ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 249

Opinion 2/2017 on data processing at work

Adopted on 8 June 2017

Contents

1 Executive summary

This Opinion complements the previous Article 29 Working Party ("WP29") publications *Opinion 8/2001 on the processing of personal data in the employment context* (WP48)[1], and the 2002 *Working Document on the surveillance of electronic communications in the workplace* (WP55)[2]. Since the publication of these documents, a number of new technologies have been adopted that enable more systematic processing of employees' personal data at work, creating significant challenges to privacy and data protection.

This Opinion makes a new assessment of the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies and undertaking a proportionality assessment of a number of scenarios in which they could be deployed.

Whilst primarily concerned with the Data Protection Directive, the Opinion looks toward the additional obligations placed on employers by the General Data Protection Regulation. It also restates the position and conclusions of Opinion 8/2001 and the WP55 Working Document, namely that when processing employees' personal data:

- employers should always bear in mind the fundamental data protection principles, irrespective of the technology used;
- the contents of electronic communications made from business premises enjoy the same fundamental rights protections as analogue communications;
- consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence;
- performance of a contract and legitimate interests can sometimes be invoked, provided the processing is strictly necessary for a legitimate purpose and complies with the principles of proportionality and subsidiarity;
- employees should receive effective information about the monitoring that takes place; and
- any international transfer of employee data should take place only where an adequate level of protection is ensured.

2. Introduction

The rapid adoption of new information technologies in the workplace, in terms of infrastructure, applications and smart devices, allows for new types of systematic and potentially invasive data processing at work. For example:

- technologies enabling data processing at work can now be implemented at a fraction of the costs of several years ago whilst the capacity for the processing of personal data by these technologies has increased exponentially;

[1] WP29, *Opinion 08/2001 on the processing of personal data in the employment context*, WP 48, 13 September 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] WP29, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29 May 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- new forms of processing, such as those concerning personal data on the use of online services and/or location data from a smart device, are much less visible to employees than other more traditional types such as overt CCTV cameras. This raises questions about the extent to which employees are aware of these technologies, since employers might unlawfully implement these processing without prior notice to the employees; and
- the boundaries between home and work have become increasingly blurred. For example, when employees work remotely (e.g. from home), or whilst they are travelling for business, monitoring of activities outside of the physical working environment can take place and can potentially include monitoring of the individual in a private context.

Therefore, whilst the use of such technologies can be helpful in detecting or preventing the loss of intellectual and material company property, improving the productivity of employees and protecting the personal data for which the data controller is responsible, they also create significant privacy and data protection challenges. As a result, a new assessment is required concerning the balance between the legitimate interest of the employer to protect its business and the reasonable expectation of privacy of the data subjects: the employees.

Whilst this Opinion will focus on new information technologies by assessing nine different scenarios in which they can feature, it will also briefly reflect on more traditional methods of data processing at work where the risks are amplified as a result of technological change.

Where the word "employee" is used in this Opinion, WP29 does not intend to restrict the scope of this term merely to persons with an employment contract recognized as such under applicable labour laws. Over the past decades, new business models served by different types of labour relationships, and in particular employment on a freelance basis, have become more commonplace. This Opinion is intended to cover all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract.

It is important to state that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent—such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees.

Regardless of the legal basis for such processing, a proportionality test should be undertaken prior to its commencement to consider whether the processing is necessary to achieve a legitimate purpose, as well as the measures that have to be taken to ensure that infringements of 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).

3. The legal framework

Whilst the analysis below is primarily conducted in relation to the current legal framework under Directive 95/46/EC (the Data Protection Directive or "DPD")[3], this Opinion will also

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281, 23/11/1995, p.31-50*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

look toward the obligations under Regulation 2016/679 (the General Data Protection Regulation or "GDPR")[4], which has already entered into force and which will become applicable on 25 May 2018.

With regard to the proposed ePrivacy Regulation[5], the Working Party calls on European legislators to create a specific exception for interference with devices issued to employees[6]. The Proposed Regulation does not contain a suitable exception to the general interference prohibition, and employers cannot usually provide valid consent for the processing of personal data of their employees.

3.1 Directive 95/46/EC—Data Protection Directive ("DPD")

In Opinion 08/2001, WP29 previously outlined that employers take into account the fundamental data protection principles of the DPD when processing personal data in the employment context. The development of new technologies and new methods of processing in this context have not altered this situation—in fact, it can be said that such developments have made it *more* important for employers to do so. In this context, employers should:

- ensure that data is processed for specified and 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;
- be transparent with employees about the use and purposes of monitoring technologies;
- enable the exercise of data subject rights, including the rights of access and, as appropriate, the rectification, erasure or blocking of personal data;
- keep the data accurate, and not retain them any longer than necessary; and
- take all necessary measures to protect the data against unauthorised access and ensure that staff are sufficiently aware of data protection obligations.

Without repeating the earlier advice given, WP29 wishes to highlight three principles, namely: legal grounds, transparency, and automated decisions.

3.1.1 *LEGAL GROUNDS (ARTICLE 7)*

When processing personal data in the employment context, at least one of the criteria set out in Art. 7 has to be satisfied. If the types of personal data processed involve the special categories (as elaborated in Art. 8), the processing is prohibited unless an exception applies[7,8].

---

[4] Regulation 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), *OJ L 119, 4.5.2016, p. 1-88*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[5] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] See WP29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation*, WP 247, 04 April 2017, page 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

[7] As stated in part 8 of Opinion 08/2001; for example, Art. 8(2)(b) provides an exception for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards.

