EMPLOYMENT LAW COMMENTARY

Volume 29, Issue 10
October 2017

San Francisco
Lloyd W. Aubry, Jr., Editor
Karen J. Kubin
Eric A. Tate

Palo Alto
Christine E. Lyon
Tom E. Wilson

Los Angeles
Tritia M. Murata
Timothy F. Ryan
Janie F. Schulman

New York
Miriam H. Wugmeister

London
Annabel Gillham

Berlin
Hanno Timner

Beijing
Paul D. McKenzie

Hong Kong
Stephen Birkett

Tokyo
Mitsuyoshi Saito

Sidebar:
What does Brexit mean for...

HOT TOPICS FOR MULTINATIONAL EMPLOYERS: PRIVACY IN THE WORKPLACE, THE EU GENERAL DATA PROTECTION REGULATION, AND BREXIT

by Hanno Timner, Annabel Gillham, Jens Wollesen, and Lara Sirimanne

Increasing digitalisation of the workplace means that many routine activities nowadays entail the processing of employees' personal information. Sophisticated data management tools allow for greater efficiency and help to identify and contain business risks. What often follows is harmonisation of HR data platforms within an employer's group of companies, seeking to

MORRISON FOERSTER

continued on page 2

deliver consistent and seamless HR management across business units and national borders.

With the growth of workplace digitalisation, employers need to ensure that their policies and procedures adapt to a growing awareness amongst the general population of privacy rights and to expanding regulatory requirements and oversight, especially in the European Union (EU). As of 25 May 2018, privacy law within the EU will be governed by the EU General Data Protection Regulation (GDPR). This framework updates and modernises the principles enshrined in the 20-year-old EU Data Protection Directive, and will be directly applicable in all EU Member States. Notably, the GDPR provides for an unprecedented sanctions framework, with fines of up to 4% or EUR 20 million of an undertaking, whichever is higher.

In this article, we consider three key areas that can become data privacy minefields for employers in the EU:

(1) *Conducting background checks, or vetting staff or potential hires*: in the EU, in-depth screening is only permitted on an exceptional basis;

(2) *Monitoring IT equipment and workplace correspondence, both on a systematic basis and as a one-off (e.g., into suspected misconduct)*: getting it wrong can be costly, as EU laws can require significant works-council involvement and may result in criminal liability in some cases; and

(3) *Transferring employee data outside the EU*: where an employer seeks to integrate its workforce planning tools with affiliates in the EU, it will need to be mindful of the restrictions on data transfers under the EU privacy regime.

The UK will leave the EU in March 2019. In the sidebar adjacent, we consider the impact of Brexit on UK employee data privacy rights and wider UK employment law.

PRE-EMPLOYMENT SCREENING

It has become common practice for employers to check the internet for publicly available content about job candidates. However, just because information is publicly available does not mean an employer should review it. A recently published

What does Brexit mean for...

–the UK legislative system?

Amidst all the politics and speculation, there are few responses we can give to this question with confidence. The UK is due to leave the European Union at midnight on 29 March 2019. We know that, as things stand, the draft European Union (Withdrawal) Bill 2017 – coined as the Great Repeal Bill – will end the primacy of EU law with, effective from the point at which the UK exits. At that point, most EU law (as it stands at midnight at the point of exit) will be converted into domestic law. Existing judgments of the Court of Justice of the European Union will continue to be given effect in domestic law at the point of exit and until overturned by subsequent UK legislation or judgments of the UK Supreme Court. We also know that the UK Government's current estimate for the length of a transitional period is two years after exit. Therefore, it seems unlikely that substantive changes will be made to EU-derived employment laws until 2021 at the earliest. After this, however, the UK legislature would be free to (in the language of the Bill) "amend, repeal and revoke" these laws as necessary (with, of course, whatever constraints membership or access to the EU single market requires).

–the GDPR?

