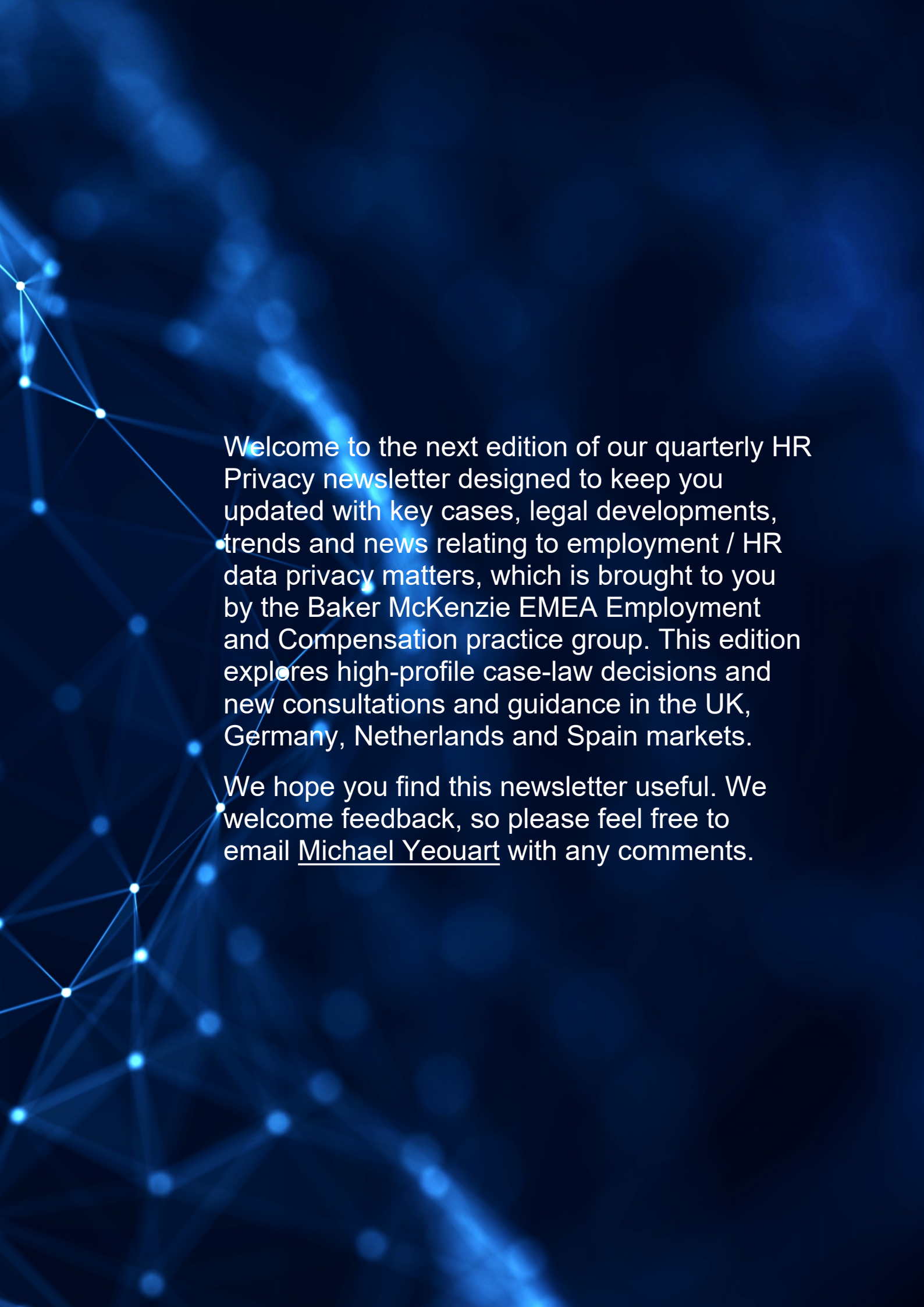




**Baker
McKenzie.**

EMEA HR Privacy Newsletter

November 2023



Welcome to the next edition of our quarterly HR Privacy newsletter designed to keep you updated with key cases, legal developments, trends and news relating to employment / HR data privacy matters, which is brought to you by the Baker McKenzie EMEA Employment and Compensation practice group. This edition explores high-profile case-law decisions and new consultations and guidance in the UK, Germany, Netherlands and Spain markets.

We hope you find this newsletter useful. We welcome feedback, so please feel free to email [Michael Yeouart](#) with any comments.