Even if the employer can rely on one of those exceptions, a legal ground from Art. 7 is still required for the processing to be legitimate.

In summary, employers must therefore take note of the following:

- for the majority of such data processing at work**, the legal basis cannot and should not be the consent of the employees** (Art 7(a)) due to the nature of the relationship between employer and employee;
- processing may be necessary for **the performance of a contract** (Art 7(b)) in cases where the employer has to process personal data of the employee to meet any such obligations;
- it is quite common that **employment law may impose legal obligations** (Art. 7(c)) **that necessitate the processing of personal data**; in such cases the employee must be clearly and fully informed of such processing (unless an exception applies);
- should an employer seek to rely on **legitimate interest** (Art. 7(f)) the purpose of the processing must be legitimate; the chosen method or specific technology must be necessary, proportionate and implemented in the least intrusive manner possible along with the ability to enable the employer to demonstrate that **appropriate measures have been put in place** to ensure a balance with the fundamental rights and freedoms of employees[9];
- the processing operations must also comply with the **transparency requirements** (Art. 10 and 11), and employees should be clearly and fully informed of the processing of their personal data[10], including the existence of any monitoring; and
- **appropriate technical and organisational measures** should be adopted to ensure security of the processing (Art. 17).

The most relevant criteria under Art. 7 are detailed below.

- **Consent (Article 7(a))**

Consent, according to the DPD, is defined as any freely-given, specific and informed indication of a data subject's wishes by which the he or she signifies his or her agreement to personal data relating to them being processed. For consent to be valid, it must also be revocable.

WP29 has previously outlined in Opinion 8/2001 that where an employer has to process personal data of his/her employees it is misleading to start with the supposition that the processing can be legitimised through the employees' consent. In cases where an employer says they require consent and there is a real or potential relevant prejudice that arises from the employee not consenting (which can be highly probable in the employment context, especially when it concerns the employer tracking the behaviour of the employee over time), then the consent is not valid since it is not and cannot be freely given. Thus, for the majority

[8] It should be noted that in some countries, there are special measures in place that employers must abide by to protect employees' private lives. Portugal is one example of countries where such special measures exist and similar measures may apply in some other Member States too. The conclusions in section 5.6 as well as the examples presented in sections 5.1 and 5.7.1 of this Opinion are therefore not valid in Portugal for these reasons.
[9] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted 9 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[10] Pursuant to Art. 11(2) of the DPD, the controller is exempted from the obligation to provide information to the data subject in cases where the recording or collection of data is expressly laid down by law.

of the cases of employees' data processing, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required.

Moreover, even in cases where consent could be said to constitute a valid legal basis of such a processing (i.e. if it can be undoubtedly concluded that the consent is freely given), it needs to be a specific and informed indication of the employee's wishes. Default settings on devices and/or the installation of software that facilitate the electronic personal data processing cannot qualify as consent given from employees, since consent requires an active expression of will. A lack of action (i.e, not changing the default settings) may generally not be considered as a specific consent to allow such processing[11].

- **Performance of a contract (Article 7(b))**

Employment relationships are often based on a contract of employment between the employer and the employee. When meeting obligations under this contract, such as paying the employee, the employer is required to process some personal data.

- **Legal obligations (Article 7(c))**

It is quite common that employment law imposes legal obligations on the employer, which necessitate the processing of personal data (e.g. for the purpose of tax calculation and salary administration). Clearly, in such cases, such a law constitutes the legal basis for the data processing..

- **Legitimate interest (Article 7(f))**

If an employer wishes to rely upon the legal ground of Art. 7(f) of the DPD, the purpose of the processing must be legitimate, and the chosen method or specific technology with which the processing is to be undertaken must be necessary for the legitimate interest of the employer. The processing must also be proportionate to the business needs, i.e. the purpose, it is meant to address. Data processing at work should be carried out in the least intrusive manner possible and be targeted to the specific area of risk. Additionally, if relying on Art. 7(f), the employee retains the right to object to the processing on compelling legitimate grounds under Art. 14.

In order to rely on Art. 7(f) as the legal ground for processing it is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees.[12] Such measures, depending on the form of monitoring, should include limitations on monitoring so as to guarantee that the employee's privacy is not violated. Such limitations could be:

---

[11] See also WP29, *Opinion 15/2011 on the definition of consent*, WP187, 13 July 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, page 24.

[12] For an example of the balance that needs to be struck, see the case of *Köpke v Germany*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), in which an employee was dismissed as a result of a covert video surveillance operation undertaken by the employer and a private detective agency. Whilst in this instance the Court concluded that the domestic authorities had struck a fair balance between the employer's legitimate interest (in the protection of its property rights), the employee's right to respect for private life, and the public interest in the administration of justice, it also observed that the various interests concerned could be given a different weight in future as a result of technological development.

- geographical (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places and for example sanitary zones and break rooms should be prohibited),
- data-oriented (e.g. personal electronic files and communication should not be monitored), and
- time-related (e.g. sampling instead of continuous monitoring).

3.1.2 *TRANSPARENCY (ARTICLES 10 AND 11)*

The transparency requirements of Articles 10 and 11 apply to data processing at work; employees must be informed of the existence of any monitoring, the purposes for which personal data are to be processed and any other information necessary to guarantee fair processing.

