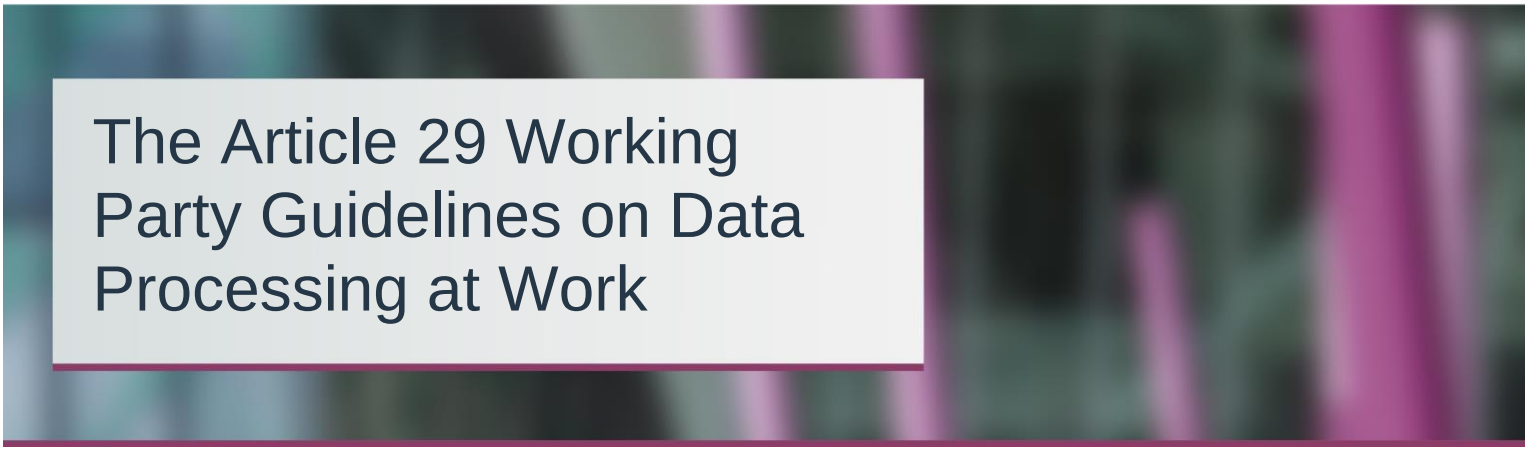
WILLIAM FRY

// PRIVACY SOURCE



The Article 29 Working Party Guidelines on Data Processing at Work

The Article 29 Working Party (now called the European Data Protection Board ("**EDPB**") adopted guidelines on data processing at work, in June 2017. These guidelines consider the data protection implications of the latest types of systematic monitoring of employee personal data by employers in light of technological advancements in the workplace. The guidelines focus on the balance between the legitimate interests of employers and the reasonable expectation of privacy of employees in the workplace by outlining the risks posed by new technologies and by providing an assessment of the necessity and proportionality of such new technologies. The EDPB assesses a number of scenarios in which new technologies are deployed and analyse how employers can process employee personal data in a proportionate manner.

This InFocus article will detail the EDPB guidelines.

Background

Employers are rapidly adopting new technologies in the workplace. These technologies are cheaper than ever before and their capacity for the processing of personal data has increased exponentially allowing for new types of systematic and potentially invasive data processing of employee personal data. While these technologies have many benefits on the surface (e.g. they can help detect or prevent the loss of company property and improve employee productivity), they also create significant privacy and data protection challenges. New forms of processing vis-à-vis new technologies are less visible to employees than more traditional methods such as CCTV. The EDPB provides that "the boundaries between work and home have become increasingly blurred" (e.g. employees now work off-site and remotely).

The EDPB emphasises that the development of new technologies makes it even more important for employers to apply the fundamental data protection principles under Directive 95/46/EC and the General Data Protection Regulation (GDPR) when processing employee personal data.

Principles of Data Protection

Under data protection law, employers must apply and comply with the principles of data protection and should:

- have a legal basis to process employee personal data;
- ensure that data are processed for specified **legitimate purposes** that are **proportionate and necessary;**
- take into account the principle of **purpose limitation**, while making sure that the data are **adequate**, **relevant**, and not **excessive** for the legitimate purpose;
- apply the principles of **proportionality** and **subsidiarity** regardless of the applicable legal ground for processing employee personal data; and
- be **transparent** with employees about the **use** and **purpose** of monitoring technologies.

