provides for some of the novel concepts associated with the use of data, for example profiling and automated decision making (*see "Profiling" below*).

Competition law

Data are also starting to come onto the radar of competition authorities, giving rise to questions as to the circumstances in which competition laws can or should apply and whether the existing competition law rules can keep pace with technological innovation. Data and access to data can play a role in competition analysis where it is a relevant parameter of competition. However, some commentators question the applicability of existing competition regulation due to the potential for data to be replicated and acquired from a range of sources.

There is currently no EU case law that prohibits controls on data in merger cases; in fact the Commission has found in various cases that the combination of two parties' data did not raise sufficient concerns to block the mergers. The Commission has also stated that the protection of privacy is outside the scope of merger control except when it is a relevant factor of competition. However, competition authorities remain vigilant; for example, the German competition authority is investigating whether a potential breach of data protection by Facebook is also an abuse of dominance as an unfair term imposed on consumers. As data become the new global currency, their regulation is likely to remain a high priority for competition authorities.

Sectoral regulation

Overlap and possible conflict between data protection legislation and sector-specific regulatory regimes can add another layer of complexity. For example, the recast Markets in Financial Instruments Directive (*2014/65/EU*), which came into force on 3 January 2018, imposes more stringent record-keeping requirements on financial institutions, requiring them to store recordings of pertinent telephone conversations and electronic communications for five years or, potentially, up to seven years if requested by competent authorities (*see feature article "MiFID II and MiFIR: challenges ahead", www.practicallaw.com/w-010-7941*). Financial institutions will also need to consider this obligation in light of the key principles of proportionality, necessity and data retention limitation set out in the GDPR.

Similarly, with the extension of the Senior Managers and Certification Regime to all financial services firms rather than just banks, the enhanced regulatory reference obligations mean that regulated firms will need to retain certain data on departing employees for longer than anticipated under the GDPR (*see Briefing "Senior managers and certification regime: the first year", www.practicallaw.com/1-639-3048*). Overlapping regulatory regimes are also relevant in the context of a cyber attack (*see "Cyber security" below*).

Only time will tell where the balance sits in the regulatory tug of war. However, regulatory considerations remain key when developing any commercial strategy around data and these go beyond just specific data protection legislation.

GDPR COMPLIANCE

The key to GDPR compliance is not just in satisfying a checklist of requirements; it requires a business-wide effort to change an organisation's attitude and operational approach to data protection, privacy and cyber security compliance, as well as the way in which compliance pervades an organisation.

This is embedded in the accountability principle, which makes controllers expressly responsible for demonstrating that they comply with the data protection principles. While risk can be outsourced to others in the supply chain, overall statutory responsibility cannot be outsourced. The principle runs through the various provisions of the GDPR and represents a change in mindset towards data protection that can help organisations future-proof their businesses going forward.

Another key principle is transparency; that is, ensuring that individuals are aware of how and why the organisation is processing their personal data. The GDPR also gives statutory recognition to best practice concepts such as privacy and security by design and default by requiring controllers to think about privacy and cyber security at the inception of projects and system designs.

The increased sanctions regime under the GDPR has no doubt been a major catalyst in forcing organisations to focus on data protection and cyber security risk management. It is also a primary reason that data protection and cyber security have been elevated to board-level issues in the last 12 to 18 months. With maximum fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater, for certain breaches, the current monetary penalties of up to £500,000 under the DPA pale into insignificance.

Businesses can take some comfort from the fact that the Information Commissioner's Office (ICO), the UK data protection authority, has indicated that issuing fines will continue to be used as a last resort and top-level fines will not become the norm, in line with current practice. However, the prospect of the new penalties gives rise to a very different risk assessment for organisations. In addition to financial penalties, organisations also need to consider the equally significant risk of reputational damage for getting it wrong.

A successful implementation programme is therefore not simply a static strategy in the domain of a legal or compliance team; it is an evolving exercise and requires engagement from a range of other business functions across an organisation such as IT, cyber security, HR, compliance and procurement. Oversight and buy-in from senior executives, governance, training and ongoing review will also be fundamental to build a culture that ingrains privacy and these new principles in the fabric of an organisation and its overall strategy.

As well as the challenges that the GDPR brings, a well-run GDPR programme brings with it opportunities beyond simply achieving compliance. It goes without saying that it can build customer confidence and improve internal data handling. It is also an opportunity to consider a broader data transformation that could benefit a whole business by streamlining existing data management platforms to add value and lower costs and by bringing greater flexibility to be able to respond more readily to any future regulatory changes. In turn, this enables an organisation to better use its data and better engage with the new and exciting opportunities that emerging technologies will continue to generate.