Contents

UK	2
In the courts.....	3
Employee unfairly dismissed for refusing to install intrusive work app on personal phone	3
Unlawful access of personal data by former employees	5
New consultations and guidance.....	6
ICO publishes updated guidance on processing worker health data	6
ICO guidance on monitoring of workers: Key takeaways for employers.....	8
Germany	10
In the courts.....	11
ECJ decision lends weight to proposals for new legislation on employee data protection	11
Admissibility of evidence in data privacy dispute	13
Offensive and racist remarks about colleagues on private WhatsApp group can justify immediate dismissal.....	15
Netherlands	17
In the courts.....	18
Court upholds employer's right to restrict data subject's access to personal data	18
New consultations and guidance.....	19
Dutch regulator changes approach to GDPR breach fine calculations	19
Spain	21
In the courts.....	22
No fundamental breach of privacy in WhatsApp monitoring	22
Installation of geolocation tracking in company cars was an adequate and proportionate measure to monitor employee activity	24

UK



In the courts

Employee unfairly dismissed for refusing to install intrusive work app on personal phone

In brief

A dismissal was found to be unfair where it was driven by the employee's refusal to install an intrusive work-related messaging app on her personal phone, using her personal number. The employer had failed to explore reasonable alternatives, such as providing a corporate phone or installing the app on an existing work laptop.

Facts

The Claimant worked as an Online News Editor for the Respondent newspaper. The Respondent began to require its staff to use the messaging app Viber to help with work allocation and supervision. The Claimant was specifically asked to install the app on her personal phone on several occasions following concerns around mistakes in her publication of articles.

The Claimant refused as she was concerned about the "flood of notifications coming through 24/7" on the platform. She asked for it to be installed on a separate, Company-provided mobile phone which she could switch off when not at work. The Respondent did not agree to this, blocked the Claimant's access to its systems and ultimately terminated her employment.

Reasonableness of refusal to install app

The Claimant brought a number of employment claims against the Respondent, including for unfair dismissal. The Employment Tribunal was satisfied that the principal reason for dismissal was her refusal to use the Viber App on her personal phone for work purposes.

The Tribunal concluded that this decision was one that "no reasonable employer" would take and was substantively unfair. It acknowledged that employers had discretion as to the kinds of software employees should use, but said that there were other viable solutions which would have enabled the Claimant to "separate her home and work life". Reasonable alternatives, such as the provision of a corporate phone or use of a work laptop, had not been properly explored by the Respondent.

Comment

With employers increasingly seeking to use new and potentially intrusive technologies to communicate with, supervise and monitor their employees, this decision serves as a reminder that individual privacy rights should factor into procurement and implementation processes. The benefits of new systems should be weighed against any potential intrusion into employees' private lives in advance, with a view to demonstrating proportionality. Data protection impact assessments can be a useful tool in documenting this kind of assessment.

The decision here also illustrates the importance of following a fair process prior to taking disciplinary action in response to employee resistance to the use of particular technologies. An employee's failure to follow a reasonable management instruction may provide grounds for a fair conduct dismissal, but a degree of investigation should take place before confirming any decision. Here, no fair process had been carried out prior to the decision to terminate; she was never given any warning or told of the potential

consequences of failing to install Viber, no proper investigation was carried out and no disciplinary hearing was held before a final decision had been reached.

Alsnih v Al Quds Al-Arabi Publishing & Advertising (ET 2203652/2020)

Authors



Julia Wilson
Partner
London
+44 20 7919 1357
julia.wilson@bakermckenzie.com



Sam Rayner
Senior Associate
London
+44 20 7919 1260
sam.rayner@bakermckenzie.com

Unlawful access of personal data by former employees

There have been two recent cases relating to the unlawful access of personal data by former employees for their own purposes, one resulting in a successful prosecution, and the other resulting in summary dismissal, which the Employment Tribunal held was fair.

In the first case, a former family intervention officer was fined after she pleaded guilty to the offence of unlawfully obtaining personal data in breach of section 170(1) of the Data Protection Act 2018. The incident came to light following an internal audit by the council for which she worked, which revealed she had unlawfully looked at the records of 145 people whilst she was employed in their social services department. She resigned from her employment before disciplinary proceedings commenced.

In the second case, the Claimant, who had been an immigration enforcement officer at the Home Office was found to have been fairly dismissed when she accessed the visa records of members of her family for personal reasons unrelated to work. The Home Office had an express 'zero-tolerance' policy against accessing records without a legitimate business need, which was set out in several places including its disciplinary policy. The Claimant was summarily dismissed for gross misconduct after the unlawful access was discovered during an internal audit. The Tribunal held that it was reasonable for the Home Office to treat the unlawful access as gross misconduct based on its policies and express warnings. Even if the Tribunal was wrong on the unfair dismissal claim, it would have found that the Claimant's numerous and repeated breaches in the face of a zero-tolerance policy struck at the heart of the employment relationship and was significant contributory fault which would have made it just and equitable to reduce her compensation to nil.

The cases are a good reminder that individual employees have a duty themselves to ensure that they are complying with data privacy laws. Personal data should only be accessed where there is a lawful basis for doing so – having access to personal data as part of your role does not give you carte blanche to access others' personal data. This is particularly important with sensitive personal data.

Employers may wish to remind employees of their individual data protection compliance obligations as part of their employees' data privacy training. They should also make it clear in their policies that unlawful access of personal data is prohibited and will amount to a disciplinary offence.

Author



Mandy Li
Knowledge Lawyer
London
+44 20 7919 1033
[mandy.li](mailto:mandy.li@bakermckenzie.com)
[@bakermckenzie.com](mailto:mandy.li@bakermckenzie.com)

New consultations and guidance

ICO publishes updated guidance on processing worker health data

Processing worker health data can be a tricky area to get right. It is one of the more sensitive categories of data that employers will process, and a category that employees are likely to be particularly concerned about. There will be circumstances where employers legitimately need to process worker health data, but a balance needs to be struck to ensure that any processing is proportionate and necessary. The new more detailed [guidance](#) from the UK Information Commissioner's Office (ICO) on this topic is therefore a welcome addition.

The new guidance was published at the end of August, and is part of the ICO's ongoing effort to revise its employer guidance and the Employment Practices Code. The guidance does not say anything particularly new or surprising, but it does offer more practical and accessible guidance for employers. It recognises that employers will need to process health data in a number of circumstances, and covers some common areas that arise in practice. For example:

- **Health questionnaires and medical examinations** – the guidance recognises that these steps are often necessary for health and safety reasons, for example for those working in hazardous environments or with clinically at risk people, but emphasises that employers must think about data minimisation. The ICO views medical examinations and testing as inherently intrusive so particular caution is required with them. In all cases you should use targeted health assessments that are bespoke to the specific roles that you are recruiting for, rather than using a default approach for all staff.
- **Occupational health referrals** – the guidance reminds employers that their interest is in knowing whether an employee is fit to work, and that occupational health referrals and the specific questions posed should be targeted with that in mind. That means limiting your requests to relevant information only, rather than asking for full details of an employee's condition. It also clarifies that the ICO expects occupational health providers to be data controllers rather than data processors, and that employers should consider putting in place a data sharing agreement if they use a regular OH provider.
- **Drug and alcohol testing** – again, the guidance emphasises that this should be carefully tailored to specific roles and the risks associated with those roles. It should not be a means of simply revealing whether an employee uses illegal substances in their private life. Drug and alcohol testing should be justified, properly documented and based on clear criteria. The guidance makes it clear that randomised testing will rarely be justified.

- **Health monitoring, including wearables** – the guidance expressly flags that health monitoring technology, such as wearables, has the potential to be much more intrusive than traditional record keeping around health and sickness absence. It is clear that employers will need to think very carefully about how they justify these sorts of measures and the ICO explains that in some cases you *must* carry out a Data Protection Impact Assessment (DPIA). This is significant because in other instances the guidance states that employers *should* carry out a DPIA.

Another useful section of the guidance for employers is the section titled "*What lawful basis might apply if we want to process workers' health information?*". This section runs through the six lawful bases for processing personal data, with examples, as well as the special category conditions under Article 9 GDPR and the accompanying additional conditions and safeguards found in Schedule 1 of the Data Protection Act 2018. As noted throughout the guidance, processing of health data is often intrusive and it is strongly recommended to carry out a DPIA before introducing a new method of processing health data.

Finally, the difficulties of relying on consent in the employment context are well-rehearsed but the ICO reiterates them in the guidance, noting that:

- "...you may find it difficult to rely on consent to process health information about your workers. This is because, as an employer, you will generally be in a position of power over your workers. They may fear adverse consequences and might feel they have no choice but to agree to the collection of their health information. Therefore, they cannot freely give their consent. If the worker has no genuine choice over how you use their information, you cannot rely on consent as a lawful basis."; and
- "You should avoid relying on consent unless you are confident you can demonstrate it is freely given. This means that a worker must be able to refuse without fear of a penalty being imposed. They must also be able to withdraw their consent at any time. If you think it will be difficult for you to show that your workers' consent is freely given, you should consider relying on a different lawful basis, such as legitimate interests."

If your organisation processes worker health data we strongly recommend reading the guidance and taking advice if there are any areas where you have questions or where you have concerns with your current compliance.