Furthermore, employers must invoke and enable the exercise of employee data protection rights such as the rights of **access**, **rectification**, **erasure**, **data portability** and **objection** in relation to employee personal data and in relation to **automated decision making**. Employers must also take all necessary measures to protect the data against unauthorised access and destruction.

In order to put these principles into context in the context of new technologies, the EDPB focuses on key practical scenarios where employee personal data are processed using new technologies.

Risks

The EDPB also considers the risks associated by employers using new technologies which involve the processing of employee personal data.

Modern technologies enable employees to be tracked over time by a variety of different devices including smartphones, desktops, tablets, vehicles and wearables both in their workplaces and at home. Due to the increased capabilities of these new technologies employees may not be aware of what personal data are being processed or for what purposes. This has the potential to affect the fundamental rights and freedoms of employees, such as their rights to communicate confidentially and to access information. In some cases, employees may not even be aware of the existence of the monitoring technology itself.

Data are being utilised in the workplace environment in unprecedented ways and there are risks associated with the "over-collection" of data by new technologies. These new techniques create risks of incompatible further processing of data, for instance where an employer uses data of a geolocation system (such as WiFi or Bluetooth tracking) to constantly check an employee's movements and behaviour.

Without the appropriate protections, there is a high risk that employers' legitimate interests in increasing employee efficiencies and protecting company assets may turn into unjustifiable and intrusive monitoring which will impact upon the privacy rights of employees and which may mean that employers risk breaching data protection legislation.

Scenarios

The EDPB guidelines address a number of scenarios in which the new technologies and/or developments of existing technologies have the

potential to result in high risks to employee personal data and right to privacy. We have provided a high-level overview.

1. Processing operations during the Recruitment Process: Inspection of Social Media and Networks.

The EDPB states that employers must have a legal basis for processing the personal data of a potential employee, where such data are publicly available and accessed by an employer on a social media network. The EDPB further recommends that employers are only allowed to process such data to the extent that it is necessary and relevant to the performance of the job which is being applied for and the individual must be informed of any such processing before s/he engages in the recruitment process (e.g. in the text of the job advertisement).

2. Processing operations: in- employment screening

The social media profiles of employees are often publicly available. This fact, combined with new analytical technologies, means that employers have potential access to a wealth of information concerning employees' private and family lives (and potentially, sensitive personal data). The EDPB states that in-employment screening of employees' social media profiles should not take place on a generalised basis. Further, employers should refrain from requiring that an employee provide access to

information that s/he shares with others through social networking. The EDPB states that employees should not be required to utilise a social media profile that is provided by their employer. If a work social media profile is necessary in light of the employee's role (e.g. organisation spokesperson) the option for an employee to use a separate non-work, non-public profile must be provided to such an employee.

3. Processing operations during employment

New technological developments of IT monitoring tools such as Data Loss Prevention tools, Next-Generation Firewalls, Unified Threat Management Systems and Security Applications enable potentially intrusive monitoring of employee personal data, notwithstanding the fact that an employer may have a legitimate interest in deploying these technologies. The EDPB clarifies that monitoring every online activity of employees is generally a disproportionate response and an interference with the right to data protection and privacy of employees. The EDPB states that employers need to investigate the **least invasive means** to implement these technologies and, if possible, configure applications to prevent permanent logging of employee activity.

It is often the case that monitoring by employers is possible because employees are expected to use online applications provided by the employer which process personal data (e.g. cloud based applications such as document editors, calendars and social networking). The EDPB recommends that employees should be able to designate certain "private spaces" to which employers cannot gain access except under exceptional circumstances.

The EDPB also emphasises that the principle of subsidiarity may mean that no monitoring can take place at all. Prevention should be given more weight than detection. For example, where it is possible to block websites rather than continuously monitor all communications, this option should be preferred.

4. Processing operations: monitoring ICT usage outside the workplace

Monitoring of Home and Remote Working

An increasing number of employees are working remotely. This poses additional risks for employers such as the risk of company information being lost or destroyed as the same physical security measures will generally not be in place at an employee's home. Employers may be of the view that, in order to mitigate such a risk, there is justification for using software packages that have the capabilities of logging keystrokes and mouse movements, screen capturing and logging of applications used and enabling webcams and collecting webcam footage. The EDPB advises that such processing is disproportionate and employers are unlikely to be able to rely on the "legitimate interest of the employer" as a legal basis for processing such data.

Bring Your Own Device (BYOD)

Where employees are using their own devices to carry out their duties of employment, the device will sometimes also be used for personal purposes. Consequently, this could lead to employers processing private/non-corporate information about the employee and any family members who use the device. The EDPB advises that appropriate measures should be put

in place to prevent the monitoring of such private information. If there is no way for an employer to prevent the monitoring of such private information, employers may need to consider prohibiting employees from using work devices for private purposes.