It is difficult to make informed predictions as to how the legislature may choose to amend the domestic provisions of the GDPR after Brexit; however, there is a variety of potential issues:

- International data transfers – In order to "maintain the unhindered flow of data" — one of the Government's main objectives — from EU trading partners, the UK will need a formal adequacy decision from the European Commission as any other non-EU "third country" would. Any delays in the issuance of a formal decision will

continued on page 3

opinion by the Article 29 Working Party (WP29), an advisory body made up of a representative from the data protection authority of each EU Member State, provides useful guidance in determining whether employers may use information collected online. As far as social media platforms are concerned, a distinction is made between social media for mainly private purposes and social media for mainly professional purposes. The WP29 stresses that employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to use that information for their own purposes. Much depends on the source of the information. Employers will typically have a legitimate interest in reviewing candidates' profiles on LinkedIn and other sites, which contain information relevant to the candidates' professional qualifications. Social media such as Facebook and Twitter, on the other hand, contains private content that is typically irrelevant to the candidate's application and is therefore off-limits. Searches on public websites and via search engines such as Google serve a legitimate interest, if they are limited to information relevant to a candidate's position.

Information provided by the candidate during the application process may be used, and the employer is free to verify this information and contact references provided by the candidate for this purpose. However, this process should again focus on *relevant information* and should not be used as an opportunity to gather unrelated information, such as on the candidate's private life or any health issues (save where the information is necessary in order to make reasonable adjustments to the recruitment or interview process for disabled candidates) or union activities. In the UK, questions about health (other than information necessary to make reasonable adjustments for disabled candidates) would only be defensible after an offer of employment has been made.

Whether information is relevant will depend on the specific position in question. For example, checks on a candidate's financial probity or criminal background checks may be appropriate for some positions, e.g., to screen delivery staff for past road traffic offences. For other positions, such as in securities trading, they may even be required by local law. For most jobs, however, a criminal background check will not be relevant and is prohibited. Similarly, drug tests will only be permitted on an exceptional basis, e.g., where the

cause disruption to trade and to the free movement of data, one of the primary objectives of the GDPR. This issue is high on the Government's agenda, and it has made clear its commitment to the highest standards of data protection for the UK.

- Supervisory authorities – For many international organisations headquartered in the UK, their "lead" supervisory authority for GDPR purposes will be the Information Commissioner's Office (ICO), the UK's supervisory authority, as this is the location of their main establishment. Therefore, once the UK is no longer an EU member state, these organisations will need to choose, as far as they are able to, an alternative state's supervisory authority to be their "lead" authority. Although the GDPR harmonises the enforcement powers across all supervisory authorities, consideration will still need to be given to the resources and practicalities associated with each, and which is preferable.

– UK employment law in general?

In the absence of a significant societal shift in attitudes towards workers' rights, we think it unlikely that a future legislature would choose to make any major deviations from EU employment laws. Aside from the fact that many domestic protections – for example, family leave rights, equal pay, race and disability discrimination laws – actually preceded and/or exceed those stipulated by EU laws, the UK will need to maintain a trading relationship with the EU, and this will likely involve maintenance of equivalent employment protections.

We have listed below a selection of regulatory areas that may be contenders for reform, and briefly indicated potential reforms that have been suggested:

- Agency workers – The regulations governing agency workers in the UK might

continued on page 4

position requires the employee to operate heavy machinery or vehicles.

The "relevance test" will also inform the applicable retention periods for data collected in the recruitment process. Personal information collected during the recruitment process should generally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the candidate. If data is required to justify the employer's rejection of a candidate, however, it may be kept for a longer period of time (not longer than the applicable statute of limitations). If employers wish to retain the candidate's information for future vacancies, they should obtain explicit consent (e.g., in their rejection notification). Consent is also required if, within a group of companies, affiliates intend to share candidates' information.

Candidates must receive fair notice about the processing of their data. Art. 14 GDPR provides a list of specific items to include in this notice and requires that notice be given, at the latest, one month after the processing. For reasons of transparency, it is advisable to provide notice beforehand by way of a privacy policy or similar document posted on the recruitment page. Where employers have established uniform recruitment policies or staff questionnaires, these may require works-council approval in some EU jurisdictions. Moreover, the employer's data protection officer, if there is one, may have to be involved when conducting background checks.

EMPLOYEE MONITORING

Monitoring employees has become standard practice in many workplaces, and the rapid adoption of new information technologies provides employers with an ever-increasing visibility over employee behaviours. At the same time, the reasons for monitoring can vary greatly. In some industries, monitoring may serve to ensure workers' safety in hazardous working environments or even be required by industry-specific regulation (e.g., in the financial services sector). Employers may monitor to check the smooth operation of their IT systems. For many employers, however, the primary motive for monitoring is to check employees' performance, detect misconduct, or ensure compliance with specific company policies and procedures.

Under the EU's privacy regime, any processing of personal information is permitted only if either the

be a candidate for complete repeal, as the requirement they impose on employers to provide agency workers equivalent benefits to permanent employees after 12 weeks is hugely unpopular with employers.

- Discrimination – A cap could be imposed on discrimination compensation (as with awards for unfair dismissal), or positive discrimination could be permitted in broader circumstances than is currently the case.
- Employee protection legislation on business transfers (TUPE) – Greater flexibility may be added to certain provisions of TUPE to lift the current restrictions on changing terms of employment post-transfer, allowing businesses greater flexibility to harmonise employment terms.
- Annual leave/holiday pay – Various aspects of holiday provisions are unpopular with UK businesses, including the right to accrue holiday while on sick leave, and the ECJ's ruling that holiday pay can include all aspects of remuneration, including overtime and commissions. The UK may elect to restrict holiday pay to basic pay and limit the right to accrue/carry it over.

Although it has been almost a year since the UK gave notice to leave the EU, the terms of exit are far from being agreed with the EU, and this may have a bearing on the approach the UK takes to its legislative regime post-Brexit. However, it is unlikely that there will be significant change in the employment law field in the short term. The more immediate impact will be the immigration status of EU workers in the UK (and UK workers in the rest of the EU). In the short term, many UK employers are auditing their EU workforce to ensure that they maximise the chances of EU workers receiving settlement status and indefinite leave to remain in the UK post-Brexit.

individual consents or the employer can rely on a basis stipulated under statutory privacy law. The WP29 has, however, consistently stressed that employers should not rely on employees' consent to workplace monitoring (with few exceptions). This is because of the inequality in bargaining power between employer and employee, which calls into question whether employees can ever validly consent. The WP29 reasons that employees are in a situation of dependence and might fear adverse consequences if they refuse to consent. Monitoring may be permissible where it is required in order to perform the employment contract or serves legitimate interests of the employer, provided the monitoring is strictly necessary for a legitimate purpose and complies with the "principles of proportionality and subsidiarity." The "proportionality test" requires the employer to balance its business needs with the counterweighing privacy interests of the affected employees, taking into account, *inter alia*, the degree of invasiveness and potential consequences for the employee's private life. "Subsidiarity" means that the employer should first investigate other, less invasive means to protect its interests. For example, monitoring of every online activity of the employees is usually disproportionate. The WP29 stresses that prevention should be given much more weight than detection, as the employer's interests are better served by preventing IT misuse through technical measures (such as blocking certain websites) than by expending resources in detecting misuse.

These principles have been confirmed by a recent judgement of the European Court of Human Rights in Strasbourg (ECHR – not to be confused with the Court of Justice of the European Union in Luxembourg). In the case before the Court, a Romanian employee, Mr. Bărbulescu, had used his workplace email account to exchange private messages with his fiancée and his brother – and was subsequently dismissed. His employer had recorded his messages and introduced the transcriptions as evidence in the dismissal procedure. While the employer had expressly forbidden personal use of company resources, it was unclear whether he had been given adequate notice of this policy. The Court ruled that the monitoring had breached Mr. Bărbulescu's right to respect for private life per Article 8 of the European Convention on Human Rights. The Court recurred to the principles of proportionality and subsidiarity and held that the employer had failed to substantiate a legitimate reason for the monitoring and take into account potential repercussions for the employee (his fiancée had subsequently decided to end their relationship). The Court also stressed the need for proper notification, in particular of (i) the possibility that the employer may take measures to monitor communications, (ii) the implementation of such measures, and (iii) the extent of the monitoring (including whether it applies only to the flow or additionally to the content of communications and any limits in volume/portion, time, space, and number of individuals accessing the monitoring results).

As an example of good practice, monitoring should be subject to a prior privacy impact assessment. This vetting mechanism has been introduced under Art. 35 GDPR for high-risk processing activities and requires the employer to, *inter alia*, identify safeguards and security measures for the privacy risks arising from the anticipated processing (irrespective of the technology concerned or the capabilities the technology possesses). In addition, the conditions of potential monitoring should be transparently set out in a privacy policy, and employers should introduce acceptable-use policies, outlining the permissible use of the company's IT equipment, as well as its limits. In some countries, such as Germany, the introduction of technology capable of monitoring (even if it is not intended for that purpose) must also be negotiated with the works council. More generally, employers should be aware that the monitoring of employee communication is subject to country-specific regulation, in particular by local telecommunications and telemedia law. These regulations may impose even more stringent requirements, including criminal liability for violations of telecommunication secrecy.

TRANSFER OF EMPLOYEE DATA

Most US employers with UK operations are likely already aware of the potential barriers to data flows between the EU and the US In 2015, the once commonly used mechanism, known as the Safe Harbor regime (under which organisations receiving data in the US self-certified adherence to certain data privacy principles), became defunct after a ruling by the Court of Justice of the European Union that the regime did not provide adequate protection to personal information transferred from the EU. Whilst a replacement framework and self-certification regime (the "Privacy Shield") has now been approved by the European Commission, most multinational employers deal with cross-border transfers of employee data using "binding corporate rules" (if the transfer is intra-group) or European Commission–form "standard contractual clauses" (if the transfer is between the employer and a third party, and one of them is based outside the EU).

As part of preparation for GDPR, multinational employers should audit what employee data is transferred outside the EU and the purpose for which it is transferred and ensure that, to the extent such transfers are necessary, data is transferred securely and adequate mechanisms are in place (such as those described above) allowing the non-EU recipient to receive the data.

Employers are also well advised to keep an eye on Brexit negotiations to see what approach will be taken to UK data privacy standards post-Brexit. The UK will be subject to the GDPR prior to Brexit, but it remains to be seen whether it will be deemed to provide adequate protection post-Brexit to receive employee personal information from the EU.

CONCLUSION

Workplace digitalisation presents employers with vastly growing opportunities but brings along an array of new compliance risks as well. Within the European Union, the processing of employee data is subject to a number of stringent tests set out under statutory law. Most often, employees cannot waive the protection afforded to them by the law. Consequently, while employers are required to provide transparent notice, they will typically not be able to rely on employees' consent for their data processing.

As the GDPR enters into force on 25 May 2018, introducing an unprecedented catalogue of financial sanctions, the stakes will be rising considerably.

Employers are advised to review their processing operations, and implement any necessary changes, well before this deadline. Depending on the type of data processed, employers may be required to consult their data privacy officer (if there is one) and conduct a prior privacy impact assessment. Under local law in various EU Member States (such as Germany), the processing may also trigger works-council co-determination rights and even potential criminal liability, in particular where employee data falls under the protection of local telecommunication and telemedia law. The latter will typically be the case if the employer introduces technology that permits the monitoring of workplace communication, via phone, email, or other devices.

Hanno Timner is a partner in our Berlin office and can be reached at +49 (30) 72622-1235 or htimner@mofo.com.

Annabel Gillham is of counsel in our London office and can be reached at +44 (20) 7920 4147 or agillham@mofo.com.

Jens Wollesen is an associate in our Berlin office and can be reached at +49 (30) 72622-1259 or jwollesen@mofo.com.

Lara Sirimanne is an associate in our London office and can be reached at +44 (20) 7920 4182 or lsirimanne@mofo.com.

To view prior issues of the ELC, click here.