Employment investigations Part 2: Privacy and data protection considerations

In the second of a three part series of articles, Julia Wilson, Partner, and Sam Rayner, Associate, at Baker McKenzie LLP, look at data protection and privacy considerations in the context of employee investigations and explain how to minimise associated risks

Employee investigations are data heavy. Not only do they produce large quantities of material in the form of correspondence, meeting minutes and reports, they also require employers to locate and review various categories of record such as personnel files, expense reports, CCTV and email traffic.

Where these materials either identify or relate to particular individuals - as they inevitably do - they will contain personal data and trigger stringent obligations under the General Data Protection Regulation (GDPR), which has been implemented into and supplemented for the purposes of UK law by the Data Protection Act 2018 (DPA).

Investigations raise particular sensitivities under applicable privacy and data protection laws. Not only are the stakes often high for the individuals concerned, the data involved can be sensitive, (for example where an employee's health is intertwined with the conduct subject to the investigation), and the method by which they are retrieved and reviewed can be intrusive (such as where covert monitoring software is used).

Data protection compliance in employee investigations has historically been overlooked as a "nice to have". But priorities have shifted in recent years with the prospect of significantly enhanced fines (of up to €20 million or 4% of worldwide annual turnover) for GDPR breaches, enhanced regulator interest in employee monitoring, and increasing employee awareness of relevant data protection rights.

It is therefore crucial for employers to consider privacy and data protection compliance from an early stage, and embed these considerations into planning, implementation and ongoing review of the conduct of employee investigations. There is also an opportunity for employers to be proactive in addressing privacy compliance considerations, in order to allow investigations to proceed safely at the fast pace at which they often move.

For further commentary on broader employment law risks associated with investigations, please see *10 top tips: employment and privacy law dangers in carrying out employee investigations Compliance & Risk Journal Volume 9 Issue 6,* and for other specific risks, see also *Employment investigations Part 1: Criminal issues, Compliance & Risk Journal Volume 10 Issue 1.*

Accountability

One of the GDPR's key aims was to shift perceptions of data protection away from a passive, tick-box exercise to an ongoing, evolving and active obligation to demonstrate compliance with relevant legal obligations. As part of this principle of accountability, employers must document Data Protection Impact Assessments (DPIAs) before undertaking higher risk data processing activities.

Regulators will generally consider employee investigations to meet this "higher risk" threshold because they involve a "vulnerable" category of data subjects (in view of the subordinate position of employees within the employment relationship and the limited ability for employees to object to the processing by their employer), sensitive categories of data (potentially relating to criminal offences) and generally involve monitoring or evaluation processes (see Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)).

In any event, DPIAs are a sensible first step in most cases as they allow employers to identify potential privacy risks and mitigation strategies in advance. Should employees subsequently raise data protection concerns, regulators will inevitably ask for a copy of any relevant DPIA (and increasingly employees or their representatives also ask for the DPIA); well-drafted assessments provide crucial evidence of compliance steps taken and help mitigate prospects of severe enforcement action. Employers can prepare template DPIAs for investigations

that can be adapted at the start of a specific scenario.

Broader accountability obligations also require organisations to:

- document any decision to rely on their legitimate interests as the relevant lawful basis for processing, by balancing this against potential risks to data subjects (this is discussed further below); and
- maintain a living "record of processing activities", which should provide a snapshot of all data processing operations on the part of a controller. These should be updated as investigations progress.

Lawful bases

Amongst other things, a DPIA will help identify valid legal bases for data processing; a central element of any lawful investigation. In this context, employers generally rely on the fact that processing is necessary: (i) for compliance with a legal obligation to which they are subject; or (ii) for the purposes of the their legitimate interests. Employee consent is not a viable option.

Reliance on an organisation's legitimate interests requires those interests to be balanced against the privacy rights of the data subjects who might be impacted by the investigation. This usually takes the form of a legitimate interests assessment (LIA) which will explain the scope of any investigation and why the relevant processing is justified. Employers should consider various steps in an attempt to strike the required balance.

