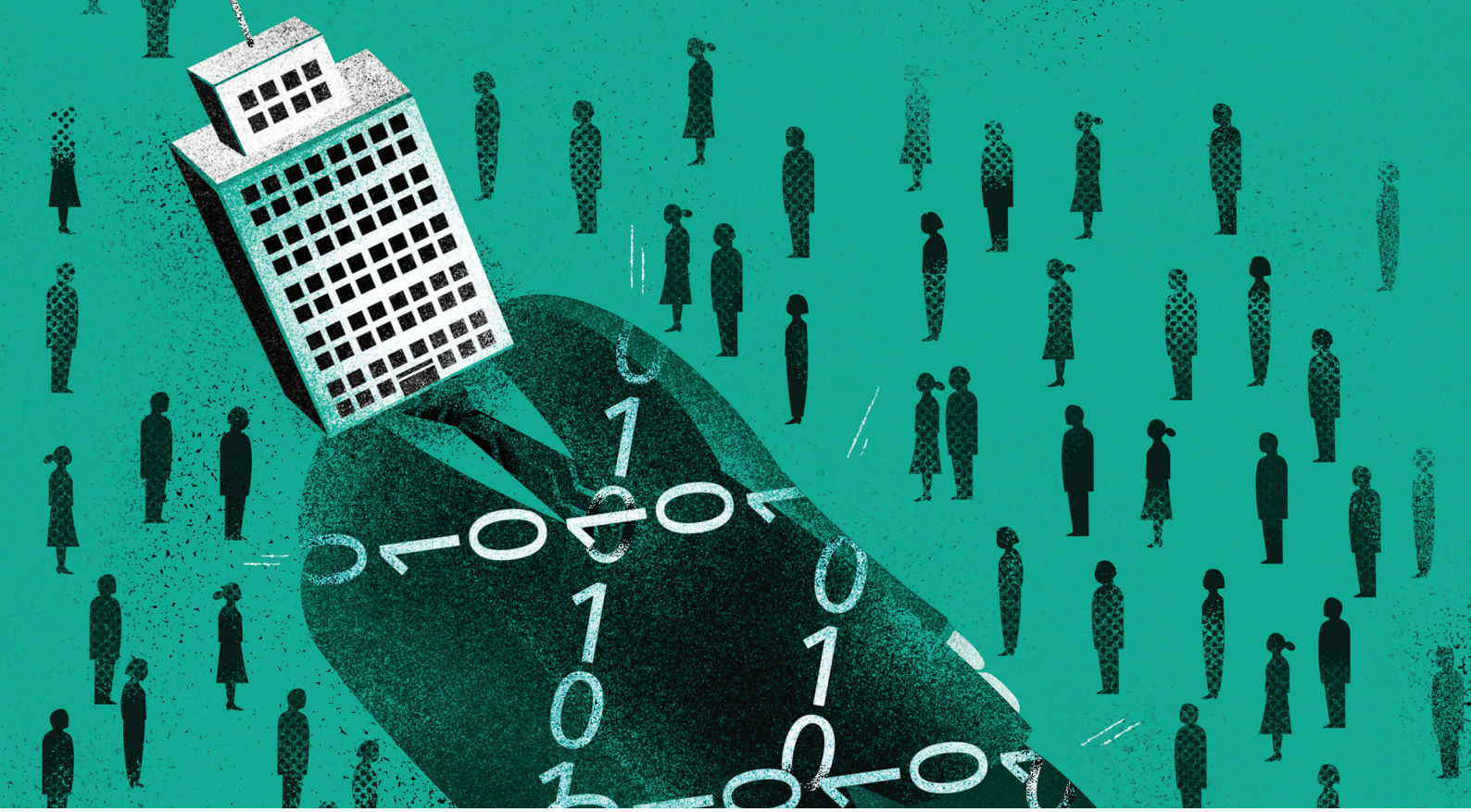

CYBER INCIDENTS
MANAGING THE EMPLOYEE FALLOUT

Khurram Shamsee, Nicola Geary and Eleanor Ludlam of DAC Beachcroft LLP look at the key practical and legal considerations for employers in their capacity as data controllers when dealing with ransomware attacks and other cyber incidents.

In a recent poll of risk management experts, cyber incidents were identified as the biggest business risk for 2022 (*www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html*). The threat of ransomware attacks and data breaches concerns companies even more than business interruption or another pandemic outbreak.

Rarely out of the headlines, one of today's most disruptive forms of cyber incidents is ransomware attacks involving large-scale data exfiltration, where criminals threaten to publish the data unless a ransom is paid. Sensitive details relating to employees working at the targeted organisation often form part of the compromised data set.

This article looks at the key practical and legal considerations for employers in their capacity as data controllers when:

- Preparing for a cyber incident.
- Managing the initial incident response phase.
- Dealing with the longer term fallout from a cyber incident.
- Considering what forms of redress employees might seek.

CYBER INCIDENTS

A cyber incident is a security breach that affects the confidentiality, integrity or availability of personal data. These incidents have increased significantly in recent years, with attacks becoming ever more prevalent for businesses of all sizes and not just those in the public eye.

Generally, cyber incidents are sector agnostic, however certain sectors have been particularly targeted more recently, such as the charity, education and professional services sectors.

It has been estimated that if it were measured as a country, cyber crime would be the world's third largest economy after the US and China (*www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf*).

Methods of attack

Cyber incidents can take many different forms, from the deployment of malware on a company's systems, to phishing attacks and denial of service attacks. While business email compromise attacks were the more prominent form of attack until around two years ago, the most common incident seen now is ransomware, which is the primary focus of this article (*see News brief "Ransomware cyber attacks: lessons learned at last", www.practicallaw.com/w-009-3512*).

The tactics of the cyber criminals have also evolved, notably in relation to ransomware attacks. While, previously, cyber criminals would encrypt files and demand payment

in return for a decryption key, they are now carrying out large-scale exfiltrations of data with the threat to leak it publicly unless a ransom is paid. There has also been an increase in the pressure being exerted by cyber criminals on the relevant decision makers within the company's leadership, with telephone calls being made to board members, employees and clients alike, informing them of the cyber incident and asserting that data has been taken.

Inevitably, the transition to homeworking when the COVID-19 pandemic first struck exposed vulnerabilities in companies' IT infrastructure, with weaker controls on home IT systems and many businesses changing security settings in order to facilitate remote access (*see feature article "Homeworking in the wake of COVID-19: issues for employers", www.practicallaw.com/w-027-8073*). With remote working becoming far more prevalent today, it is clear that vulnerabilities will need to be remedied, if they have not already, otherwise a business leaves itself exposed to a cyber attack, with potentially crippling consequences.

Cyber attacks also now play a role on the international stage. Many businesses have been operating on high alert following the recent unrest in Ukraine and in light of warnings that have been issued by the National Cyber Security Centre that recommend taking action to improve resilience. While there are no known, specific threats to UK organisations at the time of writing, there have been cyber attacks against Ukrainian institutions that have resulted in international consequences. For example, the deployment of HermeticWiper, a wiper malware used against Ukrainian organisations which erases data from the hard drive of an infected computer, has the potential to affect organisations outside of Ukraine.

HR issues

From an HR and people management perspective, there is invariably a connection between cyber security issues and people issues. For example, a ransomware attack frequently involves the compromise of employees' personal data, and a system security issue could be the result of an employee's advertent or inadvertent actions. Therefore, grappling with the people issues is an integral part of any organisation's cyber incident response plan.

PRE-INCIDENT READINESS

Employees play a crucial role in preventing and identifying cyber incidents. Whatever the size of the organisation, employers should consider proactively taking a number of steps to guard against cyber security breaches occurring and mitigate their consequences.

Staff training and awareness

Employees are the first line of defence in a cyber incident. According to the government's 2020 cyber security breaches survey, 63% of breaches or attacks were spotted by members of staff, while antivirus or antimalware programmes identified only 7% of incidents (*www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020*). Therefore, the most important step that an employer can take in relation to its workforce is to train staff to identify and report cyber breaches promptly.

Staff should be trained on how to identify and handle suspicious emails, and how to react in the event of a breach. Training should also focus on the organisation's cyber security and data protection policies and procedures, which could cover a range of features such as the appropriate use of IT, remote working and document management systems, and what can be stored on removable devices. This training typically forms part of an employee's induction, but it should also feature in refresher training courses so that the principles are regularly reinforced. Staff can also be tested, such as through simulated phishing exercises or tabletop workshops, to gauge how they respond in a mock scenario and to test the company's overall resilience to an attack targeted at employee error.

Mapping HR data

Understanding the organisation's framework for storing and processing employee data is vital. This knowledge is critical during the assessment, containment and recovery stages in the aftermath of a cyber security attack where employee personal data forms part of the compromised data set. The mapping analysis should include:

- The categories of employee personal data, including special category personal data, held by the organisation.
- On what systems the data is held and who can access it.
- The purposes of the data processing.
- The categories of recipients of employee personal data, including details of international transfers.
- The technical and organisational security measures in place in relation to the data.
- Applicable retention periods (*see below*).

Retention issues

The principle of storage limitation, that data is held for no longer than is necessary for the purposes for which the personal data is processed, is a fundamental element of the data protection regulatory framework (*Article 5(1)(e), the retained EU law version of the General Data Protection Regulation (679/2016/EU)*) (UK GDPR). It means that information that is no longer needed should be promptly and securely deleted.

As well as the compliance and commercial risks of failing to adhere to the storage limitation principle, there are a number of increased risks from a cyber security perspective:

- The retention of personal data is inherently linked to security risks; the more personal data that is retained, the more there is to lose or to be stolen.
- The Information Commissioner's Office (ICO) is more likely to take enforcement action against an organisation that has suffered a cyber incident if the organisation is also non-compliant with the storage limitation principle (*see box "Cathay Pacific ICO fine"*).
- There are reputational risks if it comes to light that the personal data had been retained for longer than necessary before it was lost or stolen.
- It is harder to notify affected individuals about the breach if contact details are out of date.
- The costs of responding to a cyber incident can increase if an organisation is holding data that it no longer has a justification to retain. For example, when it comes to mining the affected data set to ascertain the affected individuals and associated data elements, the greater the amount of data to be reviewed, the higher the mining costs.

Specific time limits for retention are not prescribed in the UK GDPR or other UK data protection laws, and it is for the data controller to determine the period that it considers to be appropriate for each document category based on its processing purposes. In terms of HR records, the general principle is that employers should purge data during employment and in a reasonable period following termination, unless there is a specific reason for the data to be retained. Relevant considerations for determining retention periods include:

- Whether any mandatory retention periods apply, for example, six years from the end of the relevant tax year in relation to wage and payroll records, or three years after the end of the pay reference period in relation to working time records.
- Regulatory requirements, such as the regulatory reference regime under which a firm should retain records that are relevant to the assessment of an individual's fitness and propriety for at least six years after termination (*see Briefing "Senior managers and certification regime: another year on", www.practicallaw.com/w-013-8923*).
- The applicable limitation periods for possible claims, which, in the employment context, are three months for statutory claims and six years for contractual claims.
- Underlying business needs.

In addition, employers should be wary of keeping special categories of personal data for long periods of time without a robust business requirement and enhanced security measures.

Reviewing HR documents

HR contracts, policies and procedures should be reviewed and updated from time to time to ensure that they include appropriate preventative and protective measures from a cyber security perspective. One of the most important policies in this regard is an organisation's record retention policy, which needs to be accurate and implemented effectively (*see feature article "Information governance: surfing the wave or drowning?", www.practicallaw.com/7-386-1696*). The following are also important and will be relevant in the event that an employer needs to take action against an individual due to a cyber security breach:

- Confidentiality clauses and post-termination restrictive covenants to prevent current and former employees from disseminating confidential information about the organisation, its business partners and clients (*see News brief "Non-disclosure agreements: time for straight talking", www.practicallaw.com/w-024-1619*).
- Information technology policies, such as IT acceptable use policies or electronic communications policies, or other data protection policies.
- The information security clauses in hybrid and homeworking policies (*see News brief "Hybrid working after COVID-19: home is where the work is", www.practicallaw.com/w-031-0840*).
- Bring your own device (BYOD) policies, if appropriate.
- The definition of misconduct offences, which is typically included in an employee handbook, to include deliberate, reckless or negligent data breaches.
- Introducing or reviewing protocols or standard procedures for responding to data subject rights to streamline these processes; for example, in relation to data subject access requests (DSARs).

Monitoring

Organisations can employ a variety of tools to increase the security of their networks. Tools that involve the monitoring of employee activity must comply with applicable laws and related guidance for monitoring (*see box "Employee monitoring and data protection"*). In particular, the monitoring must be proportionate to the employer's legitimate interests in conducting the monitoring (*see feature article "Employee monitoring: the value of being prepared", www.practicallaw.com/3-629-9945 and News brief "Workplace privacy: striking a balance", www.practicallaw.com/w-010-4936*). Systematic, routine monitoring for the purpose of identifying cyber risks is likely to be justified from a proportionality perspective given the materiality of these risks.

Employers commonly use data loss prevention software to detect and block certain information from leaving the corporate network. If using this software, employers should provide a level of transparency to employees by confirming the applicable triggers, or categories of triggers, that will generate a block or alert.

INCIDENT MANAGEMENT

It is important that organisations have effective processes in place to help detect, investigate, assess and record any breaches that they experience, as cyber attacks are often intentionally perpetrated at times when responding to them is more difficult, such as during weekends or on public holidays.

It can sometimes take weeks following a cyber incident to identify the affected data subjects, including employees, and the relevant personal data that has been compromised. The initial incident response steps include containment of the incident, recovery, assessment of legal and regulatory obligations, notification to applicable regulators and, on conclusion, evaluation. The containment and recovery phases can take some time to progress, particularly

Cathay Pacific ICO fine

In October 2018, Cathay Pacific Airways Ltd reported that it had suffered a large-scale data breach exposing the details of 9.4 million customers, including passport details and travel history.

In March 2020, the Information Commissioner's Office (ICO) found 12 contraventions of data security, including that Cathay Pacific's retention periods relating to loyalty scheme data were too long. The loyalty scheme data was retained indefinitely and only purged after seven consecutive years of inactivity, with passengers becoming inactive only on request or death (*https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf*). The ICO imposed a penalty of £500,000, which was the maximum penalty at the time.

with a large-scale and complex ransomware incident. While cyber criminals may provide a file directory tree or similar, it may take time to ascertain what data sits behind that and to then undertake data mining. Any downtime can be used to plan aspects of the HR response.

Triaging HR issues

Early consideration should be given to relevant HR issues, including:

- Whether to add an HR representative to the core incident response team.
- Asking members of the core incident response team to sign non-disclosure agreements.
- Considering whether existing resources are sufficient to deal with the incident or if steps should be taken to temporarily increase resources. According to the 2021 cyber security breaches survey, almost 40% of organisations reported needing extra staff time to deal with the incident (*www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021*).
- Considering which categories of data are affected, where they are stored and whether the data relates to current or former employees (*see "Mapping HR data" above*).
- Putting decision trees in place around, for example, a methodology for responding to data subject rights requests.
- Anticipating questions from staff and preparing stock responses in conjunction with any PR or crisis communications team.
- Agreeing the framework for determining risk ratings for employees or starting the risk-rating process to ascertain which data subjects require formal breach notifications (*see box "Compulsory data subject notification"*).
- Preparing template breach notifications.

Rogue employees

In rare instances, cyber incidents are the result of malicious employee behaviour. Although the immediate priority will be to recover, preserve and protect the lost or stolen data, the employer will want to take decisive action regarding the ongoing employment relationship. Depending on the circumstances, including the nature and severity of the incident, a range of actions could be justified, from initiating the employer's disciplinary proceedings or suspending the employee, to dismissing them for gross misconduct or even informing the police with respect to any criminal actions (*see feature article "Disciplinary actions and dismissals: handling the processes fairly", www.practicallaw.com/w-029-8702*).

The highly publicised class action brought against Wm Morrison supermarket involved the rogue actions of an aggrieved former employee, Andrew Skelton (*see feature article "Data class actions: the outlook after Morrison", www.practicallaw.com/w-026-2617; Various Claimants v Wm Morrison Supermarkets Plc [2020] UKSC 12*). This was an extreme case. It involved Mr Skelton publishing the personal details of almost 100,000 colleagues as revenge for Morrisons disciplining him in connection with a separate, comparatively innocuous, matter. Mr Skelton went to great lengths to cover his tracks, so Morrisons was unable to immediately identify the perpetrator when it became aware of the breach. However, within a few hours of receiving notification of the breach, Morrisons had launched internal investigations, informed the police and taken steps to remove the data from the internet. The police arrested and charged Mr Skelton six days later, and he was subsequently sentenced to eight years in prison.

Staff communications

A key strategic question for any organisation that has experienced a cyber incident is to determine if, and when, to notify its workforce. The desire to be transparent with employees must be balanced with the risks of causing undue concern, especially at a time when limited facts may be known. Unsurprisingly, the first questions that an individual will ask when told there has been a cyber incident is whether their own data has been compromised and, if so, what data is involved. If the business cannot answer these questions, anxiety levels may be raised. The timing and wording of communications are therefore critical.

Organisations will often engage external crisis communication experts who will provide strategic advice in relation to the timing, cascading and development of the messaging. Communication packs may include internal and external statements to employees, clients and other stakeholders, follow-up Q&A documents, online announcements and reactive media statements.

A distinction should be drawn between communication and notification. It is often the case that an organisation will have

Employee monitoring and data protection

In order to comply with the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR) and other UK data protection laws when carrying out employee monitoring, employers should note that:

- Monitoring is a recognised part of the employment relationship. UK law generally permits employee monitoring if the collection and use of personal data through monitoring is transparent, fair, limited and proportionate.
- An employer can rely on the UK GDPR's processing condition of pursuing its legitimate interests to justify much of its day-to-day monitoring.
- Employee monitoring is likely to be considered high-risk processing, which will require a data privacy impact assessment (DPIA) to be completed. In short, a DPIA should document the specific business need to undertake the monitoring, and why the form of monitoring proposed is proportionate in light of this need.
- To obtain personal data through employee monitoring fairly and lawfully, employers must notify employees before undertaking monitoring activities. Employers typically include this notice in their employee privacy or fair processing notice.

little choice but to communicate details of the incident to employees and clients. For example, if there is a significant operational impact, the incident will be obvious to staff or there is the risk of staff hearing about the incident from a third party. However, this is distinct from the compulsory, formal notification which is required under the UK GDPR (*see box "Compulsory data subject notification"*).

Mitigating effects on employees

Taking steps to mitigate the effect of cyber incidents on employees is critical from an employee relations perspective, in order to provide timely and necessary reassurance to employees about the integrity of their data and the employer's systems. This will also find favour with the ICO when it is assessing whether to issue a penalty and what level of fine.

These measures could include, for example, forcing a password reset or paying for a replacement passport or driving licence, if these particular documents form part of the compromised data set.

Commonly, employers also offer complimentary access to a credit monitoring service, given the increased chances of credit fraud or identity theft after a cyber incident. Pricing models for providers vary depending on volume and complexity. However, in a large-scale breach affecting thousands of employees it is possible that, even with a modest take-up rate of the services, the accumulative cost of these services could be significant. In *Morrison*, the Supreme Court noted that Morrisons spent more than £2.26 million in dealing with the immediate aftermath of the disclosure, a significant portion of which was spent on identity protection measures for its employees.

POST-INCIDENT MANAGEMENT

Once the immediate crisis is over, employers need to consider the longer term aspects of dealing with a cyber incident.

Managing data subject requests

Although less common than in the consumer data context, it is possible that disgruntled current or former employees may seek to avail themselves of one or more data subject rights following a cyber incident, not least as there is no cost to them attached to this exercise (*see box "Data subject rights"*).

Compulsory data subject notification

Article 34 of the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR) requires data controllers to notify a data subject of a personal data breach if it is likely to result in a high risk to a data subject's rights and freedoms.

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data (*Article 4(12), UK GDPR and section 33(3), Data Protection Act 2018*).

Whether the breach is high risk should be considered on a case-by-case basis, focusing on the potential negative consequences for individuals. This will depend on the sensitivity of the personal data that has been compromised, such as financial information, copies of passports or health data, and the likelihood of harm.

The notification must take place without undue delay. It must describe the nature of the security breach in clear and plain language, including at least the following information:

- The name and contact details of the data protection officer or other contact person (*see feature article "Data protection officers: a many-faceted role", www.practicallaw.com/w-029-4571*).
- The likely consequences of the security breach.
- The measures taken to address the breach and to mitigate potential adverse effects.

The controller is not required to notify data subjects of a personal data breach under certain limited circumstances, including when notification requires disproportionate effort. This may apply in the case of former employees whose data has been compromised, given that the contact details held by the organisation may be out of date. In this case, the controller is permitted to notify data subjects through a public communication or other effective measure, such as by an announcement on its website.

The penalty for failing to notify is a possible administrative fine under the UK GDPR of up to £8.7 million or 2% of annual global turnover.

Right of access

A cyber incident may prompt current or former employees to make a DSAR. The volume of DSARs in the fallout of a cyber incident can be significant if the incident is well publicised. Organisations that receive multiple DSARs should consider ways to streamline the response process (*see "Reviewing HR documents" above*).

Some of the key issues for employers to consider in practice when responding to DSARs in the data breach context are discussed below.

Scope of request. Often, an employee who submits a DSAR in these circumstances is simply interested in seeing the personal data that has been compromised. It is also often the case that the data originates from the personnel file, as a convenient source of personal details about an employee, including, in some instances, special category personal data. This information is appealing to attackers who can sell or post the details, such as photocopies of passports, salary or bank details, on the dark web.

DSARs submitted by former employees are more likely to extend beyond the exfiltrated data to include other personal data held by the data controller. This may be because the individual wants to understand their broader exposure in the event of a future data incident or to support an associated erasure request, or both (*see "Right of erasure" below*). The DSAR may extend to personal data processed in general email traffic within

Data subject rights

Right	Key grounds for data subject's request	Key exceptions and exemptions for data controller	Modalities
Access to personal data.	None, provided that the data controller processes the personal data of the data subject.	• Third-party data. • Legally privileged material. • Management forecasts and planning documents. • Confidential references. • Negotiations.	**Identification.** The data controller can request confirmation of the data subject's identity, which may be relevant for former employees and stops the clock until the necessary identification documents are received. **Timing.** There is a standard response period of one month on a corresponding calendar date basis, which can be extended by two months, taking into account the complexity and number of requests. **Fee.** No charge except for requests that are manifestly unfounded or excessive, in which case a reasonable fee can be charged.
Erasure of personal data.	• No longer necessary for collection purposes. • Consent has been withdrawn. • Objection to legitimate interests as the lawful processing ground and no overriding interest of a third party or the data controller.	• Compliance with a legal obligation. • The establishment, exercise or defence of legal claims.	
Rectification of personal data.	• Personal data is inaccurate. • Personal data is incomplete.	Data is not processed for purposes that require the data controller to identify the data subject.	
Restriction of processing of personal data.	• Personal data is inaccurate. • Processing is unlawful. • The data controller no longer needs to process the personal data but the data subject needs the data for the establishment, exercise or defence of legal claims. • Objection to legitimate interests as the lawful processing ground and no overriding interest of a third party or the data controller.	Data can continue to be stored, provided that it is not processed or used.	

in the company's IT systems, which is likely to involve a laborious retrieval and search process.

In appropriate cases, such as if the terms of the DSAR are unclear, the data controller may choose to seek clarification, which is permitted under recital 63 to the UK GDPR. For example, the data controller may invite the data subject to confirm the specific types of personal data that they are seeking, along with date ranges, suggested search terms and the details of specific employees who might have been involved in processing the individual's personal data. However, the data subject does not have to agree to narrow down their DSAR in this way. A request for clarification "stops the clock" in terms of the timescale for responding to the DSAR.

Searches. In principle, a data controller should apply the same considerations to its searches as it ordinarily would on receipt of a DSAR from a current or former employee. This could prove onerous in practice, particularly when dealing with multiple or complex DSARs at a time when resources are already stretched. There is scope for employers to take a pragmatic and commercial approach when responding to DSARs, and the time and costs of responding are relevant factors in determining what constitutes a reasonable and proportionate search.

Timing. Whether the two-month extension for the response is applicable will depend on a number of factors, not least whether the DSAR is limited to the personnel file, in which case a one-month period is likely to be achievable, or whether the response will involve searches of multiple databases, including archived materials, in which case the data controller may well require the two-month extension to respond on the basis that the response is complex.

Format of response. In cases where only exfiltrated data that is limited to details in the personnel file has been requested, it may be appropriate to provide the response in a schedule format, as opposed to providing the underlying documents in their native file format.

Right of erasure

Given the link between data retention and cyber incidents, erasure requests are common in response to a cyber incident. Considerations that can arise for data controllers in these circumstances are discussed below.

Erasure grounds. The right to erasure only applies in certain circumstances and each request needs to be considered on its merits.

With regards to requests from current employees, it is unlikely that any of the erasure grounds will apply as the employer will need to continue to process much, if not all, of the employee's personal data in the context of the ongoing employment relationship.

However, the erasure grounds are more likely to apply to the personal data of former

employees. The erasure ground that could apply is that data has been retained for longer than necessary, which could be by reference to data being held beyond the employer-set retention periods or where the employer-set retention periods are too long. Another erasure ground that may apply is where the data subject objects to processing which is based on legitimate interests. The erasure ground relating to the data subject's withdrawal of their consent is unlikely to be relevant as employers are not able to rely on consent to justify their day-to-day processing of personal and sensitive employee personal data.

Exemptions. The data controller then needs to consider whether an exemption applies. The two exemptions that are most likely to apply in these circumstances in the authors' experience are that the ongoing processing is necessary for:

- Compliance with a legal obligation; for example, to comply with mandatory retention periods, such as payroll and wage records (*Article 17(3)(b), UK GDPR*).
- The establishment, exercise or defence of legal claims (*Article 17(3)(e), UK GDPR*). This could be relevant if a data controller has brought injunctive proceedings against the cyber criminals, for which it is necessary to retain a record of the data that has been compromised. In these cases, the exemption is likely to apply just to the personal data held in the records. Personal data outside that category, such as the native documents that were compromised or other personal data held on the data subject which was not compromised in the breach, will still potentially be subject to the right of erasure.

A suggestion or threat that a data subject may bring a wider privacy claim against an organisation, such as a claim that their personal data was retained for longer than necessary, is unlikely to justify a data controller retaining personal data to guard against this type of potential claim, although the requests should be analysed on a case-by-case basis.

Retention queries. An individual who left an organisation several years ago may be surprised to hear that their data is still being held. Therefore, cyber incidents often prompt queries or complaints about an organisation's retention procedures. Although these enquiries may fall short of a formal erasure request, the data controller still needs to consider and respond to them carefully.

Although there can be a number of legitimate reasons for an employer to hold personal data on its current and former employees, the employer will face added difficulties responding to these requests if it does not have a retention policy, or if the organisation's retention periods are longer than one would expect or have not been implemented.

British Airways class action

Between May and November 2018, British Airways (BA) suffered a cyber attack that went undetected for two months. The attacker was believed to have gained access to BA's systems through a remote access gateway using the credentials of a third-party employee. Over 400,000 individuals, both customers and staff, received data breach notifications.

The Information Commissioner's Office imposed a penalty of £20 million, reduced from £183 million after representations from BA (*see Exclusively online article "ICO fine for BA: iron enforcement with a velvet glove", www.practicallaw.com/w-027-9929*).

More than 16,000 claimants brought the largest group action privacy claim to date. The claims settled in July 2021 on confidential terms (*Weaver and others v British Airways plc [2021] EWHC 217 (QB)*).

EMPLOYEE REDRESS

Employees may seek redress in a number of different ways.

ICO complaints

If an employee is unsatisfied with the organisation's response, they can raise a query or complaint with the ICO. While the ICO takes a pragmatic approach to the enforcement of employers' breaches of the GDPR principles, seeking remedial action on the part of the employer wherever appropriate as opposed to imposing fines or taking more severe enforcement action, it may be inclined to take a harder line with organisations that are already on the ICO's radar due to the reporting of a recent cyber incident.

Privacy claims

Organisations are often aware of the potential for a regulatory fine being issued under the UK GDPR following a cyber incident, but they are less aware of the exposure in relation to individuals, whether employees, clients or others, bringing privacy claims to compensate them for the harm, whether financial or distress, allegedly caused by the breach. Following a data subject notification exercise, privacy claims can be brought collectively by affected individuals in a class action. While they are typically low value, where significant numbers of claims are brought, the costs of defending or settling them, or both, can quickly escalate.

The law in this area is developing fast and a number of recent key judgments have clarified the way in which courts assess what claimants can claim for, how actions can be brought, what level of damages are awarded, which forum and jurisdiction is appropriate for bringing a low-value data breach claim and the costs associated with them.

The notable cases in 2021 were:

- *Warren v DSG Retail Limited*, where the High Court held that the misuse of private information and breach of confidence will never be appropriate causes of action in the event of a data breach; the only question is whether the security of the data was sufficient (*[2021] EWHC 2168 (QB); see News brief "Data breach claims: encouraging news for data controllers and processors", www.practicallaw.com/w-032-3675*).
- *Lloyd v Google LLC*, where the Supreme Court dismissed Mr Lloyd's £3 billion representative action against Google for the use of Apple's Safari browser, with the court finding that "damage" must involve financial loss or distress, and does not extend to the mere loss of control of data (*[2021] UKSC 50; see feature article "Lloyd v Google: the upshot for data class actions", www.practicallaw.com/w-034-4674 and News brief "Lloyd v Google: one door closes but*

another one opens?", www.practicallaw.com/w-033-4736).

- *Johnson v Eastlight Community Homes*, in which the High Court observed that the claim included overlapping and often inadequately pleaded causes of action (*[2021] EWHC 3069 (QB)*). The court struck out the entirety of the claim, save for the GDPR claim and confirmed that the case had all the hallmarks of a small claims track claim. This decision will therefore have significant ramifications for how low-value data breach claims should be brought. They may still be brought but should be simplified and brought within the cost-controlled environment of the small claims track of the County Court with no recoverability of after-the-event insurance premium from the defendant.

- British Airways' settlement of the largest data breach claim in the UK (*see box "British Airways class action"*).

Employment tribunal claims

Employment tribunals do not have jurisdiction specifically to hear complaints by individuals alleging breaches of their privacy rights, whether under the Data Protection Act 2018 or other data protection legislation. However, cyber issues and data breaches lie increasingly at the heart of employment tribunal claims, for example, by whistleblowers who raise issues relating to information security issues and claim that they have been treated detrimentally or dismissed, or both, as a result.

Khurram Shamsee is a partner, Nicola Geary is a senior associate, both specialising in employment law, and Eleanor Ludlam is a senior associate, specialising in cyber and data risk, at DAC Beachcroft LLP.

Related information

This article is at practicallaw.com/w-035-0663

Other links from uk.practicallaw.com/

Topics

Data protection offences	topic/1-607-9647
Data security	topic/8-616-6189
Employee data, monitoring and privacy	topic/5-200-0623
Information technology	topic/5-103-2074
Internet	topic/8-383-8686
Privacy	topic/6-383-8687
Rights of data subjects	topic/6-616-6190
Technology: data protection	topic/8-616-6207

Practice notes

Cybercrime: overview	1-589-1905
Cybercrime risks for businesses	6-615-3705
Cybersecurity: crisis management	4-625-5413
Data security under the UK GDPR and DPA 2018	w-013-5138
Data subject access requests in employment (UK)	w-011-9105
Data subject rights (UK)	w-024-3178
Managing cybersecurity risk and compliance	6-615-8326
Monitoring employees	3-200-4245
Overview of cybersecurity	9-617-7682
Overview of privacy law	1-507-0879
Overview of UK GDPR	w-013-3757

Previous articles

Lloyd v Google: the upshot for data class actions (2022)	w-034-4674
Changing face of cyber insurance: the devil finds work for idle hands (2021)	w-031-9892
Data protection officers: a many-faceted role (2021)	w-029-4571
GDPR enforcement: a changed landscape (2021)	w-030-5470
Data class actions: the outlook after *Morrison* (2020)	w-026-2617
GDPR one year on: taking stock (2019)	w-020-0982
Cyber risk and directors' liabilities: an international perspective (2016)	2-635-5748
Cyber security: top ten tips for businesses (2016)	3-621-9152
Employee monitoring: the value of being prepared (2016)	3-629-9945

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