With new technologies, the need for transparency becomes more evident since they enable the collection and further processing of possibly huge amounts of personal data in a covert way.

3.1.3 *AUTOMATED DECISIONS (ARTICLE 15)*

Art. 15 of the DPD also grants data subjects the right not to be subject to a decision based solely on automated processing, where that decision produces legal effects or similarly significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects, such as performance at work, unless the decision is necessary for entering into or performance of a contract, authorised by Union or Member State law, or is based on the explicit consent of the data subject.

3.2 Regulation 2016/679—General Data Protection Regulation ("GDPR")

The GDPR includes and enhances the requirements in the DPD. It also introduces new obligations for all data controllers, including employers.

3.2.1 *DATA PROTECTION BY DESIGN*

Art. 25 of the GDPR requires data controllers to implement data protection by design and by default. As an example: where an employer issues devices to employees, the most privacy-friendly solutions should be selected if tracking technologies are involved. Data minimisation must also be taken into account.

3.2.2 *DATA PROTECTION IMPACT ASSESSMENTS*

Art. 35 of the GDPR outlines the requirements for a data controller to carry out a Data Protection Impact Assessment (DPIA) where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing itself, is likely to result in a high risk to the rights and freedoms of natural persons. An example is a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing including profiling, and on which decisions are taken that produce legal effects concerning the natural person or similarly significantly affect the natural person.

Where the DPIA indicates that the identified risks cannot be sufficiently addressed by the controller—i.e., that the residual risks remain high—then the controller must consult the supervisory authority prior to the commencement of the processing (Art. 36(1)) as clarified in the WP29 guidelines on DPIAs[13].

3.2.2 "*PROCESSING IN THE CONTEXT OF EMPLOYMENT*"

Art. 88 of the GDPR states that Member States may, by law or collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context. In particular, these rules may be provided for the purposes of:

- recruitment;
- performance of the employment contract (including discharge of obligations laid down by law or collective agreements);
- management, planning and organisation of work;
- equality and diversity in the workplace;
- health and safety at work;
- protection of an employer's or customer's property;
- exercise and enjoyment (on an individual basis) of rights and benefits related to employment; and
- termination of the employment relationship.

In accordance with Art. 88(2), any such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to:

- the transparency of processing;
- the transfer of personal data within a group of undertakings or group of enterprises engaged in a joint economic activity; and
- monitoring systems at the workplace.

In this Opinion, the Working Party has provided guidelines for the legitimate use of new technology in a number of specific situations, detailing suitable and specific measures to safeguard the human dignity, legitimate interest and fundamental rights of employees.

4. Risks

Modern technologies enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables. If there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring.

Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organise, set up workers' meetings, and to communicate confidentially

[13] WP29, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is likely to result in "high risk" for the purposes of Regulation 2016/679*, WP 248, 04 April 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, page 18.

(including the right to seek information). Monitoring communications and behaviour will put pressure on employees to conform in order to prevent the detection of what might be perceived as anomalies, in a comparable way to the way in which the intensive use of CCTV has influenced citizens' behaviour in public spaces. Moreover, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.

Monitoring IT usage also differs from other, more visible observation and monitoring tools like CCTV in that it can take place in a covert way. In the absence of an easily understandable and readily accessible workplace monitoring policy, employees may not be aware of the existence and consequences of the monitoring that is taking place, and are therefore unable to exercise their rights. A further risk comes from the "over-collection" of data in such systems, e.g. those collecting WiFi location data.

The increase in the amount of data generated in the workplace environment, in combination with new techniques for data analysis and cross-matching, may also create risks of incompatible further processing. Examples of illegitimate further processing include using systems that are legitimately installed to protect properties to then monitor the availability, performance and customer-friendliness of employees. Others include using data collected via a CCTV system to regularly monitor the behaviour and performance of employees, or using data of a geolocation system (such as for example WiFi- or Bluetooth tracking) to constantly check an employee's movements and behaviour.

As a result, such tracking may infringe upon the privacy rights of employees, regardless of whether the monitoring takes place systematically or occasionally. The risk is not limited to the analysis of the content of communications. Thus, the analysis of metadata about a person might allow for an equally privacy-invasive detailed monitoring of an individual's life and behavioural patterns.

The extensive use of monitoring technologies may also limit employees' willingness to (and channels by which they could) inform employers about irregularities or illegal actions of superiors and/or other employees threatening to damage the business (especially client data) or workplace. Anonymity is often necessary for a concerned employee to take action and report such situations. Monitoring that infringes upon the privacy rights of employees may hamper necessary communications to the appropriate officers. In such an instance, the established means for internal whistle-blowers may become ineffective[14].

5. Scenarios

This section addresses a number of data processing at work scenarios in which new technologies and/or developments of existing technologies have, or may have, the potential to result in high risks to the privacy of employees. In all such cases employers should consider whether:

[14] See for example WP29, *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*, WP 117, 1 February 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

- the processing activity is necessary, and if so, the legal grounds that apply;
- the proposed processing of personal data is fair to the employees;
- the processing activity is proportionate to the concerns raised; and
- the processing activity is transparent.

5.1 Processing operations during the recruitment process

Use of social media by individuals is widespread and it is relatively common for user profiles to be publicly viewable depending on the settings chosen by the account holder. As a result, employers may believe that inspecting the social profiles of prospective candidates can be justified during their recruitment processes. This may also be the case for other publicly-available information about the potential employee.

However, employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process those data for their own purposes. A legal ground is required for this processing, such as legitimate interest. In this context the employer should—prior to the inspection of a social media profile—take into account whether the social media profile of the applicant is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection. In addition, employers are only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for.

Data 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 individual concerned[15]. The individual must also be correctly informed of any such processing before they engage with the recruitment process.

There is no legal ground for an employer to require potential employees to "friend" the potential employer, or in other ways provide access to the contents of their profiles.

Example

During the recruitment of new staff, an employer checks the profiles of the candidates on various social networks and includes information from these networks (and any other information available on the internet) in the screening process.

Only if it is necessary for the job to review information about a candidate on social media, for example in order to be able to assess specific risks regarding candidates for a specific function, and the candidates are correctly informed (for example, in the text of the job advert) the employer may have a legal basis under Article 7(f) to review publicly-available information about candidates.

[15] See also Council of Europe, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment*, paragraph 13.2 (1 April 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). In cases where the employer wishes to retain the data with a view to a further job opportunity, the data subject should be informed accordingly and be given the possibility to object to such further processing, in which case it should be deleted (Id.).

5.2 Processing operations resulting from in-employment screening

Through the existence of profiles on social media, and the development of new analytical technologies, employers have (or can obtain) the technical capability of permanently screening employees by collecting information regarding their friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviours therefore capturing data, including sensitive data, relating to the employee's private and family life.

In-employment screening of employees' social media profiles should not take place on a generalised basis.

Moreover, employers should refrain from requiring an employee or a job applicant access to information that he or she shares with others through social networking.

Example
An employer monitors the LinkedIn profiles of former employees that are involved during the duration of non-compete clauses. The purpose of this monitoring is to monitor compliance with such clauses. The monitoring is limited to these former employees.

As long as the employer can prove that such monitoring is necessary to protect his legitimate interests, that there are no other, less invasive means available, and that the former employees have been adequately informed about the extent of the regular observation of their public communications, the employer may be able to rely on the legal basis of Article 7(f) of the DPD.

Additionally, employees should not be required to utilise a social media profile that is provided by their employer. Even when this is specifically foreseen in light of their tasks (e.g. spokesperson for an organisation), they must retain the option of a "non-work" non-public profile that they can use instead of the "official" employer-related profile, and this should be specified in the terms and conditions of the employment contract.

5.3 Processing operations resulting from monitoring ICT usage at the workplace

Traditionally, the monitoring of electronic communications in the workplace (eg, phone, internet browsing, email, instant messaging, VOIP, etc.) was considered the main threat to employees' privacy. In its 2001 *Working Document on the surveillance of electronic communications in the workplace*, WP29 made a number of conclusions in relation to the monitoring of email and internet usage. While those conclusions remain valid, there is a need to take into account technological developments that have enabled newer, potentially more intrusive and pervasive ways of monitoring. Such developments include, amongst others:

- Data Loss Prevention (DLP) tools, which monitor outgoing communications for the purpose of detecting potential data breaches;
- Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) systems, which can provide a variety of monitoring technologies including deep packet inspection, TLS interception, website filtering, content filtering, on-appliance reporting, user identity information and (as described above) data loss prevention. Such technologies may also be deployed individually, depending on the employer;

- security applications and measures that involve logging employee access to the employer's systems;
- eDiscovery technology, which refers to any process in which electronic data is searched with the aim of its use as evidence;
- tracking of application and device usage via unseen software, either on the desktop or in the cloud;
- the use in the workplace of office applications provided as a cloud service, which in theory allow for very detailed logging of the activities of employees;
- monitoring of personal devices (e.g., PCs, mobile phones, tablets), that employees supply for their work in accordance with a specific use policy, such as Bring-Your-Own-Device (BYOD), as well as Mobile Device Management (MDM) technology which enables the distribution of applications, data and configuration settings, and patches for mobile devices; and
- the use of wearable devices (e.g., health and fitness devices).

It is possible that an employer will implement an "all-in-one" monitoring solution, such as a suite of security packages which enable them to monitor all ICT usage in the workplace as opposed to just email and/or website monitoring as was once the case. The conclusions adopted in WP55 would apply for any system that enables such monitoring to take place.[16]

Example

An employer intends to deploy a TLS inspection appliance to decrypt and inspect secure traffic, with the purpose of detecting anything malicious. The appliance is also able to record and analyse the entirety of an employee's online activity on the organisation's network.

Use of encrypted communications protocols is increasingly being implemented to protect online data flows involving personal data against interception. However, this can also present issues, as the encryption makes it impossible to monitor incoming and outgoing data. TLS inspection equipment decrypts the data stream, analyses the content for security purposes and then re-encrypts the stream afterwards.

In this example, the employer relies upon legitimate interests—the necessity to protect the network, and the personal data of employees and customers held within that network, against unauthorised access or data leakage. However, monitoring every online activity of the employees is a disproportionate response and an interference with the right to secrecy of communications. The employer should first investigate other, less invasive, means to protect the confidentiality of customer data and the security of the network.

To the extent that some interception of TLS traffic can be qualified as strictly necessary, the appliance should be configured in a way to prevent permanent logging of employee activity, for example by blocking suspicious incoming or outgoing traffic and redirecting the user to an information portal where he or she may ask for review of such an automated decision. If some general logging would nonetheless be deemed strictly necessary, the appliance may

[16] See also *Copland v United Kingdom*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), in which the Court stated that emails sent from business premises and information derived from the monitoring of internet use could be a part of an employee's private life and correspondence, and that the collection and storage of that information without the knowledge of the employee would amount to an interference with the employee's rights, although the Court did not rule that such monitoring would never be necessary in a democratic society.

also be configured not to store log data unless the appliance signals the occurrence of an incident, with a minimization of the information collected.