Mobile Device Management (MDM)

The EDPB provides that employers who are deploying any new MDM technology for the first time need to carry out a Data Protection Impact Assessment (DPIA). The EDPB emphasises that data collected as part of remote location capabilities should be processed for a specified purpose only and should not

form part of a wider programme enabling ongoing monitoring of employees. Furthermore, any tracking features should be mitigated – for example, location data should only become available to the employer when a device is lost or stolen.

Wearable Devices

Many employers are providing wearable devices to employees in order to track and monitor their health and activity at work and, sometimes, at home. The EDPB provides that the ensuing information from these devices should only be available to the employee and not to the employer. Even if the employer uses a third party to collect the health data and provide solely aggregated information about general health developments to the employer, this would still be unlawful for the purposes of data protection law. This is because it is very difficult to ensure the data remain completely anonymous and (even in a relatively large work environment) employers would still be able to single out individual employees with health issues given the availability of other data about the employees.

5. Processing Operations: time and attendance

New technologies, including those that process biometric data (e.g. finger prints or facial recognition) as well as mobile device tracking, are increasingly deployed by employers to control who enters and exits their premises. The EDPB provides that the continuous monitoring of the frequency and exact entrance and exit times of employees cannot be justified if these data are also used for another purpose, such as employee performance evaluation.

6. Processing Operations: video monitoring systems

The EDPB recommends that employers should generally refrain from the use of facial recognition technologies in order to identify deviations from predefined movement patterns, as this type of processing is likely to involve processing and, possibly, automated decision making.

7. Processing Operations: tracking vehicles used by employees / event data recorders.

The EDPB acknowledges that employers may have a legitimate interest in installing a tracking device in a vehicle (such as being able to locate a vehicle) or that an employer may have to install such a device to demonstrate compliance with legal obligations (such as health and safety obligations). However, even if an employer has a legal basis for installing a tracking device, such an employer should consider whether it is **necessary** and **proportionate** to use such technologies. The EDPB states that employees must be informed that a tracking device or event data recorder has been installed and that their movements and possibly their driving behaviour) are being recorded. It also states that this information should be displayed prominently in every car, within the eyesight of the driver.

8. Processing Operations: disclosure of employee data to third parties

It has become increasingly common for employers to transmit employee personal data to their customers to ensure reliable service provision and consumer trust e.g. a delivery company sending customers e-mails with a link to the name, location, and photo of the employee delivering goods. The EDPB considers that it is neither **necessary** nor **appropriate** for employers to provide the name and photo of their employees to customers. An employer, in such a scenario, would not be able to rely on its "legitimate interest".

9. Processing Operations: international transfers of HR and other data

Employers are increasingly using cloud-based applications and services (such as those designed for the handling of HR-data as well as online office applications). The guidelines note that this use will likely result in the international transfer of employee personal data. Employers should ensure that personal

data transferred to a third country outside the EU takes place only where an adequate level of protection is ensured to safeguard the transfer of personal data and that the data shared outside the EU/EEA (and any subsequent access by other entities within the company group) remains limited to the minimum necessary for the intended purposes.

GDPR

Some of the GDPR obligations the EDPB looked at include:

- the requirement for employers to implement the principles of data protection "by design and default" in all data processing activities and projects. This means, for example, where an employer provides devices to its employees, the most privacy-friendly settings must be selected if tracking technologies are involved. It also means that data protection should not be an afterthought but rather built into all processes and procedures.
- the requirement for employers to carry out DPIAs where (amongst other considerations) the processing (especially processing using new technologies) is likely to result in a high risk to the fundamental rights and freedoms of employees. Where a DPIA indicates that the risks identified remain high and cannot be sufficiently addressed by the employer, then the employer will need to contact the Data Protection Commission prior to the commencement of the processing.

Recommended Next Steps

Based on the EDPB guidelines, it is recommended that employers:

- consider what legal basis they are relying upon to legitimise the processing of the employee personal data;
- consider whether the technologies they are using are necessary and proportionate and whether any additional actions can be taken to mitigate or reduce impact of the data processing being carried out on the right to privacy of employees;
- If they have not already, start the process of maintaining up-to-date records of their processing activities;
- provide ongoing training on data protection to employees; and
- establish and document policies and procedures, such as a BYOD Policy and recruitment procedures, to reflect the EDPB recommendations and the requirements of the GDPR.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA