Helping you succeed in tomorrow's world

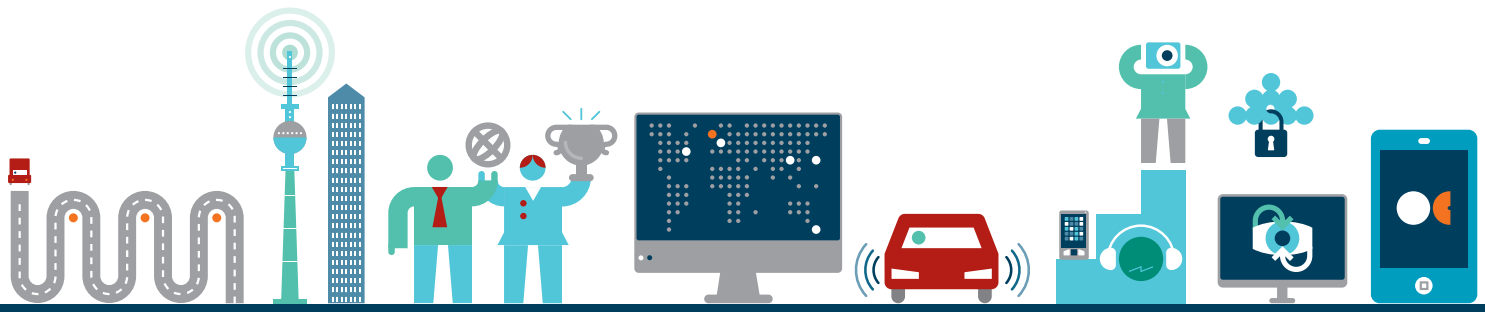
Article 29 Working Party issues new Opinion on data processing at work

Shortly before the summer break, the Article 29 Data Protection Working Party (WP29) issued an opinion 2/2017 on data processing at work (the Opinion).

The Opinion is an update/restatement of the WP29's previous opinions (WP48 and WP55). The WP29 continues to push for a broad interpretation of "employment", as covering not only employment contracts but also agreements with contractors and freelancers, etc.

The Opinion expresses both general advice as well as practical recommendations, commonly accepted by all EU data protection authorities, of what employers should consider when implementing collective measures involving the processing of employee/contractor personal data. These guidelines do not prevent the employer from taking appropriate measures in individual situations, subject to a careful assessment on a case-by-case basis. The WP29 continues to stress the importance of maintaining a balance between on the one hand the employers' interests (including of an economic or business nature or related to the company's or employees' security and safety etc.) and on the other hand maintaining privacy at work.

The Opinion is particularly important and timely considering that the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) leaves the Member States some leeway to regulate the processing of personal data in employment relationships (see article 88 of the GDPR), especially in relation to recruitment, performance at work, management, planning and organisation of work equality and diversity, health and safety, protection of employer's or customer's property, the exercise and enjoyment of employment related rights and benefits and the termination of the employment relationship. Article 88(2) of the GDPR provides that the supplementary rules adopted by the Member States should include 'suitable and specific' measures to protect employees' fundamental rights and interests, with particular regard to: (i) the transparency of processing, (ii) the transfer of employee data within a group of companies or a group of enterprises engaged in a joint economic activity and (iii) monitoring systems at the workplace. It is in relation to these requirements that the WP29 provides further guidance to employers. including by describing such safeguarding measures in 9 practical scenarios (ranging from recruitment, employment screening, ICT monitoring inside and outside the workplace, time and attendance management, video monitoring, fleet vehicles, disclosure to third parties and international transfers).



General overview

The WP29 starts by describing the context in which systematic and potentially invasive data processing at work may occur. This includes:

- The ever increasing capacity of data processing technologies, versus their decreasing cost of implementation;
- The existence of more opaque surveillance techniques such as the use of location data on smart devices or miniature cameras and microchips; and
- The blurred boundaries between home and work life (e.g. monitoring of activities when working from home, undertaking business travels, etc. may inadvertently lead to monitoring of the employee or contractor in a private context.).

Practical recommendations

Rather than restating the 9 scenarios developed by the WP29, we focus on a number of practical points put forward by the WP29.

Generally speaking, the WP29 acknowledges that employers do have a legitimate interest in protecting the company's assets, proprietary information, etc., which may even justify more advanced forms of employee monitoring or tracking. However, the WP29 stresses the importance of taking into account – among other things - the principles of transparency (informing the employees about such monitoring or tracking) and purpose-limitation (refraining from using information collected for one purpose, e.g. to control access to a secured data centre, for other purposes, such as evaluating the performance of employees working in that data centre).

These principles also apply where **fleet or company vehicles are being tracked** ("geo-tracking"), and the Opinion offers a number of practical suggestions in that respect, including among other things:

- Employers should always inform employees that a tracking device has been installed in the vehicle, that their movements are being recorded and that their driving behaviour may also be recorded (depending on the technology used). The WP29 suggests displaying that information prominently in the car, within the driver's view.
- Employees should have the option to temporarily turn off the location tracking, e.g. for private trips.
- Vehicle locations should not be tracked outside agreed working hours, unless for instance when a necessity exist (and even in that case employers must consider an implementation proportionate to the risks). For example, in order to prevent theft, a fleet vehicle is not monitored outside of working hours, unless the vehicle leaves a widely defined circle (region or even country)In addition, employers must in that case ensure that the location is only shown in a "break-the-glass" kind of way, i.e. visibility of the location is only activated (thereby accessing the data already stored by the system) when the vehicle leaves a predefined region.
- Employers must ensure that the data resulting from tracking fleet vehicles is not used for illegitimate further processing, such as the tracking or monitoring of employees' performance at work.

Where specific technologies are concerned, such as using employees' **biometric data or facial recognition technologies**, the WP29 generally holds the view that the fundamental rights and freedoms of employees prevail and that employers should refrain from the use of such technologies employers.

With respect to **mobile device management**, the WP29 notes that technology makes it possible to locate devices, deploy specific configurations or applications, record or locate the device in real time, and delete data on demand. Therefore, the WP29 concludes that a data protection impact assessment must be conducted before deploying such technology, at least where it is new or new to the employer. The WP29 stresses that even where such technology appears to be necessary and proportionate, employers must ensure that the data collected cannot form part of a wider programme enabling the on-going monitoring of employees, and calls for a limitation of the tracking features and systems.

Finally, below you will find some more practical do's and don'ts, put forward by the WP29 and relating to new(er) technological possibilities, which are becoming more and more commonplace on the work-floor.

Social media profiles:
- used for recruitment & employment screening;
- used by current employees

Job candidates/Potential employees:

- **Do not** use social media profiles to screen applicants, unless: (i) there is a legal ground to do so (such e.g. legitimate interest) ;(ii) the social media profile of the applicant is business-related, and (ii) to the extent that the profile information collected is absolutely necessary and relevant to assess the applicant's abilities for the job, e.g. if it is necessary to assess specific risks regarding candidates for a specific function;
- **Do not** require potential employees to "friend" the potential employer or otherwise require them to provide access to their social media profiles;
- **Do** inform candidates (e.g. in the text of the job advert) before they engage with the recruitment process that their social media profile is likely to be investigated;
- **Do** delete data collected during the recruitment process as soon as it becomes clear that an offer of employment will not be made or is not accepted by the applicant.

Current employees:

- **Do not** require employees to "friend" their employer or otherwise require them to provide access to their social media profiles;
- **Do not** require employees to use a social media profile provided by their employer, as they must retain the option of a "non-work" social media profile – which, according to the WP29, should be specified in the employment contract;
- **Do not** screen social media profiles of employees (on a generalised basis);
- **Do** note that specific monitoring of former employees for the duration of their non-compete clauses may be deemed acceptable, provided that (i) the employer can prove that such monitoring is necessary to protect his legitimate interests; (ii) there are no other, less invasive, means available; and (iii) the former employees have been adequately informed on the (extent of the) regular observation of their public communications.

Monitoring ICT usage at the workplace

- **Do** consider proportionality and necessity prior to implementing any type of monitoring solution and refrain from systematically monitoring every online activity of employees on the company's network, or their e-mail exchange (such as by means of TLS traffic inspection appliances and Data Loss Prevention tools), as there will usually be other, less intrusive, means of protecting the company's network and assets (e.g., blocking specific websites is less intrusive than continuously monitoring all communications).
- **Do** set up such monitoring tools to prevent permanent logging of all activities (especially when no incidents have been detected).Do set up the same tools to avoid monitoring websites or resources that are part of the employees' legitimate private use, such as private webmails, online banking sites or tools, or health websites. §
- **Do** When an incident is detected, instead of logging everything systematically, the system should block the suspicious content temporarily and notify the employee to allow him to ask for review of the blocking decision, or to give him the option to cancel a potentially suspicious communication (e.g. in the case of "false positives").
- **Do** be transparent and sufficiently detailed about the acceptable and non-acceptable use of the company's network and facilities, about the type of communications that are being monitored and about the rules followed by the monitoring tools to classify activity, information or communications as suspicious or not (all to be described in the acceptable use policy).
- **Do** focus on the prevention of internet misuses rather than on detection. It serves the interest of the employer better and is less intrusive of the employee's privacy.
- **Do** - to the extent possible - involve employees in the assessment of the monitoring policy (including regarding necessity of the monitoring and the logic and accessibility of the policy).
- **Do** re-evaluate – preferably on an annual basis - the acceptable use policy, to assess whether the monitoring solution delivers the intended results and whether less intrusive means could achieve the same results/purpose.
- **Do** provide (as a recommended best practice) employees with the possibility of unmonitored access, so that they may exercise their right to use the network for private usage, e.g. by means of free WiFi or stand-alone devices (with appropriate safeguards to ensure confidentiality of the communications), but also by means of 'privacy' options/features or settings in the use of cloud-based office applications (e.g. calendar or tasks items marked as "private", etc.).

Home and remote working, Bring Your Own Device, mobile device management and wearables

- **Do not** deploy advanced monitoring of home and remote working devices, such as logging keystrokes and mouse movements, screen capturing, enabling webcams or collecting the footage thereof or logging applications used.
- **Do** implement measures so that you are able to distinguish between private and business use of the device, and to securely transfer business data from the device to the network.
- **Do not** access sections of remote devices that are presumed to be private, such as folders containing pictures taken with the device.
- **Do not** distribute wearable devices collecting health information about employees unless such health data is only accessible to the employee and not the employer. Also when choosing the device or service, the employer should evaluate the privacy policy of the manufacturer and/or service provider, to ensure that it does give way to unlawful processing of health data on employees.

International HR data transfers

- **Do** ensure compliance with the GDPR when using online office or cloud-based applications and services designed for the handling of HR data, especially when resulting in employee personal data being transferred outside of the EEA; Do opt for relying on adequate protection rather than the derogations listed in article 26 of the current data protection directive (article 49 of the GDPR);
- **Do** ensure that the transfer of HR data outside of the EU/EEA, and their subsequent access by other entities within the group, remains limited to the minimum necessary for the intended purposes.

Osborne Clarke comment

Implementing these recommendations in your practice will require a careful analysis of the particularities of each case. Our lawyers can help you understand and address any questions you may have. For more information, please get in touch with one of our experts.

Benjamin Docquir
Partner
T +32 2 515 93 36
benjamin.docquir@osborneclarke.com

Vinciane Rysselinck
Senior Counsel
T +32 2 515 93 08
vinciane.rysselinck@osborneclarke.com

Thierry Viérin
Partner
T +32 2 515 93 04
thierry.vierin@osborneclarke.com

Ann-Sophie De Graeve
Counsel
T +32 2 515 93 30
annsophie.degraeve@osborneclarke.com