Author



Rob Marsh

Senior Associate

London

+44 20 7919 1344

[rob.marsh](mailto:rob.marsh@bakermckenzie.com)

[@bakermckenzie.com](mailto:rob.marsh@bakermckenzie.com)

ICO guidance on monitoring of workers: Key takeaways for employers

Employee monitoring has become common practice for many employers in the UK. Monitoring is often part of an organization's security procedures to secure personal information or prevent loss of property, often deployed for health and safety reasons, or companies may even have to monitor employees to comply with legal requirements (for example, in the financial services sector). Increasingly, employers are monitoring employee office attendance as many organisations are requiring their staff back into the office for all or part of the working week. For whatever reason, it is important that any such monitoring is carried out in compliance with data protection law. This is why the ICO has released tailored guidance to clarify the do's and don'ts of monitoring of workers by employers, and how this interacts with data protection.

Who is affected by this guidance?

The ICO guidance relates to any form of monitoring of people who carry out work on an employer's behalf. This will include monitoring workers on particular work premises or elsewhere (e.g., if working from home), and can also include monitoring carried out during or outside work hours. This guidance will also cover you if you employ a visiting worker to your household, such as a nanny or gardener, and monitor their activity routinely, or on an ongoing basis.

What sort of monitoring is covered?

This guidance broadly covers systematic and occasional monitoring. Practical instances may include keystroke monitoring to track, capture and log keyboard activity, productivity tools which log how workers spend their time, tracking internet activity, body worn devices to track the locations of workers, hidden audio recording, camera surveillance, webcams and screenshots, technologies for monitoring timekeeping or access control, and tracking use of company communication systems.

Key Takeaways

Some key tips for employers to note are as follows:

- Is monitoring workers allowed? The ICO makes it clear that monitoring staff is allowed as long as it is done in accordance with data protection legislation. This means you must have a lawful basis to carry out the monitoring, must clearly communicate your monitoring practices and the monitoring must be proportionate.
- You should only monitor workers in ways they would reasonably expect and not in ways that cause unjustified adverse effects on them, unless exceptional circumstances apply. For example, you should not monitor the content of communication on a worker's personal email account as an ordinary course of conduct.
- If the monitoring activity is likely to capture special category data, even incidentally, you must identify a special category condition. This is particularly relevant for workplace investigations which involve imaging of personal device.
- How about covert monitoring? Generally, covert monitoring would not be justifiable under the UK GDPR. However, there are exceptional circumstances where it can be justifiably employed for example, where it is necessary to prevent or detect suspected criminal activity or gross misconduct, and a less intrusive means of preventing or detecting such activity is not available. The ICO has laid down stringent guidelines to be observed before covert monitoring should take place, of which the key ones are:

- Covert monitoring should only be authorised by senior management.
 - In most circumstances you should not covertly capture personal, non-work, communications (e.g., personal emails or instant messages).
 - It must be infrequent monitoring that is targeted at fulfilling an objective within a limited time frame.
 - Limit information collected to only what is needed and disclosure to only a limited number of people involved in the investigation.
 - Only use the information you obtain for the relevant purpose, unless the monitoring reveals unrelated information no employer could reasonably be expected to ignore.
- Unless there is a compelling reason not to, consult with employees before monitoring is undertaken.
 - If your monitoring activity captures special category data, even incidentally, the ICO expects you to identify a special category condition.
 - Define and record the purpose of your monitoring before doing so.
 - The ICO expects you to carry out a DPIA before any employee monitoring, even if it is not legally necessary under the GDPR.
 - Employees must be given clear and understandable information regarding monitoring. This would involve informing workers about the nature, extent and purpose of any monitoring.
 - You should also consider implementing monitoring policies and training to provide guidance to staff who are involved in the monitoring process so that they are aware of their responsibilities.
 - If your employees work from home, keep in mind that their privacy expectations are likely to be higher at home than in the office.

Comment

Much of the information in the ICO guidance is not new, however employers may want to re-evaluate their processes in the light of this guidance when implementing new monitoring systems in the workplace. This is particularly relevant considering the recent trend among employers in monitoring employee attendance at the workplace to ensure compliance with hybrid working policies. For example, many employers may not have routinely consulted with their workforce prior to implementing monitoring systems. Ultimately, an employer's key compliance document when seeking to carry out employee monitoring will be a DPIA. In addition to this, employers should review their monitoring policies to ensure they are clear on the nature, extent and purpose of any monitoring that takes place.