As a good practice, the employer could offer alternative unmonitored access for employees. This could be done by offering free WiFi, or stand-alone devices or terminals (with appropriate safeguards to ensure confidentiality of the communications) where employees can exercise their legitimate right to use work facilities for some private usage[17]. Moreover, employers should consider certain types of traffic whose interception endangers the proper balance between their legitimate interests and employee's privacy—such as the use of private webmail, visits to online banking and health websites—with the aim to appropriately configure the appliance so as not to proceed with interception of communications in circumstances that are not compliant with proportionality. Information on the type of communications that the appliance is monitoring should be specified to the employees.

A policy concerning the purposes for when, and by whom, suspicious log data can be accessed should be developed and made easily and permanently accessible for all employees, in order to also guide them about acceptable and unacceptable use of the network and facilities. This allows employees to adapt their behaviour to prevent being monitored when they legitimately use IT work facilities for private use. As good practice, such a policy should be evaluated, at least annually, to assess whether the chosen monitoring solution delivers the intended results, and whether there are other, less invasive tools or means available to achieve the same purposes.

Irrespective of the technology concerned or the capabilities it possesses, the legal basis of Article 7(f) is only available if the processing meets certain conditions. Firstly, employers utilising these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology. Secondly, employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organisation's network and equipment, and strictly detailing the processing taking place.

In some countries the creation of such a policy would legally require approval of a Workers' Council or similar representation of employees. In practice, such policies are often drafted by IT maintenance staff. Since their main focus will mostly be on security, and not on the legitimate expectation of privacy of employees, WP29 recommends that in all cases a representative sample of employees is involved in assessing the necessity of the monitoring, as well as the logic and accessibility of the policy.

[17] See *Halford v. United Kingdom*, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), in which the Court stated that "telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 paragraph 1 [of the Convention]"; and *Barbulescu v. Romania*, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), concerning the use of a professional instant messenger account for personal correspondence, in which the Court stated that monitoring of the account by the employer was limited and proportionate; the dissenting opinion of Judge Pinto de Alberquerque which argued for a careful balance to be struck.

Example

An employer deploys a Data Loss Prevention tool to monitor the outgoing e-mails automatically, for the purpose of preventing unauthorised transmission of proprietary data (e.g. customer's personal data), independently from whether such an action is unintentional or not. Once an e-mail is being considered as the potential source of a data breach, further investigation is performed.

Again, the employer relies upon the necessity for his legitimate interest to protect the personal data of customers as well as his assets against unauthorised access or data leakage. However, such a DLP tool may involve unnecessary processing of personal data —for example, a "false positive" alert might result in unauthorized access of legitimate e-mails that have been sent by employees (which may be, for instance, personal e-mails).

Therefore, the necessity of the DLP tool and its deployment should be fully justified so as to strike the proper balance between his legitimate interests and the fundamental right to the protection of employees' personal data. In order for the legitimate interests of the employer to be relied upon, certain measures should be taken to mitigate the risks. For example, the rules that the system follows to characterize an e-mail as potential data breach should be fully transparent to the users, and in cases that the tool recognises an e-mail that is to be sent as a possible data breach, a warning message should inform the sender of the e-mail prior to the e-mail transmission, so as to give the sender the option to cancel this transmission.

In some cases, the monitoring of employees is possible not so much because of the deployment of specific technologies, but simply because employees are expected to use online applications made available by the employer which process personal data. The use of cloud-based office applications (e.g. document editors, calendars, social networking) is an example of this. It should be ensured that employees can 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. If the employee sets an appointment to "Private" or notes this in appointment itself, employers (and other employees) should not be allowed to review the contents of the appointment.

The requirement of subsidiarity in this context sometimes means that no monitoring may take place at all. For example, this is the case where the prohibited use of communications services can be prevented by blocking certain websites. If it is possible to block websites, instead of continuously monitoring all communications, blocking should be chosen in order to comply with this requirement of subsidiarity.

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

5.4 Processing operations resulting from monitoring ICT usage outside the workplace

ICT usage outside the workplace has become more common with the growth of homeworking, remote working and "bring your own device" policies. The capabilities of such technologies can pose a risk to the private life of employees, as in many cases the monitoring systems existing in the workplace are effectively extended into the employees' domestic sphere when they use such equipment. .

5.4.1 *MONITORING OF HOME AND REMOTE WORKING*

It has become more common for employers to offer employees the option to work remotely, e.g., from home and/or whilst in transit. Indeed, this is a central factor behind the reduced distinction between the workplace and the home. In general this involves the employer issuing ICT equipment or software to the employees which, once installed in their home/on their own devices, enables them to have the same level of access to the employer's network, systems and resources that they would have if they were in the workplace, depending on the implementation.

Whilst remote working can be a positive development, it also presents an area of additional risk for an employer. For example, employees that have remote access to the employer's infrastructure are not bound by the physical security measures that may be in place at the employer's premises. To put it plainly: without the implementation of appropriate technical measures the risk of unauthorised access increases and may result in the loss or destruction of information, including personal data of employees or customers, which the employer may hold.

