FACT SHEET PRIVACY AND MONITORING AT WORK UNDER THE GDPR

On May 25th 2018, the General Data Protection Regulation ("GDPR") will enter into force. With penalties of up to the higher of 20 million euro and 4% of global turnover, executives across the EU are preparing to get their organisations GDPR compliant. If you would like to know how your organisation can ensure privacy compliance at work, this fact sheet is for you.

1 | WHAT DOES PRIVACY AT WORK MEAN, AND WHY IS IT IMPORTANT NOW?

It is important to be aware that privacy compliance under the GDPR is not just about customer data. Respecting the privacy of your employees and protecting their personal information is equally important.

As most people spend a significant amount of their time at work, and the right to privacy is recognised as a fundamental right that is essential to the well-being of every human being, it is crucial that a reasonable level of privacy is ensured at work. While new (digital) technologies offer tremendous capabilities to help organisations and their employees improve work performance, and also enable opportunities like working from home, they can also blur the line between work and private life, creating significant challenges to privacy and data protection.

Employers should meet these challenges head-on, not only to avoid considerable penalties under the GDPR, but also to be competitive in attracting and keeping skilled and talented employees.

It should be noted that people who may not formally qualify as employees but are comparable to employees, such as interns and freelancers, enjoy the same privacy rights under the GDPR. The term ‘employee’ as used throughout this fact sheet therefore also includes those individuals who, from a privacy perspective, are comparable to employees.

2 | WHAT KIND OF PERSONAL DATA DOES AN EMPLOYER PROCESS?

Every employer processes personal data of all employees. For example, their names, address information, contact details, bank account numbers, and salary data. The need to process such data is self-evident, and processing such data is often mandatory for employers.

Besides such minimal mandatory data processing, employers may process a substantial amount of personal data of their employees. For example, personal data can be accrued automatically every day, as a by-product of employees’ every-day use of digital equipment and applications provided by the employer (e-mails, calendars, standard logs). Some employers even process personal data using specific monitoring or surveillance technologies. Consider for example:

- Camera images or video surveillance records;
- Information of software that maintains and analyses the use of Internet and e-mail traffic;
- Recordings of phone calls or instant messaging;
- Remote management of all mobile devices, such as phones and laptops;
- Tracking or location data of company cars or equipment.

Another thorny issue for employers is the processing of information about the health of employees, and perhaps even their sexual preferences. The GDPR contains additional requirements and safeguards to protect such sensitive information.

3 | HOW TO DETERMINE WHAT PROCESSING OF WHICH PERSONAL DATA IS PERMITTED?

The mere fact that there are many technical possibilities for monitoring employees, and storing and analysing information, does not mean that they are all legally permitted. A valid legal basis is required for all processing of personal data.
The GDPR provides the following legal grounds for processing personal data:

- Necessary for the performance or preparation of the employment contract;
- Necessary to comply with a legal obligation;
- Necessary to protect the vital interests of an employee or another natural person;
- Necessary for the fulfilment of a task carried out in the public interest or in the exercise of public authority;
- Necessary for the legitimate interests of the employer or a third party, unless the fundamental rights of the employee outweigh these interests;
- Consent of the employee for one or more specific purposes.

While consent generally may be the most important and most widely used legal ground for the processing of personal data, this is not the case in the workplace. Because the employer has authority over the employee and the employee is financially dependent on the employer, permission from an employee to an employer in principle cannot be considered as freely given. Because employers generally cannot base the processing of personal data of employees on the ground of consent, another legal ground must apply. This means that the processing must be necessary, for one or more of the purposes listed above.

4 | WHAT IS A PROPORTIONALITY TEST, AND A PRIVACY IMPACT ASSESSMENT (PIA)?

Every employer must be able to demonstrate that all processing of personal information is necessary for a purpose listed in the GDPR. Processing can only be considered necessary, if it is also proportionate. Processing cannot be considered necessary or proportionate, if the interest served by the processing is only of little importance, while the impact on privacy is high. It also means that an employer must perform only those processing operations which can achieve the intended purpose while having the least impact on privacy.

A privacy impact assessment (PIA) is an essential tool for performing and documenting such a proportionality test. A PIA is explicitly required under the GDPR if a type of processing is likely to pose a high risk to the privacy of natural persons (such as employees), in particular when new technologies are used. A high risk must be assumed and a PIA must be performed in particular if the processing involves more information, involves more sensitive information, or occurs systematically over a longer time-period, and may cause decisions about a person which have a significant effect on their life (such as legal decisions).

The GDPR also requires employers to implement privacy by design and by default. Privacy by design means that whenever new systems, applications or technologies are developed, the impact on privacy should be considered from the very beginning. Privacy by default means that the default settings of systems, applications or technologies should minimise the amount and the sensitivity of personal data processed automatically. Therefore, privacy by design and by default help ensure that personal data is only processed if this is necessary and proportionate.

While the employer’s own legitimate interests, or those of a third party, constitute a legal basis that may justify processing, this should not be assumed too easily. To apply this legal ground, a careful balancing of interests is required, demonstrating the necessity and proportionality of the processing.

The following examples may be considered as legitimate interests of the employer:

- Detection and prevention of loss of personal data (e.g. customer data);
- Detection and prevention of loss or theft of intellectual or physical business property;
- Improving employee productivity and performance.

If such interests do not put sufficient weight on the scale in the relevant circumstances, causing the employer to fail the proportionality test – for example, if a solution is also possible with less impact on the employee’s privacy – the employer risks incurring penalties and liability.

It is important to recognize that while the improvement of employee productivity and performance is a legitimate interest, it may not easily be assumed to outweigh the fundamental right to privacy of employees.

5 | WHICH PROCESSING AND MONITORING OF PERSONAL DATA IS NOT PERMITTED?

A number of processing operations should be avoided, despite any legitimate interest. In the following examples, the fundamental rights of employees will generally prevail:

- Monitoring in sensitive areas, such as sanitation, religious spaces and break rooms;
- Automated decisions about performance at work;
- Continuous monitoring of all employee activity, instead of random checks, or targeted monitoring triggered only by certain reasonably suspect activities;
- Secret recordings, in absence of a reasonable suspicion of a crime or comparable serious offence.
6 | WHAT SHOULD EMPLOYERS DO TO ENSURE PRIVACY AT WORK?

There are several key principles and obligations to protect privacy:

• Processing of personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed (data minimisation);
• The use, purpose and method of processing must be made clear to employees (transparency);
• Employees should be given the opportunity to exercise their rights (inspection, correction, erasure and restriction of processing);
• Personal data must be stored no longer required than necessary;
• Personal data must be protected by appropriate technical and organizational security measures;
• In case of any monitoring, a representative sample of employees should be involved in assessing the necessity and proportionality of the monitoring, as well as the logic and accessibility of the policy (in some countries, prior consent of a Worker’s Council is required).

7 | WHAT SECURITY MEASURES ARE NECESSARY TO PROTECT PERSONAL DATA?

Important to know is that the law does not prescribe specific security measures or standards. According to the law, security must be appropriate for the sensitivity of the data and the risks associated with processing. The cost of the measures is also a relevant factor. However, applying a standard (such as ISO 27001, 27002, 27017 or 27018) can be a good way to determine and implement the legally required “appropriate” security measures. It is also possible that certain measures or standards in a particular sector become so common that it can be very difficult to demonstrate that security is still appropriate without applying these measures or standards. For example, it appears doubtful if there are any serious hosting providers today that have not implemented any ISO 270xx standard at all.

Today, demonstrating an appropriate level of security generally appears difficult without the following measures:

• Security and authorization policy (documenting security measures, and restricting access to those who really need to know);
• Logical access control (technically implementing the authorization policy, using strong passwords and/or multi-factor authentication);
• Patch management (ensuring the timely rollout of software security updates);
• Secure Internet connections (via SSL/TLS technology, for example);
• Security of internal networks (firewalls, with proper configuration);
• Antivirus software;
• Encryption of devices or databases containing personal data (e.g. full disk encryption of laptops and mobile devices);
• Physical access protection (such as fences, locks, alarm systems, cameras).

Of course, it is also advisable to check periodically whether the measures have been properly implemented and are working properly.

A key legal obligation that should not be overlooked, is to conclude a data processing agreement with any party processing employee data on behalf or assignment of the employer, such as a salary administrator, employment service, or pension insurer or intermediary. The GDPR contains a number of specific requirements which every data processing agreement must comply with.

8 | WHAT INFORMATION IS THE EMPLOYER REQUIRED TO PROVIDE EMPLOYEES?

The employer has an important obligation to appropriately inform employees about what information about them can be processed at work, how the information will be processed, why this is necessary, and what rights the employees have to protect their privacy. The employer can comply with this obligation by means of an internal privacy statement or an internal privacy policy. This policy must be announced in a clear way and should be easily accessible to employees. For example, you can hand over the policy to each new employee and also include it in the employee portal, so that it can be accessed and downloaded at any time. When the policy is updated, it is also important that employees are informed accordingly.

The policy must include at least:

• Whether and when employee monitoring is applied;
• The purposes of data processing;
• The means used for data processing;
• An overview of the data that is kept with the corresponding retention period;
• Who has access to what data, in what circumstances;
• How data is protected;
• The rights of the employee.

The requirement to inform employees also applies afterwards. Employees who have been monitored or surveilled must be informed by the employer afterwards, even if this sometimes may not be the easiest subject to broach.
9 | WHAT CAN AN EMPLOYER DO WITH INFORMATION OBTAINED THROUGH MONITORING?

The principle of purpose limitation is very important to ensure privacy. An employer must ensure that any results of the monitoring of employees are used solely for the purpose for which they are obtained. Results of monitoring used to detect and prevent data security breaches, or to detect and prevent fraud, may not be used to assess employees for performance. Any decisions about the performance of employees, or about the terms of their employment, may never be made solely on automated processing and monitoring.

A simple, practical guideline is that monitoring employees and processing personal information obtained through monitoring is never permitted, unless the following requirements are met:

- There is a clear internal policy, that has been communicated and made available to employees.
- This policy clearly describes in which cases monitoring and processing of the resulting information can take place, for what purposes, by whom, how long the data will be stored, and the rights of employees.
- Employees, or a representative selection of employees, are actively invited to provide input to the internal policy.
- As evidenced by the internal policy, due care is taken to ensure that any monitoring, and the processing of resulting information, does not restrict the fundamental right to privacy of employees any more than strictly necessary for a legitimate purpose recognized under the GDPR.

10 | SOME PRACTICAL EXAMPLES

Below are some examples to help you apply the privacy rules correctly, in accordance with the opinions published by the Article 29 Working Party (WP29). WP29 is an official EU institution to promote the uniform application of privacy laws in the EU, composed of representatives of each national privacy authority and the EU institutions.

Social media and recruiting new staff

Is it permitted to examine the social media profiles of a potential new employee? The answer to this question can be found by answering some other questions first. Is the social media account related to professional purposes? Is the profile likely to contain information about skills or characteristics of the candidate, that are highly relevant to the job on offer? If both questions can be answered with yes, and candidates are made aware that their social media profiles may be examined, for example in the vacancy description, this is permitted according to WP29.

Camera surveillance at work

For each camera that you install as an employer, you need to determine what the legitimate interest for this is. Do you want to secure business properties? That is a legitimate interest that could potentially outweigh the privacy interest of the employee. However, you should always consider whether another means with less impact on privacy may also be capable of achieving the same purpose. For example, you may consider a motion sensor, or a camera pointed at the doors rather than at the workspaces of employees. Continuous recording of employee behaviour should be avoided. Cameras installed for security against theft and similar infringements, may not be used to review employees’ general work performance and attendance.

Clear rules should be established about how long the recordings are stored, who may review such recordings, and in which cases. Employees should be appropriately informed of this. To mitigate the risk of abuse, it may also be wise to require any review of the recordings to be performed by two persons. Having a different person perform the review than the person who decides that an incident requires a recording to be reviewed, may also help.

Biometric data processing

Automated monitoring and recognition of employees’ facial features and expressions, is generally considered unlawful. Using biometrics for access control in the workspace, such as facial, iris, or fingerprint scanners, appears problematic as well, as employers cannot rely on consent, and no other exception to the general prohibition to process biometric data appears applicable. Member states are permitted to create their own rules concerning biometric data, however.

Data loss prevention and detection systems, monitoring communications

Various vendors currently offer data loss detection and prevention systems, which can automatically scan electronic communications, such as e-mails. If such solutions are used, they must be implemented carefully, so that the impact on personal privacy of employees is limited to what is strictly necessary.

As there may be significant risks of false positives in such systems, which could cause illegitimate processing of personal data of employees, affirmative steps must be taken to safeguard employee privacy. For example, users should be clearly informed of the rules that the system follows to characterize an e-mail as a potential data breach. Whenever a message or communication is suspected by the system, users should be clearly informed as well, so that they have the option to cancel the transmission.
Tracking of the means of transport used by the employee
For many modes of transport, GPS is able to track the location real-time and possibly even get additional information about the remote vehicle. An employer may be interested in following its transport trucks or pizza delivery scooters. A legitimate interest may be to be able to recover the vehicle after theft. Real-time viewing of location data will usually violate the privacy of the employee who is moving with it, unless there is a specific incident that can justify this, such as theft of the vehicle, or if the current delivery is running late.

Working from home and other forms of remote working
Today, work can often be performed from any location with a working internet connection, using a laptop, mobile phone and/or tablet. Employers therefore increasingly permit and facilitate remote working. A legitimate concern for employers may be how to appropriately safeguard the security of sensitive (personal) data processed while working remotely, and whether employees working remotely are indeed working the agreed amount of time. It is not legitimate, however, to deploy monitoring tools which record keystrokes, screen activity, webcam footage, and/or microphone recordings to keep track of the activities of employees working remotely. While such technologies may be widely available, the impact on privacy is generally too great to justify, even if the equipment is owned by the employer. If the equipment is not owned by the employer, any monitoring tools installed or used on employee equipment could potentially be classified as a computer crime.