Authors

Chiemeka Nwosu
Privacy Lawyer
London
+44 20 7072 5822
chiemeka.nwosu@bakermckenzie.com



Bobby Sarkodee-Adoo
Senior Associate
London
+44 20 7919 1752
bobby.sarkodee-adoo@bakermckenzie.com

Germany



In the courts

ECJ decision lends weight to proposals for new legislation on employee data protection

In brief

Earlier this year the European Court of Justice (ECJ) found that local employment related data protection rules that apply in the state of Hesse likely do not provide the level of protection required by the General Data Protection Regulation (GDPR) and if this is the case, they shall not be applied by the courts. As the local rules considered by the ECJ are broadly similar to those that apply at federal level, the decision lends weight to proposals to revise employee data protection rules in Germany more generally.

Facts

While the GDPR has direct effect across the European Union, it permits member states to implement national rules on processing employee personal data provided certain conditions are met and specific safeguards are in place.

The case involved the live-streaming of school classes during the COVID-19 pandemic. Consent to data processing involved was obtained from the students or their parents, but not the teachers. Instead the relevant local authority relied upon a lawful basis for processing employee personal data set out in local data protection legislation.

The question for the ECJ was whether the local legislation complied with the provisions of the GDPR that permit member states to implement their own rules in relation to processing employee data but only if local legislation contains "more specific rules" and if further conditions are met (cf. Art. 88 GDPR). The ECJ ruled that in the present case the local law likely does not comply with these requirements, in particular because local provisions that simply repeat the GDPR regulatory content would not be a "more specific rule" as required under the GDPR; in practice this would mean that the local legislation should not be taken into account by the courts and instead they should apply the relevant provisions of the GDPR.

Impact

The ECJ decision is of wider relevance in Germany because the local data protection legislation that it considered is almost identical in wording to the employee data protection provisions of the Federal Data Protection Act (FDPA). It potentially lends weight to proposals by the Federal Ministry of the Interior (*Bundesministerium des Inneren*) and the Federal Ministry of Labour and Social Affairs (*Bundesministerium für Arbeit und Soziales*) for a new federal employee data protection law with more specific regulations. The proposals were, although never officially announced by the ministries, leaked in May 2023 by some associations in Germany to which they have been sent; some of the key points include:

- increased restriction on monitoring employees;
- stricter rules, including an exemplary list of concrete cases, on the use of consent as a lawful basis for data processing in an employment relationship;
- written law on the employer's right to ask questions in interviews, to make tests and examinations with applicants and employees;
- more specific data subject rights;

- enhanced transparency requirements around the use of AI in the employment and hiring context;
- expanding employment data protection rights to platform workers; and
- introducing new rights of co-determination for German works councils in connection with employee data protection and data privacy rights.

Comment

These proposals are at a very early stage and are likely to change as they would make their way through the legislative process. It seems clear, however, that more specific and onerous employee data protection rights are likely to be implemented in the future. This will lead to increased compliance obligations for employers in Germany in relation to employees' and applicants' data processing.

We will continue to report relevant updates in this newsletter.

European Court of Justice - Judgment of 30 March 2023 (docket no. C-34/21)

Admissibility of evidence in data privacy dispute

In brief

The German Federal Labor Court (*Bundesarbeitsgericht, BAG*) has again confirmed that courts can still consider relevant video surveillance evidence in employment related claims even where it was processed in breach of certain data protection rights. In addition, the BAG clarified that the parties to a works agreement do not have the authority to place restrictions on admissibility of evidence that go beyond those that apply generally in civil procedure law. Infringement of works council co-determination rights in relation to employee monitoring is also irrelevant to the question of admissibility of evidence.

Facts

The employer alleged that the employee, a foundry worker, was paid for an overtime shift in June 2018 which he did not work. Following an anonymous tip-off, the employer checked video surveillance recordings from a camera installed at the gate to the plant; this showed that the employee had left the premises before the start of his shift. The video camera was visible and marked with signage. The employer dismissed the employee with immediate effect and, in the alternative, with due notice.

In his action for unfair dismissal, the employee claimed that the video evidence was inadmissible on a number of grounds including that the employer had breached some of his data protection rights and a works agreement expressly prohibited evaluating personal data from video surveillance.

The lower courts found in favor of the employee but the employer was successful on appeal before the German Federal Labor Court (*Bundesarbeitsgericht, BAG*).

The BAG ruled that the video surveillance evidence of the employee leaving the premises before his shift was admissible and could be used as evidence of the employee's misconduct. It went on to clarify that such evidence would only be inadmissible where the relevant surveillance activities had been carried out in serious breach of the employee's fundamental human rights and that sanctions imposed on the employer as a result (such as damages or a fine under the GDPR) would be an insufficient remedial action. This would rarely be the situation in cases where employee misconduct has been captured by an open surveillance measure.

In addition, it confirmed that a works agreement cannot dictate whether evidence is admissible in court proceedings; this is a matter for the Code of Civil Procedure that applies to the judicial process in Germany and is the responsibility of the legislator. Likewise breach of works council co-determination rights in relation to installation of the surveillance equipment does not have a bearing on admissibility of evidence.

Comment

This is a helpful decision in addressing a number of questions. The BAG has confirmed that an employer's breach of data protection rights does not generally in itself prevent evidence obtained by open surveillance measures from being used to show employee misconduct. The position might be different were the surveillance measures carried out covertly. Employers should note that notwithstanding the admissibility of surveillance evidence, an employer could still be liable to pay damages to the employee and subject to a fine under the GDPR where data protection rights are breached.

The BAG has for the first time confirmed that the parties to a works agreement do not have the authority to restrict the judicial assessment of evidence. Disputes over independent rules on the use of evidence in works agreements, which are often sought by works councils, should now be off the table. The same applies on the question of

whether infringement of works council co-determination rights in relation to the introduction and use of employee monitoring equipment has an impact on the admissibility of the evidence obtained. The BAG has clearly rejected this.

Federal Labour Court (BAG) 29 June 2023 (docket no.: 2 AZR 296/22)

Offensive and racist remarks about colleagues on private WhatsApp group can justify immediate dismissal

In brief

Can offensive and racist remarks about a superior in a private WhatsApp chat group justify immediate dismissal? Yes, finds the Federal Labour Court (*Bundesarbeitsgericht, BAG*), clearing the way in what has so far been an inconsistent and unclear legal landscape.

Facts

The employee had been a member of a private WhatsApp chat group since 2014. The group comprised initially five and later six current and former co-workers who were long term friends or even relatives. Besides merely private topics, the employee - as well as several other group members - expressed himself in an offensive and degrading manner about superiors and work colleagues, among others. The chat history contained various deeply racist, sexist and grossly insulting statements. Upon learning of this practice by chance, the employer terminated the employee's employment without notice and, in the alternative, with a period of social notice.

The employee brought an action for unfair dismissal. Both lower courts ruled in his favor; in their view the group messages were confidential and protected by the right to privacy.

The employer's appeal on questions of law only was successful. The BAG found that the lower courts had erred in deciding that the employee had a reasonable expectation of confidentiality with regard to the group messages and in rejecting the existence of sufficient grounds for dismissal. It ruled that in cases such as these involving deeply offensive and discriminatory statements about co-workers, an employee would only be able to establish a right to privacy in exceptional circumstances. This would depend on the content of the messages and the size and composition of the chat group; the employee would also need to demonstrate confidentiality existed within the group and that they could reasonably expect that the content of the messages would not be passed on to a third party by any group member.

The case has now been referred back to the Regional Labor Court which must now provide the employee with the opportunity to explain why he had a reasonable expectation of confidentiality as regards the group messages taking into account the BAG guidance.

Comment

Overall, the ruling of the BAG is welcome. Although the reasoning of the judgment has to be awaited to draw final conclusions, it is helpful that the BAG has carved out legal standards for the evaluation of offensive private communication in chat groups in an employment law context. It remains to be seen whether private communication will become a reason for terminating employment relationships more often. It will also be interesting to see how the courts will deal with less clear-cut cases in the future. In any event, the Court's ruling demonstrates that while every employee has a right to express negative comments about colleagues and superiors in a private and confidential manner, insulting and degrading statements may mark a boundary. If the employee cannot reasonably rely on confidentiality and accepts the risk that the information could be passed on to third parties, they have to face consequences under employment law – even if this means termination without notice.

German Federal Labor Court, Judgment of 24 August 2023 - 2 AZR 17/23

Authors and HR Privacy Leads for Germany



Matthias Koehler
Partner, Berlin
+49 30 2 20 02 81 662
matthias.koehler@bakermckenzie.com



Christian Koops
Partner, Munich
+49 89 5 52 38 147
christian.koops@bakermckenzie.com



Sebastian Pfrang
Associate, Frankfurt
+49 69 2 99 08 439
sebastian.pfrang@bakermckenzie.com

Netherlands



In the courts

Court upholds employer's right to restrict data subject's access to personal data

In brief

An Amsterdam court has found that an employer was entitled to limit a former employee's access to his personal data following a data subject access request in order to protect other staff and the employer's position in legal proceedings.

The facts

The data subject was employed by a college of higher education. A colleague reported to the employer transgressive behaviour by the data subject. In response the employer engaged a third party to conduct an independent investigation into the incident. This resulted in the employer initiating a dismissal procedure in relation to the data subject.

After his dismissal, the data subject requested access to his personal data from his now former employer, specifically all personal data that could be traced directly or indirectly to him from the time his colleague made the report about his behaviour up to and including the dismissal procedure. The former employer allowed the data subject access to some of his personal data but not all. In particular it provided the data subject with a summary of the colleague's report but not the report in full. It also withheld internal notes made during the period between the report being made and the start of the dismissal procedure. The employer considered that specific exceptions set out in the GDPR applied and entitled it to limit the data subject's right of access. Broadly, reliance on these is possible in individual cases provided the restriction on the right of access is strictly necessary and applied in a proportionate manner respecting the essence of the fundamental rights and freedoms.

The Court rejected the data subject's claim for access and agreed with the employer that it was entitled to limit access on the following grounds:

- to safeguard the rights and interests of the (former) employer, the reporter and of other employees; and
- to protect the legal position of the employer in any civil law claims that might arise as a result of the former employer's obligations under Dutch health and safety legislation to investigate and take measures after a report of transgressive behaviour in the workplace.

In such circumstances the data subject's right to access his personal data was outweighed by the interests of the employer and the employee that made the report. The employer had also adopted proportionate measures by providing a summary of the nature of the report to the data subject rather than the report in full. The employer was therefore not in breach of the data subject's right of access.

Amsterdam District Court - 3 August 2023, ECLI:NL:RBAMS:2023:5257 –

New consultations and guidance

Dutch regulator changes approach to GDPR breach fine calculations

In brief

New guidelines from the European Data Protection Board (EDPB) to harmonise how fines for breach of the General Data Protection Regulation (GDPR) are calculated across the EU mean changes to the fining policy of the Dutch Data Protection Authority.

Facts

In June 2023 the EDPB, the alliance of European privacy regulators, adopted new guidelines for calculating fines for breaches of the GDPR. These should mean that all privacy regulators in the European Union calculate fines in broadly the same way; previously each regulator had its own rules.

Standardizing the approach to calculation will provide clarity for private sector organisations that process personal data and mean that the level of fine that applies to a particular infringement will not vary depending on which member state regulator is responsible for enforcement. Regulators will also be able to monitor each other's approaches to fining with the aim of developing a more consistent approach across the EU.

The new guidelines are different in three important ways from the fining policies that the Dutch Data Protection Authority (DPA) had previously implemented.

■ **Company turnover plays a greater role**

A company's size is given a greater role in determining the amount of the fine. Under the old fining policy, the DPA only took into account the size of the company at the end of the calculation of the fine. Under the new rules, this happens at the beginning.

A company can see in the guidelines the sum that is used as the starting point for calculating the fine for a given breach for a company of its size; the turnover of the parent company is also taken into account.

■ **Categories of violation severity**

Under the new guidelines, there are three categories of severity of infringement: low, medium and high. Until now, the DPA also looked at the severity of the breach when determining the level of the fine, but without attaching a category to it. With the new guidelines, a different starting point for the fine applies for each category.

■ **Bandwidth for starting amount**

As was already the case under DPA fining policies, the new guidelines use a range of fines for different types of infringement. The old DPA fine policy assumed a range within which a fine amount was basically determined. In the new guidelines however, the range is intended to determine the starting point for the fine calculation. That amount can then be increased or decreased.

Regulators begin calculating the amount of the fine with that starting amount and then consider if there are reasons to adjust the fine. For example, they might apply an increase where the company has previously committed a similar infringement or a reduction if the company did everything possible to limit the impact on the victims of the infringement.

As was already the case fines, can reach up to 20 million euros or 4 percent of a company's global turnover.

The new rules are effective immediately and will only apply to the private sector. The DPA is still investigating in a European context what rules it wants to use in the future to calculate fine levels for government organizations. For now, the DPA's old fining policies will continue to apply to government agencies.

Author and HR Privacy Lead for the Netherlands



Remke Scheepstra
Partner, Amsterdam
+31 20 551 7831
[remke.scheepstra](mailto:remke.scheepstra@bakermckenzie.com)
[@bakermckenzie.com](mailto:remke.scheepstra@bakermckenzie.com)

Spain



In the courts

No fundamental breach of privacy in WhatsApp monitoring

In brief

The Madrid High Court of Justice recently found that an employer's monitoring of WhatsApp conversations between its employees and customers on a company cell phone did not breach the fundamental right to privacy; the conversations were not strictly private and related to work. As such, the employee's dismissal for misconduct discovered as a result of the monitoring was not null and void as the employee claimed. The dismissal was ultimately found to be unjustified, however, because the Court considered that the WhatsApp evidence supporting it had been obtained unlawfully.

Facts

The employee was employed by a transport company and was responsible for managing truck trips ordered by customers. The employee had a remote working agreement and used a company cell phone to make calls, send emails and communicate with her customers via WhatsApp. She submitted a monthly report to her employer on orders she had handled showing the purchase and sale prices set by the company.

The employer reviewed her WhatsApp conversations with customers and discovered that the monthly report that the employee sent to her manager showed different purchase and sale prices from the ones applied in practice. The incorrectly reported figures resulted in the employee earning more commission than she would have received based on the true figures. The employer dismissed the employee.

Fundamental right to privacy

The Court decided that the employee's fundamental right to privacy and secrecy of communications was not violated because the cell phone was provided by the employer and the conversations were not private but work-related. The employee therefore had no reasonable expectation of privacy in relation to the WhatsApp conversations reviewed by her employer. As there was no breach of the employee's fundamental rights the dismissal was not null and void as the employee claimed; had it not been valid the employer would have been required to reinstate the employee with back pay. The Court decided, however, that the dismissal was unjustified because in its view the WhatsApp evidence was obtained unlawfully so could not be taken into account in demonstrating the employee's misconduct. This meant that she was entitled to statutory severance compensation.

Comment

The Court's decision does not clearly explain why it considered that the evidence was unlawfully obtained. It is likely that that this was because the employer breached data protection and labor law requirements around informing the employee in a sufficiently detailed and clear manner about the rules on use of electronic devices provided by the company and did not expressly prohibit personal use.

What is most interesting about this decision is the distinction that the Court makes between a dismissal that violates a fundamental right to privacy - which would make the dismissal null and void - and a dismissal where the evidence is obtained unlawfully - in which case the dismissal would still stand but would be unjustified in the absence of any other evidence justifying disciplinary termination .

In light of the above, employers should ensure they have a clearly communicated policy on permitted use of company devices and that staff are informed that their activity on such devices may be monitored and potentially used in disciplinary proceedings.

Madrid High Court of Justice ruling dated 9 June 2023



Installation of geolocation tracking in company cars was an adequate and proportionate measure to monitor employee activity

In brief

The Castilla y León High Court of Justice found that the installation of a geolocation tracking system in the employee's company car was lawful. It did not breach privacy rights because the system did not capture images of the vehicle's occupants and monitoring was carried out exclusively during the working day. As a result, the employee's disciplinary dismissal based on data gathered from the geolocation system was justified and there was no right to compensation.

Facts

The employee was a sales representative for a company that sells and installs gaming and slot machines. He was provided with a company car exclusively for professional use to visit customers. The employee had been with the company for about five years when the employer informed its staff that geolocation tracking systems would be installed in their company cars. Staff were told that this would only be active during the working day and the data obtained would be used, among other things, to monitor employees' activity and if necessary, in disciplinary action.

The employee told his employer that he objected to the measure as he also used the car for personal purposes. The company nevertheless decided to install the system and did not inform the employee when this was done.

Some months later, at the employer's request, the employee prepared a list of his daily visits to customers during a specified period; this did not correspond with the data gathered from his company car. Ultimately the employer dismissed the employee for breach of good faith and trust for reporting false information regarding his customer visits.

Fundamental right to privacy

In the employee's claim in respect of his dismissal the Court found in favor of the employer on the basis that the installation of the geolocation tracking system was lawful and there was no breach of the fundamental right to privacy. This was because: (i) the company had informed the employee about the installation of the geolocation tracking system and the reasons for it; (ii) the system only registered when the car started and stopped and its location and did not capture images of its occupants and (iii) it only operated during the working day.

Additionally, although the employee objected to installation of the system, the Court confirmed that, within the employment framework, employee consent to the installation was not generally required.

In view of the facts, the Court concluded that the data gathered from the geolocation system could lawfully be used to show that the employee did not visit the customers he reported and support his disciplinary dismissal.

Comment

Though fact specific, this case shows that where the relevant requirements are met, employer rights to monitor employee activity can override individual employee rights to privacy. In this case the limitations on the monitoring in terms of the data captured meant that the geolocation tracking system could generally be considered to be a proportionate measure to monitor employee activity and therefore lawful.

Castilla y León High Court of Justice ruling dated 27 July 2023

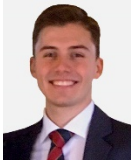
Authors and HR Privacy Leads for Spain



Maria Jose Martin
Team Leader, Madrid
+34 91 391 51 79
mariajose.martin@bakermckenzie.com



Patricia Perez
Team Leader, Madrid
+34 91 436 66 27
patricia.perez@bakermckenzie.com



Jorge Vidal
Associate, Madrid
+34 91 436 66 12
jorge.vidal@bakermckenzie.com

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com

© 2023 Baker & McKenzie LLP. All rights reserved. Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.