In order to mitigate this area of risk employers may think there is a justification for deploying software packages (either on-premise or in the cloud) that have the capabilities of, for example, logging keystrokes and mouse movements, screen capturing (either randomly or at set intervals), logging of applications used (and how long they were used for), and, upon compatible devices, enabling webcams and collecting the footage thereof. Such technologies are widely available including from third parties such as cloud providers.

However, the processing involved in such technologies are disproportionate and the employer is very unlikely to have a legal ground under legitimate interest, e.g. for recording an employee's keystrokes and mouse movements.

The key is addressing the risk posed by home and remote working in a proportionate, non-excessive manner, in whatever way the option is offered and by whatever technology is proposed, particularly if the boundaries between business and private use are fluid.

5.4.2 *BRING YOUR OWN DEVICE (BYOD)*

Due to the rise in popularity, features and capability of consumer electronic devices, employers may face demands from employees to use their own devices in the workplace to carry out their jobs. This is known as "bring your own device" or BYOD.

Implementing BYOD effectively can lead to a number of benefits for employees, including improved employee job satisfaction, overall morale increase, increased job efficiency and increased flexibility. However, by definition, some use of an employee's device will be personal in nature, and this is more likely to be the case at certain times of the day (e.g., evenings and weekends). It is therefore a distinct possibility that employees' use of their own devices will lead to employers processing non-corporate information about those employees, and possibly any family members who also use the devices in question.

In the employment context, BYOD privacy risks are commonly associated with monitoring technologies that collect identifiers such as MAC addresses, or in instances where an employer accesses an employee's device under the justification of performing a security scan, i.e. for malware. In respect of the latter, a number of commercial solutions exist that allow for

the scanning of private devices, however their usage could potentially access all data on that device and therefore they must be carefully managed. For example, those sections of a device which are presumed to be only used for private purposes (e.g. the folder storing photos taken with the device) may in principle not be accessed.

Monitoring the location and traffic of such devices may be considered to serve a legitimate interest to protect the personal data that the employer is responsible for as the data controller; however this may be unlawful where an employee's personal device is concerned, if such monitoring also captures data relating to the employee's private and family life. In order to prevent monitoring of private information appropriate measures must be in place to distinguish between private and business use of the device.

Employers should also implement methods by which their own data on the device is securely transferred between that device and their network. It may be the case that the device is therefore configured to route all traffic through a VPN back into the corporate network, so as to offer a certain level of security; however, if such a measure is used, the employer should also consider that software installed for the purposes of monitoring pose a privacy risk during periods of personal usage by the employee. Devices that offer additional protections such as "sandboxing" data (keeping data contained within a specific app) could be used.

Conversely, the employer must also consider the prohibition of the use of specific work devices for private use if there is no way to prevent private use being monitored—for example if the device offers remote access to personal data for which the employer is the data controller.

5.4.3 *MOBILE DEVICE MANAGEMENT (MDM)*

Mobile device management enables employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand. An employer may operate this functionality himself, or use a third party to do so. MDM services also enable employers to record or track the device in real-time even if it is not reported stolen.

A DPIA should be performed prior to the deployment of any such technology where it is new, or new to the data controller. If the outcome of the DPIA is that the MDM technology is necessary in specific circumstances, an assessment should still be made as to whether the resulting data processing complies with the principles of proportionality and subsidiarity. Employers must ensure that the data collected as part of this remote location capability is processed for a specified purpose and does not, and could not, form part of a wider programme enabling ongoing monitoring of employees. Even for specified purposes, the tracking features should be mitigated. Tracking systems can be designed to register the location data without presenting it to the employer—in such circumstances, the location data should become available only in circumstances where the device would be reported or lost.

Employees whose devices are enrolled in MDM services must also be fully informed as to what tracking is taking place, and what consequences this has for them.

5.4.4 *WEARABLE DEVICES*

Employers are increasingly tempted to provide wearable devices to their employees in order to track and monitor their health and activity within and sometimes even outside of the

workplace. However, this data processing involves the processing of health data, and is therefore prohibited based on Article 8 of the DPD.

Given the unequal relationship between employers and employees—i.e., the employee has a financial dependence on the employer—and the sensitive nature of the health data, it is highly unlikely that legally valid explicit consent can be given for the tracking or monitoring of such data as employees are essentially not 'free' to give such consent in the first place. Even if the employer uses a third party to collect the health data, which would only provide aggregated information about general health developments to the employer, the processing would still be unlawful.

Also, as described in *Opinion 5/2014 on Anonymisation Techniques*[18], it is technically very difficult to ensure complete anonymisation of the data. Even in an environment with over a thousand employees, given the availability of other data about the employees the employer would still be able to single out individual employees with particular health indications such as high blood pressure or obesity.

Example:

An organisation offers fitness monitoring devices to its employees as a general gift. The devices count the number of steps employees take, and register their heartbeats and sleeping patterns over time.

The resulting health data should only be accessible to the employee and not the employer. Any data transferred between the employee (as data subject) and the device/service provider (as data controller) is a matter for those parties.

As the health data could also be processed by the commercial party that has manufactured the devices or offers a service to employers, 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 not result in unlawful processing of health data on employees.

5.5 Processing operations relating to time and attendance

Systems that enable employers to control who can enter their premises, and/or certain areas within their premises, can also allow the tracking of employees' activities. Although such systems have existed for a number of years, new technologies intended to track employees' time and attendance are being more widely deployed, including those that process of biometric data as well as others such as mobile device tracking.

Whilst such systems can form an important component of an employer's audit trail, they also pose the risk of providing an invasive level of knowledge and control regarding the activities of the employee whilst in the workplace.

Example:

An employer maintains a server room in which business-sensitive data, personal data relating to employees and personal data relating to customers is stored in digital form. In order to

[18] WP29, *Opinion 5/2014 on anonymization techniques*, WP 216, 10 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

comply with legal obligations to secure the data against unauthorised access, the employer has installed an access control system that records the entrance and exit of employees who have appropriate permission to enter the room. Should any item of equipment go missing, or if any data is subject to unauthorised access, loss or theft, the records maintained by the employer allow them to determine who had access to the room at that time.

Given that the processing is necessary and does not outweigh the right to private life of the employees, it can be in the legitimate interest under Art. 7(f), if the employees have been adequately informed about the processing operation. However, the continuous monitoring of the frequency and exact entrance and exit times of the employees cannot be justified if these data are also used for another purpose, such as employee performance evaluation.

5.6 Processing operations using video monitoring systems

Video monitoring and surveillance continues to present similar issues for employee privacy as before: the capability to continuously capture the behaviour of the worker.[19] The most relevant changes relating to the application of this technology in the employment context are the capability to access the collected data remotely (e.g. via a smartphone) easily; the reduction in the cameras' sizes (along with an increase in their capabilities, e.g. high-definition); and the processing that can be performed by new video analytics.

With the capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by automated means, to identify deviations from predefined movement patterns (e.g. factory context), and more. This would be disproportionate to the rights and freedoms of employees, and therefore, generally unlawful. The processing is also likely to involve profiling, and possibly, automated decision-making. Therefore, employers should refrain from the use of facial recognition technologies. There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of such technology[20].

5.7 Processing operations involving vehicles used by employees

Technologies that enable employers to monitor their vehicles have become widely adopted, particularly among organisations whose activities involve transport or have significant vehicle fleets.

Any employer using vehicle telematics will be collecting data about both the vehicle and the individual employee using that vehicle. This data can include not just the location of the vehicle (and, hence, the employee) collected by basic GPS tracking systems, but, depending on the technology, a wealth of other information including driving behaviour. Certain technologies can also enable continuous monitoring both of the vehicle and the driver (eg, event data recorders).

An employer might be obliged to install tracking technology in vehicles to demonstrate compliance with other legal obligations, e.g. to ensure the safety of employees who drive those vehicles. The employer may also have a legitimate interest in being able to locate the

[19] See the above referenced case of *Köpke v Germany*; additionally, it should also be noted that in some jurisdictions the installation of systems such as CCTV for the purpose of proving unlawful conduct has been ruled permissible; see the case of *Bershka* in the Constitutional Court of Spain.

[20] Moreover, under the GDPR, processing of biometric data for identification purposes must be based on an exception provided by Art. 9(2).

vehicles at any time. Even if employers would have a legitimate interest to achieve these purposes, 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. Where private use of a professional vehicle is allowed, the most important measure an employer can take to ensure compliance with these principles is the offering of an opt-out: the employee in principle should have the option to temporarily turn off location tracking when special circumstances justify this turning off, such as a visit to a doctor. This way, the employee can on its own initiative protect certain location data as private. The employer must ensure that the collected data are not used for illegitimate further processing, such as the tracking and evaluation of employees.

The employer must also clearly inform the employees that a tracking device has been installed in a company vehicle that they are driving, and that their movements are being recorded whilst they are using that vehicle (and that, depending on the technology involved, their driving behaviour may also be recorded). Preferably such information should be displayed prominently in every car, within eyesight of the driver.

It is possible that employees may use company vehicles outside working hours, e.g. for personal use, depending on the specific policies governing the use of those vehicles. Given the sensitivity of location data, it is unlikely that there is a legal basis for monitoring the locations of employees' vehicles outside agreed working hours. However, should such a necessity exist, an implementation that would be proportionate to the risks should be considered. For example, this could mean that, in order to prevent car theft, the location of the car is not registered outside working hours, unless the vehicle leaves a widely defined circle (region or even country). In addition, the location would only be shown in a "break-the-glass" way—the employer would only activate the "visibility" of the location, accessing the data already stored by the system, when the vehicle leaves a predefined region..

As stated in the WP29 *Opinion 13/2011 on Geolocation services on smart mobile devices*[21]:

> "Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle."

Further, as stated in the WP29 *Opinion 5/2005 on the use of location data with a view to providing value-added services*[22]:

> "Processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge. Conversely, the Working Party considers data processing to be excessive where employees

[21] WP29, *Opinion 13/2011 on Geolocation services on smart mobile devices*, WP 185, 16 May 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[22] WP29, *Opinion 5/2005 on the use of location data with a view to providing value-added services*, WP 115, 25 November 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work where this can be monitored by other means."

5.7.1 EVENT DATA RECORDERS

Event data recorders provide an employer with the technical capability of processing a significant amount of personal data about the employees that drive company vehicles. Such devices are increasingly being placed into vehicles with the goal to record video, possibly including sound, in case of an accident. These systems are able to record at certain times, e.g. in response to sudden braking, abrupt directional change or accidents, where the moments immediately preceding the incident are stored, but they can also be set to monitor continuously. This information can be used subsequently to observe and review an individual's driving behaviour with the aim of improving it. Moreover, many of these systems include GPS to track the location of the vehicle in real-time and other details corresponding to the driving (such as the vehicle speed) can be also stored for further processing.