With increased outsourcing to the cloud and other external third-party hosted services, as well as an increasingly complex supply chain for businesses, strategies for leveraging data also give rise to potential vulnerabilities and a range of risks that need to be understood and mitigated, particularly in the context of cyber security (*see feature article "Cyber security: top ten tips for businesses", www.practicallaw.com/3-621-9152*).

Notification requirements

The GDPR introduces a new requirement for all controllers to notify the appropriate data protection authority of a personal data breach; for example, following a cyber attack. This will include providing the regulator with a significant amount of information about the breach and marks a change from the present regime where notification to the ICO is not mandatory, although the ICO encourages notification for serious breaches (*see box "GDPR mandatory notification requirements"*).

Along with the increased sanctions, mandatory reporting is intended to act as an incentive to invest more time and resources in cyber security and IT resilience. Overall, for most controllers the changes simply codify good practice. However, controllers that attempt to conceal data breaches or delay notification without good cause will be putting themselves at risk of substantial sanctions.

Fines for breach of the fundamental principle requiring integrity and confidentiality of data through implementing appropriate technical and organisational measures are set at the maximum tier under the new sanctions regime (*Article 5(1)(f), GDPR*). Article 32(1) of the GDPR gives further guidance on security of processing. Controllers must also document all personal data breaches, comprising the facts of the breach, its effects and the remedial actions taken, so as to enable regulators to verify compliance with the Article 32 requirements (*Article 33(5), GDPR*). This is a prime example of the accountability principle in action.

When and how to notify

The Article 29 Working Party (the working party), a body which reflects the consolidated view of national supervisory data protection authorities in all EU member states, issued guidance in October 2017 which discusses the notification obligations and includes some worked examples of various types of breaches, including when notification is and is not required (the guidance) (*http://ec.europa.eu/newsroom/document.cfm?doc_id=47741*).

The obligation to notify without undue delay is triggered by awareness of a breach. The guidance clarifies that a controller can undertake a brief initial investigation to determine whether or not there is a breach and during this window it may be regarded as not yet being aware. Awareness of a processor, however, will also be deemed to be awareness of a controller as a processor has an obligation in the data processing agreement to notify a controller after becoming aware of a personal data breach (Article 33(2)). The guidance accepts that bundled notifications may be appropriate for multiple similar breaches. Where a failure to notify the supervisory authority also reveals the lack of adequate security measures, there is the possibility of two sets of sanctions.

The threshold for notification of affected individuals is deliberately higher, partly to protect individuals from notification fatigue. Notifications should be in dedicated messages to make communication of the breach clear and transparent, rather than being tacked onto a normal communication. Multiple channels of communication may be preferable in certain circumstances to maximise the chance of properly communicating information to all affected individuals.

It is not clear whether notification solely by a press release can ever be sufficient. This is because the guidance states that the data breach should be communicated to the data subjects directly, unless doing so would involve a disproportionate effort, in which case a public announcement or similar measure can be used. However, in contrast, the guidance also states that a notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual.

Overlapping requirements

Publicly listed companies and organisations in particular sectors are likely to be subject to overlapping regulatory obligations both in relation to data breaches but also other types of cyber security incident that do not involve personal data.

Therefore, a single cyber incident could trigger multiple sets of notification requirements. The impact and timing of these kinds of mandatory reporting requirements will add an extra dimension to the internal investigation that follows a significant cyber incident, forcing organisations to communicate promptly with regulators with a view to avoiding or mitigating any regulatory fine or public censure through appropriate compliance. A single incident can also give rise to multinational regulatory requirements including, for example, an obligation to notify data protection regulators in jurisdictions where data subjects are affected (*see box*

GDPR mandatory notification requirements

Under the General Data Protection Regulation (*679/2016/EU*) (GDPR), controllers will be required to notify:

- The data protection authority of a personal data breach which is likely to result in a risk to people's rights and freedoms (*Article 33(1)*).
- The affected data subjects when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (*Article 34(1)*). There is an exception in relation to those parts of the data which have been rendered unintelligible to unauthorised persons through the application of technical measures such as encryption or password protection measures, for example, so-called "salting and hashing".
- The data protection authority of a personal data breach without undue delay and, where feasible, not longer than 72 hours after having become aware of it. Although if the organisation does not have all the details available after 72 hours, it can provide more information subsequently. The content of a notification is prescribed in Article 34(2).

"Examples of overlapping notification requirements").

The practical position must also be considered. Competing notification obligations and timescales will often be dictated by the most stringent obligation. Similarly, if an incident is likely to become public through other means, for example, if a critical system is obviously offline, the need to report incidents is accelerated (*see News brief "Ransomware cyber attacks: lessons learned at last?", www.practicallaw.com/w-009-3512*).

As a general principle, it is often best to provide a regulator with a brief and factually accurate, but necessarily incomplete, notification shortly after the organisation becomes aware of the potential cyber incident, informing the regulator that further updates will follow as the assessment and investigation continues. This is preferable to the regulator's first knowledge of the data breach coming through media coverage or complaints from affected data subjects.

Security by design and by default

Data protection regulation in the UK has traditionally been principles based. The GDPR represents a move to a more prescriptive regime, particularly in relation to data security. This is shown, for example, in the concepts of privacy and security by design and default which require adequate security to be implemented at the start of a project as well as processing only the personal data necessary for each specific purpose of processing (*see "GDPR compliance" above*). This may sometimes present a friction between data protection requirements and future-proofing systems, for example, collecting data in case future types of processing require it.

Processors

Another significant change under the GDPR is that processors will have direct statutory obligations and liability for the first time, reinforced by proposed mandatory provisions in the contracts with the controller, rather than the parties having discretion to negotiate the provisions themselves. In particular, processors will be required to implement appropriate technical and organisational measures for cyber security, and to notify their controller without undue delay of any personal data breach, which is necessary for the controller to satisfy its own notification requirements (*Articles 28(1) and 32, GDPR*).

Examples of overlapping notification requirements

In addition to the reporting requirements of the General Data Protection Regulation (*679/2016/EU*) (GDPR), businesses may also be subject to other notification obligations, for example:

- The Network and Information Security Directive (*2016/1148/EU*), which is due to be implemented in the UK by May 2018, requires operators of essential services and, to a lesser extent, digital service providers, to report without undue delay security incidents that would have a significant disruptive effect on the provision of an essential service that they provide. This is expected to apply to larger organisations in the transportation, banking, financial market infrastructure, health and drinking water, electricity and digital infrastructure sectors.

- Firms regulated by the Financial Conduct Authority (FCA) are subject to obligations to notify it of cyber security incidents, under Principle 11 of the FCA's principles for businesses (the duty to deal with regulators openly and co-operatively and to disclose anything of which its regulators would reasonably expect notice). This could include where customer data are compromised or if a cyber incident affects the firm's ability to continue to provide adequate services to its customers.

- The E-Privacy Directive (*2002/58/EC*) requires operators of telecommunication networks and internet service providers to notify their data protection authority if they have suffered a personal data breach, which contrasts with the current position for most controllers under the Data Protection Act 1998.

- International notification requirements may apply. For example, the Monetary Authority of Singapore can require notification of incidents within one hour, making the GDPR's 72-hour notification period seem comparatively generous.

For many processors, this will amount to formalising existing good practice as controllers would ideally already seek to include similar obligations in their contracts with processors. There should be a clear contractual allocation of responsibility and liability for data protection and cyber security between a controller and its processors (and any sub-processors). It is also vital to encourage good practice through contractual terms and ensure co-operation in the event of a cyber incident, rather than focusing exclusively on liability.

The ICO produced draft guidance on appropriate contractual arrangements in September 2017 (the draft guidance) (*https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf*). The draft guidance reiterates the proposed mandatory terms to be included in contracts, including that the processor: must assist with notification obligations; must not employ another processor without authorisation; and should have appropriate technical and organisational cyber security measures. While this might entail a substantial exercise to revisit and amend existing contracts (known as repapering), it will also remove much of the present doubt over the scope of the obligations and liabilities of processors. In conducting the repapering exercise it may be necessary to prioritise immediate areas to be rectified based on proportionality and risk, in particular, determining any key or high-risk contracts to decide the most appropriate steps to take.

The draft guidance emphasises that controllers still have direct liability to data subjects for damage suffered regardless of the use of a processor unless they are not in any way responsible for the event giving rise to the damage, which is a high threshold (*Article 82(3), GDPR*).

Supply chains

Allied to the above is the need to conduct cyber security and data protection due diligence on service providers and contractors. In addition to the requirements mandated by the GDPR and any guidance, it is common practice to undertake a risk assessment of

each contractual relationship in the supply chain before imposing prescriptive cyber security, technical, legal and operational requirements on suppliers appropriate to that risk. When undertaking any repapering exercise in relation to the GDPR, it is also worth considering cyber security issues in parallel, to avoid the need to revisit each contract more than once, which may be resisted by a supplier (*see box "Supply chain assessment"*).

Supply chain assessment

Businesses should take into account the following issues when considering any cyber security and data protection issues with their suppliers:

- A combination of due diligence, contractual protections and co-operation with suppliers is needed to improve the business's cyber security and data protection.
- There needs to be clear contractual allocation of responsibility and liability for cyber security and data protection throughout the supply chain, both in relation to preventative measures and incident response, to engender good practice.
- Contractual protections should extend up and down the entire supply chain, ideally with consistent wording.
- The new sanctions regime in the General Data Protection Regulation (*679/2016/EU*) (GDPR), twinned with the fact that processors can be directly liable under the GDPR, has materially altered the risk assessment and negotiating position between controllers and processors.
- Businesses should scrutinise the force majeure provisions in contracts to determine how they affect liability for cyber security incidents.

EMPLOYEE MONITORING

The rise of intelligent technologies provides employers with increasingly sophisticated ways to monitor their employees (*see feature article "Employee monitoring: the value of being prepared", www.practicallaw.com/3-629-9945*). Employers are no longer focusing solely on equipment and data loss prevention, for example, by installing CCTV to monitor who accesses confidential materials; they now have the ability to monitor and analyse employees' professional performance, and even their health and lifestyle choices.

Employee monitoring policies can often be vague, alluding to a broad right of the employer to monitor and intercept employee communications without providing specific scenarios or details of safeguards. The DPA contains relatively few provisions regarding employee monitoring. However, recent case law developments, together with the focus on transparency that will come with the GDPR, should give employers pause for thought; not only will they need to be far more explicit about the employee monitoring they undertake, but they may find it tougher to justify certain monitoring activities (*Bărbulescu v Romania (61496/08) [2017] ECHR 742; see News brief "Workplace privacy: striking a balance", www.practicallaw.com/w-010-4936*). Employers therefore need to be smart about workplace monitoring.

Over the last decade, there has been a proliferation of wearable fitness technology, enabling individuals to track and analyse their every movement (*see Focus "Wearable technology: intellectual property and contractual considerations", www.practicallaw.com/9-620-5227*). Many employers, recognising that a healthy workforce is often a more productive one, have been keen to encourage this trend, for example by offering employees sociometric badges that monitor their sleep patterns. While ostensibly these badges are tools that benefit employees by helping them to improve the quality of their sleep, they have faced criticism from privacy campaigners and trade unions which are concerned that the data could be used in a way that adversely affects employees, for example, by making predictions about their work performance based on the amount of sleep that they get.

What is monitoring?

The ICO describes monitoring in the employment context as activities that set out to collect information about workers by keeping them under some form of observation, normally with a view to checking their performance or conduct. This could be done either directly, indirectly, perhaps by examining their work output, or by electronic means.

There is no formal definition of "monitoring" in either the DPA or the GDPR. In the context of the territorial scope of the GDPR, the recitals state that in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet, including potential subsequent use of personal data processing techniques which consist of profiling a natural person.

Legitimate interests

Traditional employee monitoring activities, such as reviewing emails with large attachments sent to external email addresses to ensure that sensitive information is not being improperly shared, may be justified under the GDPR as being within the legitimate interests of the employer to protect its confidential information. However, reliance on this basis needs to be considered carefully as it does not give employers carte blanche to carry out any form of monitoring (*for further background, see box "Processing employee data"*).

For more intrusive forms of monitoring, such as analysing employees' sleep patterns, the interests of the employee are likely to outweigh those of the employer, and so consent will most likely still need to be relied on.

Transparency

Under the GDPR, employees will have rights to greater transparency in relation to how their data are processed, and employers should amend their policies on privacy and the acceptable use of IT to reflect this. Fair processing notices must be accessible to all employees and be transparent about any employee monitoring taking place. If an employer wants to use employee data for a different purpose than that for which the data were collected, this needs to be clearly explained to the employee. In addition, employees should be informed of their right to object to this monitoring based on their employer's legitimate interests.

The importance of clarity and transparency with regards to employee monitoring was highlighted by the Grand Chamber of the European Court of Human Rights in *Bărbulescu,* where it held that employees have a reasonable expectation of privacy in the workplace. Where an employer wishes to monitor emails and messages, it must tell the employee that their communications might be monitored. In *Bărbulescu*, although the employee knew he was forbidden to use work computers for personal purposes, he had not been told that his employer was monitoring his communications. As a result, his employer had breached his right to privacy under Article 8 of the European Convention on Human Rights.

Profiling

Profiling is an advanced form of monitoring. It involves: the automated processing of personal data; and the use of those personal data to evaluate certain personal aspects relating to the individual, in particular, to analyse or predict certain aspects concerning his performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement. The term "automated processing" refers to decisions being made by a computer without any human intervention. An example of profiling would be using automated decision-making to filter out applicants for a job role based on their personal data, such as their exam grades, without any human intervention.

Under the GDPR, not only will employers have to inform candidates about the existence of this automated decision-making, they must also provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of the processing. This will require them to tell candidates how they operate automated decision-making, for example, to filter out those without at least AAB in their A-levels. The automated processing will either need to be necessary for the performance of a contract or the candidate's explicit and informed consent must have been obtained. The candidate should also be given the right to obtain human intervention, to express his point of view and to contest the decision.

The recitals to the GDPR explain that, when putting in place automated processing systems, organisations should also:

- Use appropriate mathematical or statistical procedures.
- Implement technical and organisational measures that are appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised.
- Secure personal data in a manner that takes account of the potential risks involved for the interests and the rights of the individual.
- Prevent discrimination on the basis of factors such as race, ethnic group, political opinion or health status.

The working party's guidance on profiling sets out a number of good practice recommendations for profiling such as producing layered notices for informing data subjects about how they are profiled, where they are informed about the processing of their data on a step-by-step basis (the guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251) are available at *http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083*). This type of approach can work by providing the key privacy information in a short notice, with links to expand each section to its full version, and a just-in-time notification at the point where the data are collected.

Carrying out a data protection impact assessment will also be necessary before starting any high-risk processing activities, such as large-scale, systematic monitoring of public areas (for example, by CCTV) or large-scale processing of criminal convictions (for example, as part of an employee onboarding process). Even if an impact assessment is not strictly necessary under the GDPR, it can still be a useful way to identify and minimise non-compliance risks.

Outside the workplace

Even in situations where an employer has decided that it considers a particular form of monitoring to be within its legitimate interests, there may still be pitfalls that it will need to navigate. For example, if an employer is concerned about a potential team move and resolves that it is within its legitimate interests to monitor the location of that team's company cars by a satellite navigation system to review whether they meet up or travel to a competitor's premises (and has referred to this type of monitoring in its fair processing notice), it should ensure that this tracking is turned off outside of working hours and is only monitored for as short a timeframe

Processing employee data

To process employees' personal data, employers must either obtain their employees' freely given, specific and informed consent or rely on one of the other legal bases for data processing provided under the General Data Protection Regulation (*679/2016/EU*) (GDPR).

Currently, most employers seek to obtain a general consent from employees to all forms of processing, usually through their employment contract. However, a potential concern with continuing to do so under the GDPR is whether consent can be truly freely given by an employee to their employer. Some commentators question whether an employee is able to exercise a real choice and avoid negative consequences if he does not consent. The Article 29 Working Party opinion on data processing at work suggests that an employee cannot consent freely (Opinion 2/2017 on data processing at work (WP 249) is available at *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=605266*).

Another consideration is that, once given, the GDPR permits consent to be withdrawn at any time and requires data subjects to be made aware of this. This potentially adds further complexity to an employer's administrative burden. These limitations are resulting in a move away from relying on consent to process employee personal data, and instead relying on one of the other legal bases, such as the "legitimate interests" basis. Under this basis, it could, for example, be in an employer's legitimate interest to install CCTV at its premises to help to prevent equipment and data theft, and ensure a secure work environment.

Related information

This article is at practicallaw.com/w-012-5424

Other links from uk.practicallaw.com/

Topics

Compliance: data protection	topic1-616-6178
Data protection: general	topic1-616-6550
Data security	topic8-616-6189
Data sharing	topic2-616-6187
Employee data and monitoring	topic5-200-0623
Financial crime	topic7-103-1182
GDPR and data protection reform	topic7-616-6199
Information technology	topic5-103-2074
Internet	topic8-383-8686
Policies and procedures: employment	topic9-382-7461
Privacy	topic6-383-8687

Practice notes

Overview of EU data protection regime (Data Protection Directive 1995)	8-505-1453
Overview of EU General Data Protection Regulation	w-007-9580
Overview of UK data protection regime	7-107-4765
Overview of data sharing arrangements	4-540-2009
Overview of cybersecurity	9-617-7682
Data security and data security breaches	5-524-2341
Developing a global privacy and data protection strategy	5-503-8585
Developing a UK data protection strategy	1-504-7756
Ensuring data protection compliance	0-107-4759
EU General Data Protection Regulation: implications for employers	6-624-3481
General counsel briefing: privacy and data protection	8-503-8126
General Data Protection Regulation: key provisions and what businesses should be doing now	1-619-6000
Protecting confidential information: overview	8-384-4456
Managing cybersecurity risk and compliance	6-615-8326
Monitoring email and internet use of employees	3-200-4245
Service providers, security and data breach notification	5-549-7832

Previous articles

Cross-border transfers of data: changing times (2016)	3-627-7769
Cyber security: top ten tips for businesses (2016)	3-621-9152
Cyber risk and directors' liabilities: an international perspective (2016)	2-635-5748
Employee monitoring: the value of being prepared (2016)	3-629-9945
General Data Protection: a game-changer (2016)	2-632-5285
Big data: protecting rights and extracting value (2015)	1-595-7246
Data transfers in the cloud: the struggle for compliance (2014)	8-581-9685

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

as possible. Failure to do this would go beyond the employer's legitimate interests and may breach the employees' reasonable expectations of privacy.

Employers face a similar problem with their policies on employees bringing their own devices to work, which regulate how employees can use their personally owned devices in the workplace to access sensitive company information and applications (*see Briefing "Bring your own device: responding to the trend", www.practicallaw.com/7-530-5276*). Any monitoring of these devices should, according to the working party, be turned off when the employee is not using the device for work purposes, which is likely to cause logistical difficulties for employers (the working party's Opinion 2/2017 on data processing at work (WP 249) is available at *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=605266*).

As explained in *Bărbulescu*, fair processing notices should be clear about precisely when the employer considers it within its legitimate interest to monitor employees. Employers should also ensure that their fair processing notice interacts with other employee-facing policies. For example, in the context of an investigation into employee misconduct, where employees had been communicating through the WhatsApp Messenger app on company-owned devices, it would be in the

Monitoring issues in Germany and France

It has been a matter of ongoing debate in Germany whether, and under what circumstances, employers that allow their employees to use their email systems for private communications could be viewed as telecommunications providers under the German Telecommunications Act. Monitoring of email or internet use by a telecommunications provider is unlawful and could potentially lead to criminal liability. The general view is that employers that allow the private use by employees of internet or email in the workplace qualify as telecommunications providers. In light of this, German employers tend to state in their privacy policies that the use of their business network to access private email and the internet in the workplace is prohibited. Some of them offer their employees a separate, non-networked wifi connection that can be used for private email and internet use.

In France, where there has been a collective agreement with a representative trade union for at least two years, the trade union is permitted to post publications on a trade union site which are accessible through the company's intranet and to use the company email system to communicate these publications to employees (*Article L.2142-6, Labour code*). The employees must be informed of this possibility in order to consent to or refuse the communications. The employer must ensure the confidentiality of all exchanges between employees and the trade union; the employer cannot, for example, control the distribution lists for trade union emails.

employer's legitimate interest to review certain of these WhatsApp messages. However, the existence of this legitimate interest needs to be made clear to employees in the company's fair processing notice, and the company's policy on the acceptable use of IT should state that apps should not be downloaded for personal use and, if they are, they will be subject to monitoring (*see box "Monitoring issues in Germany and France"*).

Risks of breach

In addition to the significant penalties under the new GDPR regime, employees can bring an action against an employer for damages suffered as a result of processing carried out in breach of the GDPR, including for injury to feelings and distress (*see "GDPR compliance" above*). This may not give rise to a large amount on an individual basis, but if the employees bring a group claim, the potential liability could be significant, as has been seen with the supermarket chain, Morrisons, which in December 2017 was found vicariously liable for the criminal actions of a former employee in the UK's first ever successful group litigation arising from a data breach (*see News brief "Vicarious liability for data breach: going rogue", this issue*).

In scenarios where employee monitoring has produced evidence of employee wrongdoing, if the evidence has been obtained in breach of the DPA or GDPR, the court or employment tribunal has the discretion to exclude that evidence in any legal proceedings.

Nick Pantlin, Andrew Moir and Christine Young are partners, Miriam Everett is a consultant, and Claire Wiseman is a senior associate, at Herbert Smith Freehills LLP.