"It is therefore crucial for employers to consider privacy and data protection compliance from an early stage, and embed these considerations into planning, implementation and ongoing review of the conduct of employee investigations. There is also an opportunity for employers to be proactive in addressing privacy compliance considerations, in order to allow investigations to proceed safely at the fast pace at which they often move"

Practical steps may include the use of targeted search terms, date ranges, and sources of data when searching electronic records, ensuring those with access to the investigations data are subject to obligations of confidentiality and have received appropriate data protection training, implementing appropriate technical and organisational security measures and giving employees who are the subject of the investigation, or whose data are likely to be reviewed, the opportunity to identify data relating to private or personal matters, so that steps can be taken to try to avoid reviewing them.

Where "special categories" of data - including information revealing race/ethnic origin, religious or philosophical beliefs, trade union membership and data concerning health, sex life or sexual orientation - or data relating to criminal convictions or offences may be involved, organisations will need to satisfy an additional, enhanced legal threshold.

To satisfy this in the case of employee investigations, UK employers often seek to rely on reasons of "substantial public interest" under one of the specific public interest conditions set out in the DPA. One of these, for example, is where processing is necessary for the prevention or detection of an unlawful act (such as fraud). However, reliance on public interest conditions should be verified on a case by case basis and will require the implementation of an appropriate policy document which sets out additional safeguards. Again, this would be recorded in the DPIA.

More broadly, UK courts and tribunals have acknowledged that Article 8 of the European Convention of Human Rights (ECHR), which sets out an overarching right to private and family life: (i) extends into the work context; and (ii) should blend into broader employment protections. Any means of employee monitoring, (including that which is leveraged in an investigation), should be carefully assessed to ensure it does not disproportionately infringe any individual's reasonable expectation of privacy; this will be particularly important where organisations permit personal use of corporate IT systems. Transparency, which we come on to discuss next, is particularly important in addressing expectations of privacy.

Transparency

Employers must provide employees and other individuals with granular information about how their personal data will be processed, covering, amongst other things, the purposes for which they are used, the relevant legal bases, applicable retention periods and with whom (and where) information might be shared. These details are generally set out in a privacy notice, which should include details on the use of data for the purpose of employee investigations.

Employees are often provided with a privacy notice at the outset of their employment. But organisations should remember that the right to be informed is ongoing. Periodic updates will need to be communicated to reflect any changes in approaches to investigations including, for example, the involvement of new stakeholders (perhaps a dedicated investigations team based internationally) or use of new software (e.g. a third party document search/review platform).

(Continued on page 4)

(Continued from page 3)

It is possible for all this to be covered in the standard employee privacy notice issued at the start of employment; but if the privacy notice is not sufficiently detailed then the employer will need to consider issuing a specific (or "just in time") privacy notice to employees and other data subjects whose data are processed in the context of an investigation. If there are concerns that providing the privacy notice may prejudice the investigation, (for instance by obstructing a regulator in the prevention or detection of crime or apprehending/prosecuting an offender), then it can be appropriate to delay sending the privacy notice until the prejudice can be avoided.

The recent reliance on remote working has caused many organisations to consider implementing ongoing workforce monitoring and surveillance tools, which might be a trigger for and form the basis of investigations into employee conduct or performance in the virtual "workplace". Most European data regulators consider forms of continuous employee tracking, such as keystroke or mouse movement monitoring, deserving of enhanced scrutiny and, where lawful, transparency (Article 29 Working Party, Opinion 2/2017 on data processing at work (WP249)). Such practices may not be justifiable at all. The Hamburg DPA recently fined retailer *Hennes & Mauritz* (H & M) €35 million for intrusive employee monitoring, and the UK's ICO is currently investigating one employer's use of "always on" software intended to track worker productivity.

For completeness, investigations may involve the processing of data about individuals other than employees, including workers, independent contractors, business contacts, clients and other third parties. Ideally, privacy notices will be in place informing all data subjects that their personal data might be reviewed, and potentially shared with regulators, in the context of employee investigations. Again, if such notices are not in place, information regarding a specific investigation may need to be provided "just in time".

Data minimisation

At the beginning of an investigation, there is often a scramble to collect as much information as possible. As a first step, investigators often seek HR records, request relevant correspondence (including emails, chat records and text/WhatsApp messages), and reach out to witnesses. Some may even undertake their own searches on the internet and in conventional or social media for potentially relevant content.

Under the GDPR's data minimisation principle, the collection of personal data must be limited to what is adequate, relevant and necessary for the purposes of the relevant investigation. Controllers should also take care to ensure that they take every reasonable step to ensure that inaccurate data are erased or rectified without delay. In other words, investigators must constantly review the scope of the data they are collecting and take active steps to verify their accuracy. The DPIA plays an important role here, as a record of why specific data were required and why.

"investigations may involve the processing of data about individuals other than employees, including workers, independent contractors, business contacts, clients and other third parties. Ideally, privacy notices will be in place informing all data subjects that their personal data might be reviewed, and potentially shared with regulators, in the context of employee investigations"

Excessive data gathering also raises broader privacy risks under the ECHR. As stated above, an individual's right to a private and family life under Article 8 extends into the work context. When assessing this, judges would consider whether the relevant employee(s) have a reasonable expectation of privacy in relation to the correspondence in question and, if so, whether the interference with that privacy was both proportionate and lawful.

Targeted investigations on corporate devices/systems generally raise manageable risks. However, reliance on information held on private systems and data which are stored in private folders or within personal WhatsApp and similar messenger apps should be approached with care. The legality of any interference with Article 8 rights will depend on all relevant circumstances (*Bărbulescu v Romania (2017, 61496/08)*); including what that individual has been told about the potential for monitoring, the nature of the correspondence in question, the reasons for accessing it, whether it was sent whilst at work or on corporate devices, the potential consequences for the individual and any professional standards to which they are subject (*BC and others v Chief Constable Police Service of Scotland and others [2019] CSOH 48*). Covert access to personal chat applications, even if stored on corporate devices, may also raise significant risks under wider surveillance laws, as discussed below.

Security

The prospect of significantly enhanced fines under the GDPR, and the potential for vicarious liability for data breaches by individual employees, raises the stakes in respect of personal data security (*WM Morrisons Supermarkets plc v Various Claimants [2020] UKSC 12*). Sensitive employee investigations increase the threshold of the generic obligation to implement appropriate technical

and organisational security measures against data breaches; relevant policies should, at minimum, define key stakeholders who are accountable for data protection compliance, access limitations and "need to know" working groups, as well as key technical protections such as the need for encryption, secure file transfers and requirements of ongoing training.

Data breaches can be innocent and seemingly innocuous; perhaps forwarding a sensitive email to an unauthorised recipient, or leaving witness interview minutes on a train. But they can also be malicious, as in the case of unauthorised recordings. Where data breaches do occur, employers will need to be able to recognise, isolate and rectify them quickly, as well as report certain higher risk incidents to their regulator (within 72 hours) and affected data subjects.

IT teams must be well drilled on a dedicated data breach response policy, and investigation stakeholders on notice that failing to report a breach (electronic or physical) will be considered a disciplinary offence. Policies should be updated to make clear that intentional data breaches, including the making of unauthorised recordings, may have significant consequences that go beyond internal disciplinary action. For example, it is a criminal offence to knowingly or recklessly obtain or disclose personal data without the consent of the data controller. UK Employment Tribunals have also recently shown a willingness to make significant costs awards against claimants who bring spurious claims based on covert recordings they have made at work (*Tan v Copthorne Hotels Limited [2200986/2017]*).

Data sharing

Investigation scoping should clearly define internal and external stakeholders and map data flows to/from them. Where an organisation seeks to share personal data, whether to other group companies or third parties, such as outside investigators, regulatory authorities or information hosting platforms, it should always:

- ensure it has an appropriate legal basis for the transfer;
- classify the recipient as an independent controller, a joint controller or a data processor; and
- implement appropriate contractual terms which align with that label.

Where an entity processes personal data on behalf of and in accordance with instructions given by the employer, it will be a data processor for the purposes of data protection law. This is commonly the case in respect of third party software providers, such as HRIS and hosting or review platforms, all of which often play a central role in investigations. However, internal group companies can also constitute data processors, for example in the case of shared service or investigation support centres.

Whether internal or external, data processors must be subject to a formal contract which meets prescribed requirements under the GDPR. Amongst other things, these mandatory minimum terms oblige it to process transferred data in accordance with the controller's instructions, assist it in responding to individuals' data requests, and delete or return relevant data at the end of the relationship. Joint controllers have more freedom in allocating responsibilities, but are similarly expected to determine these and make the essence of the arrangement available to individuals.

Third party investigators and competent authorities will generally determine the purposes for and means by which they process personal data related to their investigation/internal procedures. This means, in many cases, they will be controllers in their own right and engagement documentation can be more light touch; it will generally be sufficient to formalise their classification under applicable data protection rules, seek appropriate compliance warranties (including in relation to data security), and obtain confidentiality protections.

"data transfer is broad and covers situations whereby information held on a server situated in one country is accessed in another. ...this means that multinational employers should map data flows between employing entities to ensure appropriate transfer mechanisms are in place...Risks will be enhanced where organisations have centralised investigations teams which manage processes across various jurisdictions"

International transfers

Data sharing often leads to international transfers. The GDPR prohibits controllers from transferring personal data outside the European Economic Area (i.e. the 27 EU Member States, plus Iceland, Liechtenstein and Norway) except: (i) to certain specified countries that have received an "adequacy decision" from the European Commission; or (ii) where a specific mechanism, such as the EU's standard contractual clauses or binding corporate rules, has been put in place to provide adequate protection for that personal data in the country to which it is transferred.

Post-Brexit, the UK recognises EEA states as providing adequate protection for personal data. That position is reciprocated under the UK-EU Trade Agreement until the earlier of: (i) 1 May 2021, which will be automatically extended to 1 July 2021 in the absence of any objection; or (ii) the

(Continued on page 6)

(Continued from page 5)

date on which the EU issues an adequacy decision regarding the UK. This decision has now been issued by the EU Commission and - at the time of writing - is awaiting formal approval by the European Council.

The concept of a data transfer is broad and covers situations whereby information held on a server situated in one country is accessed in another. The rules also apply without amendment to intra-group data transfers; this means that multinational employers should map data flows between employing entities to ensure appropriate transfer mechanisms are in place, as required. Risks will be enhanced where organisations have centralised investigations teams which manage processes across various jurisdictions.

Data transfers to the United States should be subject to particular scrutiny. Recent case law from the Court of Justice of the European Union (CJEU) has made clear that the legal framework in the US, particularly in relation to state surveillance for national security purposes, falls well below the standards required to confer sufficient protection for the personal data of EU citizens. In addition to declaring the previous EU-US Privacy Shield transfer mechanism invalid, the CJEU also required exporters to implement "supplementary measures" when seeking to rely on SCCs or BCRs (*Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited).*

This concept remains unclear and we suggest detailed legal advice is taken. Although the case focussed on transfers to the US, the concerns raised, and the need for exporters to consider supplementary measures, applies to any transfers to third countries.

Individual rights

All individuals, including those subject to or otherwise involved in an employment investigation, have a suite of rights in relation to their personal data. Central to this is the right of access, which gives individuals the right to obtain copies of (and prescribed information about) their personal data within one calendar month of their request, subject to limited exemptions and a narrowly interpreted ability to extend the deadline for responding for a further two months.

Safe in the knowledge that a broadly worded data subject access request (DSARs) will consume significant employer resource, as well as the fact that most regulators consider them to be purpose blind, employees may use them as leverage in order to complicate an investigation process, seek early disclosure of information, or test their employer's willingness to settle, either before or after a recommendation or decision has been reached. A poorly handled DSAR could prejudice the outcome of an investigation and, if challenged by a regulator, result in enforcement action.

With that in mind, organisations should proactively build DSAR response playbooks into their investigation procedures, with responsibilities allocated to appropriate stakeholders (such as IT, HR and Legal teams), so that requests can be swiftly recognised and addressed on both technical and practical levels. This guidance should also set out consistent approaches to common questions, such as when employers are permitted to ask for more information as to the scope of a request, when a request is sufficiently complex so as to justify an extension of time, and a clear explanation of the limited situations in which refusing to respond to a manifestly unfounded or excessive request may be acceptable.

Playbooks should also address other data subject rights, including in respect of more limited powers to: (i) have inaccurate data rectified, updated or completed; (ii) require the deletion of personal data where there is no longer a legal ground to process them; and (iii) object to the continued processing of personal data. The right to object could be particularly problematic for organisations who justify employee data processing on the basis of their legitimate interests; on receipt of such a request, an employer would need to restrict (e.g. isolate) the data in question until such point as it is able to show compelling legitimate grounds to continue processing them.

Objections to data processing are sometimes strategically leveraged by employees (particularly alleged wrongdoers) in the context of an investigation and will cause the investigation to temporarily be put on hold; having the playbook ready will enable the employer to respond quickly and enable the investigation to progress.

"compliance with privacy and data protection law is not a task that can be covered off with static underlying policies that seem to tick all of the...boxes. Organisations need to design their procedures and accountability records in a manner which is capable of evolving with their operations and software, as well as reacting to particularly high risk scenarios, for example where health or potentially criminal conduct is involved"

Criminal offences

Outside of data protection law, employers should also note that investigations, particularly those which involve covert searching or monitoring, could trigger obligations

or potential liability under national communications, secrecy, or surveillance laws. In the UK, provisions under the Investigatory Powers Act 2016 (IPA) and Computer Misuse Act 1990 (CMA) might be relevant.

Imaging and reviewing employee emails and messages on mobile and other devices generally constitutes the "interception" of communications in the course of transmission for the purposes of the IPA; which is a criminal offence in the absence of consent or another lawful authority. Lawful bases for interception are drafted broadly and will generally permit monitoring or recording for the purposes of establishing facts, detecting/preventing crimes and/or ascertaining adherence to company or regulatory standards. This should nevertheless be verified, particularly where employers seek to rely on new or intrusive forms of technology as part of their investigations, or where the investigation strays beyond the employing organisation's IT environment into private systems, communication channels and apps.

The CMA also makes it a criminal offence for a person to cause a computer to perform any function with intent to secure access to any programme or data which they are not authorised to access. The CMA is usually cited in malicious hacking cases, but it may be raised by employees who are concerned about access to their personal or private data stored on work devices. Whilst legitimate counter-arguments around the presence of any intention may be raised in those circumstances, it emphasises the importance of clearly defining the scope of search/review processes associated with any investigation.

Conclusion

The principles set out above represent a sensible framework for data protection compliance, but do not represent a "one-size fits all" solution. In practice, investigations need to be assessed based on their own risk factors and businesses should have frameworks in place to help flex their processes depending on an ongoing assessment of sensitivity.

In other words, compliance with privacy and data protection law is not a task that can be covered off with static underlying policies that seem to tick all of the above boxes. Organisations need to design their procedures and accountability records in a manner which is capable of evolving with their operations and software, as well as reacting to particularly high risk scenarios, for example where health or potentially criminal conduct is involved.

But an employer can do some of the heavy lifting up front to be well prepared for investigations as they arise. Recommended steps include implementing detailed privacy notices and monitoring procedures, creating template DPIAs, putting in place a data subject rights playbook, having template data processing terms for third parties, and addressing international data transfers etc, all of which are covered above.

These measures can all be built into an employer's compliance investigations framework, ready to be adapted as necessary to suit each investigation.

The rise in remote working, and frequent desire for employers to monitor employees with ever more intrusive software, raises the data protection and privacy stakes further. In an increasingly virtual world, to avoid all of the expensive new software becoming a blunt or risky tool in helping to implement effective investigations, businesses should also take steps to bring related investigation procedures and protocols up to date.

Julia Wilson
Sam Rayner
Baker McKenzie LLP
julia.wilson@bakermckenzie.com
sam.rayner@bakermckenzie.com