These devices have become particularly prevalent among organisations whose activities involve transport or have significant vehicle fleets. However, the deployment 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, and the processing complies with the principles of proportionality and subsidiarity.

Example

A transport company equips all of its vehicles with a video camera inside the cabin which records sound and video. The purpose of processing these data is to improve the driving skills of the employees. The cameras are configured to retain recordings whenever incidents such as sudden braking or abrupt directional change take place. The company assumes it has a legal ground for the processing in its legitimate interest under Article 7(f) of the Directive, to protect the safety of its employees and other drivers' safety.

However, the legitimate interest of the company to monitor the drivers does not prevail over the rights of those drivers to the protection of their personal data. The continuous monitoring of employees with such cameras constitutes a serious interference with their right of privacy. There are other methods (e.g., the installation of equipment that prevents the use of mobile phones) as well as other safety systems like an advanced emergency braking system or a lane departure warning system that can be used for the prevention of vehicle accidents which may be more appropriate. Furthermore, such a video has a high probability of resulting in the processing of personal data of third parties (such as pedestrians) and, for such a processing, the legitimate interest of the company is not sufficient to justify the processing.

5.8 Processing operations involving disclosure of employee data to third parties

It has become increasingly common for companies to transmit their employees' data to their customers for the purpose of ensuring reliable service provision. These data may be quite excessive depending on the scope of services provided (e.g. an employee's photo may be included). However, employees are not in a position, given the imbalance of power, to give free consent to the processing of their personal data by their employer, and if the data processing is not proportional, the employer does not have a legal ground.

Example:

A delivery company sends its customers an e-mail with a link to the name and the location of the deliverer (employee). The company also intended to provide a passport photo of the deliverer. The company assumed it would have a legal ground for the processing in its legitimate interest (Article 7(f) of the Directive), allowing the customer to check if the deliverer is indeed the right person.

However, it is not necessary to provide the name and the photo of the deliverer to the customers. Since there is no other legitimate ground for this processing, the delivery company is not allowed to provide these personal data to customers.

5.9 Processing operations involving international transfers of HR and other employee 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 use of most of these applications will result in the international transfer of data from and concerning employees. As previously outlined in Opinion 08/2001, Art. 25 of the Directive states that transfers of personal data to a third country outside the EU can take place only where that country ensures an adequate level of protection. Whatever the basis, the transfer should satisfy the provisions of the Directive.

It should thus be ensured that these provisions concerning the international transfer of data are complied with. WP29 re-states its previous position that it is preferable to rely on adequate protection rather than the derogations listed in Art. 26 of the DPD; where consent is relied on it must be specific, unambiguous and freely-given. However, it should also be ensured that the data shared outside the EU/EEA, and subsequent access by other entities within the group, remains limited to the minimum necessary for the intended purposes.

6. Conclusions and Recommendations

6.1 Fundamental rights

The contents of communications above, as well as the traffic data relating to those communications, enjoy the same fundamental rights protections as "analogue" communications.

Electronic communications made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention. Based on the current Data Protection Directive employers may only collect the data for legitimate purposes, with the processing taking place under appropriate conditions (e.g., proportionate and necessary, for a real and present interest, in a lawful, articulated and transparent manner), with a legal basis for the processing of personal data collected from or generated through electronic communications.

The fact that an employer has the ownership of the electronic means does not rule out the right of employees to secrecy of their communications, related location data and correspondence. The tracking of the location of employees through their self-owned or company issued devices should be limited to where it is strictly necessary for a legitimate

purpose. Certainly, in the case of Bring Your Own Device it is important that employees are given the opportunity to shield their private communications from any work-related monitoring.

6.2 Consent; legitimate interest

Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.

The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary.

6.3 Transparency

Effective communication should be provided to employees concerning any monitoring that takes place, the purposes for this monitoring and the circumstances, as well as possibilities for employees to prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible. The Working Party recommends involving a representative sample of employees in the creation and evaluation of such rules and policies as most monitoring has the potential to infringe on the private lives of employees.

6.4 Proportionality and data minimisation

Data processing at work must be a proportionate response to the risks faced by an employer. For example, internet misuse can be detected without the necessity of analysing website content. If misuse can be prevented (e.g., by using web filters) the employer has no general right to monitor.

Further, a blanket ban on communication for personal reasons is impractical and enforcement may require a level of monitoring that may be disproportionate. Prevention should be given much more weight than detection--the interests of the employer are better served by preventing internet misuse through technical means than by expending resources in detecting misuse.

The information registered from the ongoing monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances. Solutions that for example track vehicles can be designed to register the position data without presenting it to the employer.

Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount

of time needed with a retention period specified. Whenever information is no longer needed it should be deleted.

6.5 Cloud services, online applications and international transfers

Where employees are expected to use online applications which process personal data (such as online office applications), employers should consider enabling employees to designate certain private spaces to which the employer may not gain access under any circumstances, such as a private mail or document folder.

The use of most applications in the cloud will result in the international transfer of employee data. It should be ensured that personal data transferred to a third country outside the EU takes place only where an adequate level of protection is ensured and that the data shared outside the EU/EEA and subsequent access by other entities within the group remains limited to the minimum necessary for the intended purposes.

* * *

Done in Brussels, on 8 June 2017

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN