THOMSON REUTERS
Westlaw®

Guidance on processing personal information of employees

By Marijn L. Storm and Alex van der Wolk, *Morrison & Foerster*

JULY 28, 2017

Employers almost inevitably collect and use personal information of their employees. New technologies enable more systematic processing of personal information, creating significant challenges to privacy and data processing.

On June 8, 2017, the Article 29 Working Party ("WP29") issued an opinion on the processing of personal information of employees at work (the "Opinion").

In the Opinion, the WP29 discusses the proportionality of using these new technologies, which sheds some light on when such uses can be based on the employer's "legitimate interests."

The Opinion builds on the Opinion and Working Document on this subject, published by the WP29 in 2001 and 2002, which are available online at http://bit.ly/2trTycU and http://bit.ly/2tIj9JS.

> The Opinion applies to all situations where there is an employment relationship, regardless of the contractual basis of that relationship.

Although the Opinion mostly refers to the legal framework of the Data Protection Directive (the "DPD"), the Opinion also looks ahead towards the General Data Protection Regulation (the "GDPR").

KEY HIGHLIGHTS OF THE OPINION

There are a number of noteworthy elements to the Opinion, which we discuss below.

At the outset, the Opinion clarifies that where the term "employee" is used, it does not intend to restrict the scope merely to persons with an employment contract.

Over the past decades, new business models served by different types of labor relationships, such as on a freelance basis, have become more commonplace.

The WP29 stresses that the Opinion applies to all situations where there is an employment relationship, regardless of the contractual basis of that relationship.

Consent and other legal bases for processing employee information

The WP29 repeats a position that it has put forward in its previous opinions on the validity of employee consent: for the majority of the processing of personal information at work, the legal basis cannot and should not be the consent of the employee.

In the Opinion, the WP29 reiterates that in an employment context, there usually is a real or potential prejudice that arises from the employee refusing or revoking consent, as a result of which consent is not considered to be freely given and therefore not valid.

Furthermore, even if consent could be a valid legal basis (i.e., if it can be undoubtedly concluded that the consent is freely given), it must be a specific and informed indication of the employee's wishes. A lack of action, such as not changing default settings on devices, does not qualify as consent.

As a result of the general unavailability of consent as a legal basis, most of the processing of employee information will likely take place on the basis of performance of a contract (for instance where banking details are processed for making salary payments), legal obligations (where employment or other laws require the processing of personal information), or legitimate interest (which still requires that the interest is legitimate, that the processing is strictly necessary, and that it complies with the principles of proportionality and subsidiarity).

Data protection impact assessment

Regardless of the legal basis for the processing of personal information of employees, the employer should consider what measure(s) should be taken to ensure that the impact on the rights to private life and secrecy of communications are limited to a minimum. This can form part of a Data Protection Impact Assessment ("DPIA").

The WP29 states that, as an example of good practice, employers should undertake a DPIA prior to the introduction of any monitoring technology (irrespective of the technology concerned or the capabilities the technology possesses).

The Opinion also explicitly mentions DPIAs in the context of automated decision making and profiling involving employees (i.e., where systematic and extensive evaluation of personal aspects related to individuals is concerned, based on automated processing and where such decisions produce legal effects or similarly significantly affects individuals).

Finally, the Opinion mentions that a DPIA should be carried out specifically in the context introducing Mobile Device Management ("MDM," which allows employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand) to the company.

Employee monitoring – general

A key topic of the Opinion is the monitoring of employees and employee behavior.

The Opinion references a number of technologies that allow for more possibilities to monitor employees over time, across workplaces and at their homes, such as GPS-tracking of smartphones and vehicles, monitoring IT usage, the use of data loss prevention ("DLP") tools, Next-Generation Firewalls ("NGFWs"), Unified Threat Management ("UTM") systems, Transport Layer Security ("TLS") interception, website filtering, content filtering, on-appliance reporting, security applications and measures that involve logging employee access to the employer's systems (security and network log monitoring), eDiscovery technology, Bring-Your-Own-Device ("BYOD"), MDM technology, the use of wearable devices (e.g., health and fitness devices), and the use of CCTV (with or without facial recognition software).

New forms of monitoring, such as monitoring the use of online services or location data from a smart device, are much less visible to employees than other, more traditional types of monitoring such as overt CCTV cameras.

Therefore, the employer should provide and make readily available a monitoring policy concerning the purposes for when, and by whom, the monitored data can be accessed in order to also guide them about acceptable and unacceptable use of the network and facilities.

Moreover, mitigating measures should be put in place to balance the impact monitoring efforts can have on employees, such as geographical limitations (ensuring that employees are only monitored in specific places) and time-related limitations (ensuring that monitoring takes place on an incidental basis, rather than continuously, as well as during business hours only).

The transparency requirements (art. 10 and 11 DPD and art. 13 and 14 GDPR) demand that employees are provided with effective information on any monitoring activities, the purposes of the monitoring, and the possibilities for employees to prevent their data from being captured by monitoring technologies.

Regarding privacy policies and notices, the WP29 recommends involving a representative sample of employees in the creation and evaluation of such policies and notices.

The Opinion also notes that extensive use of monitoring technologies may limit employees' willingness and possibility to inform employers on irregularities that may damage the business.

In this way, extensive monitoring may make the internal whistle-blower policies ineffective.

Monitoring IT usage

Monitoring of IT usage may generate large amounts of data. In combination with techniques for data analysis and cross-matching, this creates the risk of incompatible further processing.

Examples of incompatible further processing are the use of WiFi-geolocation to track the behavior or performance of employees or the use of a security system to track the performance of employees.

> For the majority of the processing of personal information at work, the legal basis cannot and should not be the consent of the employee.

The WP29 stresses that this risk is not limited to the analysis of the contents of employee communications. The analysis of metadata about a person might allow for an equally privacy-invasive detailed monitoring of an individual's life.

Generally, prevention should be given more weight than detection — the interests of the employee are better served by preventing internet misuse through technical means than by expending resources in detecting misuse.

For example, where the prohibited use of communications services can be prevented by blocking certain websites (instead of continuously monitoring all communications) blocking should be chosen.

Where monitoring internet traffic takes place, the employer should — by way of good practice — provide an alternative for unmonitored access for employees, such as a free Wi-Fi network or specific devices where employees can exercise their legitimate right to use work facilities for some extent of private use.

The Opinion furthermore mentions that the use of Data Loss Prevention tools, which monitor outgoing communication in order to prevent data breaches, can be based on the legitimate interest of the employer.

However, there may be risks of unnecessary processing of personal information (e.g., in case of "false positives"), which ought to be mitigated (and for which the Opinion provides several suggestions).

Cloud services

In some cases, the monitoring of employees is already made possible because employees are expected to use online applications such as document editors, calendars, and social networks.

Employees should be enabled to designate certain private spaces to which the employer may not gain access unless under exceptional circumstances. This, for example, is relevant for calendars, which are often also used for private appointments.

Monitoring devices

The WP29 notes the rise in BYOD policies and acknowledges that some use of the device will be personal in nature. This presents employers with a challenge of avoiding to monitor private information while serving the legitimate interest to protect business and personal information of the employer.

This can only be done if there are adequate means to distinguish between privacy and business uses of the device (for instance by "sandboxing" the business applications on the mobile device).

Wearable devices

The Opinion also contains information on the use of wearable devices. The WP29 notes the increased use of wearable devices, which often involves the processing of sensitive personal information.

The employer cannot use the employees' consent as a basis for processing this information as employee consent is generally not considered valid.

Even if the employer were to use a third party to collect the health data and use the aggregated data, the processing would be unlawful.

As described in Opinion 5/2014 on Anonymisation Techniques, which is available online at http://bit.ly/1qJ5StX, it is very difficult to ensure complete anonymization of the data as the employer would be able to single out employees with particular health conditions such as obesity.

In sum, it would be generally prohibited for employers to receive any sensitive personal information generated in the context of wearable devices.

Monitoring vehicles

Any employer using vehicle telematics will be collecting data about both the vehicle and the employee using that vehicle, including information on the GPS location and possibly information on other driving behavior.

The employer might be obliged to track the vehicle to ensure the safety of employees who drive those vehicles or have a legitimate interest in being able to locate the vehicle at any time.

However, even if the employer has a legitimate interest, it should first be assessed whether the processing for these purposes is necessary and whether the actual implementation complies with the principles of proportionality and subsidiarity.

If private use the vehicle is allowed, the employer should ensure the possibility of an opt-out: the employee should have the option to temporarily turn off location tracking when special circumstances justify this turning off, such as a visit to a doctor.

The employee must also be clearly informed that their use of the vehicle is recorded. Preferably, such information should be displayed prominently in every car within eyesight of the driver.

Event data recorders enable employers to process a significant amount of personal information in case of, for example, an accident.

These systems record video (possibly including sound) in certain situations, e.g., in case of sudden braking or abrupt directional change, or continuously. The use of event data recorders can only be lawful if there is a necessity to process the ensuing personal data about the employee for a legitimate purpose.

The WP29 notes explicitly that these systems cannot be used with the purpose to improve the driving skills of employees, as other, less invasive methods exist (e.g., the installation of equipment that prevents the use of mobile phones).

Furthermore, employers should realize event data recorders may also film third parties (such as pedestrians), for which the employer would not have a legitimate interest.

Recruitment

Employers should not assume that the fact that a social media profile of a job applicant is publicly available automatically allows the employer to process personal information contained in the profile.

Any such processing requires a legal ground (which, the Opinion mentions, could be legitimate interest), and the employer should take into account whether or not it concerns a private or business social media account.

In general, employers should only use personal information from a social media account to the extent this is necessary for and relevant to the performance of the (potential) job (for example in order to be able to assess specific risks regarding candidates for a specific function).

Personal information collected during the recruitment process should generally be deleted as soon as it is clear no job offer will be made or the job offer is not accepted, and the individual must be correctly informed of the processing before the start of the recruitment process.

In-employment screening

The WP29 notes that in-employment screening of employees' social media profiles (i.e., the continuous screening of employees' profiles to collect information regarding their friends, opinions, beliefs, interests, habits, whereabouts,

attitudes, and behaviors) should not take place on a generalized basis.

In addition, employers should not require employees to use a corporate social media profile by their employer, even if this is a natural result of a specific task (e.g., a spokesperson).

The Opinion is also available at http://bit.ly/2sY8v4h.

This article appeared in the July 28, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHORS

Marijn L. Storm (L) is an associate based in the Brussels office of **Morrison & Foerster** and is a member of its data privacy group. He can be reached at mstorm@mofo.com. **Alex van der Wolk** (R) is a partner in the firm's Brussels and London offices. He advises global companies on data protection strategy and compliance governing all aspects of information management. He can be reached at avanderwolk@mofo.com. This expert analysis first appeared as a July 11 client alert. Republished with permission.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.