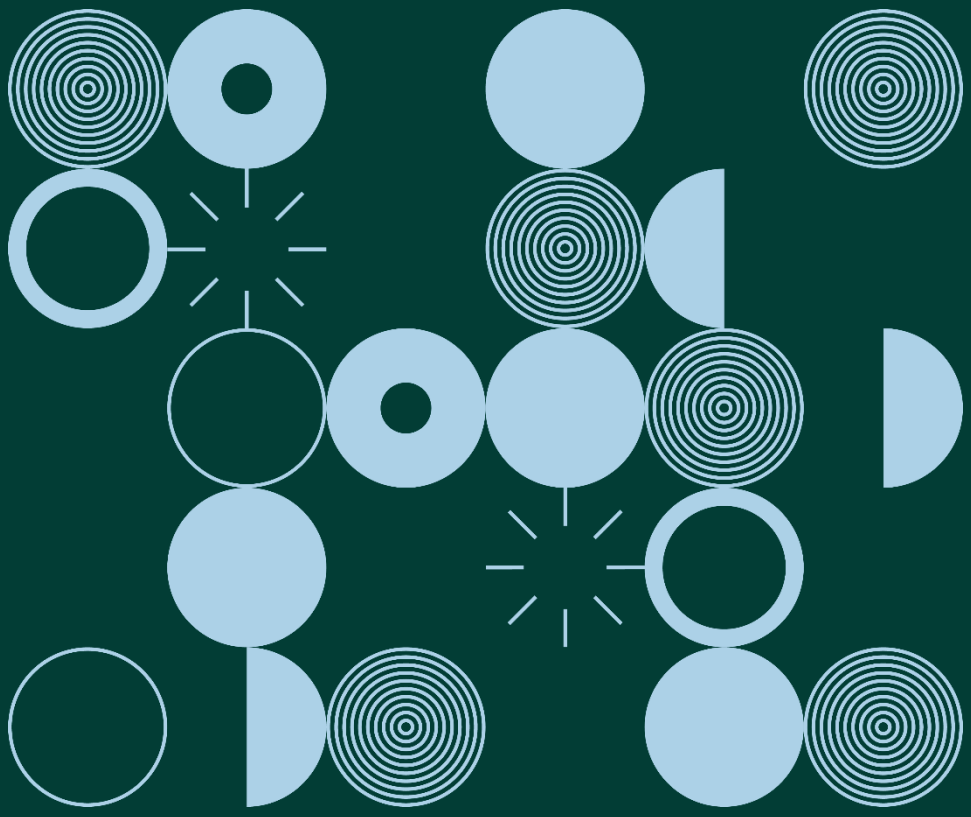
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Data Protection in the Workplace:

Employer Guidance

April 2023



Contents

Introduction

The Data Protection Commission (DPC) has extensive guidance for organisations which can be accessed here. This guidance document is specifically aimed at assisting employers as data controllers regarding their data processing obligations and duties when processing the personal data of their employees, former employees and prospective employees. In particular, employers as data controllers ought to be aware that Chapter IV of the General Data Protection Regulation ("GDPR") concerns controllers and processors, and their respective responsibilities and agreements. For further information on this please see here.

Employers collect and process significant amounts of personal data on prospective and current employees. In some instances, employers may also continue to process personal data of former employees. This personal data can range from basic information such as names, addresses and PPSNs, but can also include information on occupational health, sick leave, performance reviews or disciplinary actions. Therefore, employers ("data controllers") must be mindful of their responsibilities, obligations and duties under the GDPR and the Data Protection Act 2018 ("2018 Act").[1] This includes ensuring they have appropriate policies and procedures in place as well as understanding how to respond to requests from employees (including former employees and unsuccessful candidates in the recruitment process whose data they may continue to retain) regarding the exercise of their data protection rights.

Although not all organisations are required to have a Data Protection Officer (DPO), organisations might find it useful to designate an individual within their organisation as the data protection contact. This also applies to employers as data controllers.

Is it Personal Data?

Within the employment context, it is important to distinguish between commercial and personal data, as the GDPR applies to personal data, but does not apply to commercial data. In many cases, it will be obvious what is commercial or personal data, however, in other instances it will be less clear.

Employee emails

An area which the DPC receives a large amount of queries on is the status of work emails. This query arises primarily within the context of an employee making a data subject access request. While it is clear that an individual's name is their personal data, within the employment setting does the content of an email signed off by an individual in their professional or work capacity constitute their personal data? It is unlikely that it does. Where this is most relevant is if a subject access request is made. Under those circumstances there is an obligation on employers to investigate the content of their commercial or business emails to ascertain if the content of the email, which may be signed off by an employee, can be considered the personal data of the employee.

[1] Article 88 of the GDPR provides for processing in the context of employment. This Article permits Member States to adopt laws, collective agreements or rules for the protection of the rights and freedoms in respect of the processing of personal data of employees within the employment context.

Name in a work email address

Work email addresses can be found in different formats. Some email addresses are generic, such as info@abc.ie. Such an email address does not contain personal data although it may be manned by only one individual. Occasionally a work email address may contain an individual's first name such as John@abc.ie. This may or may not constitute an individual's personal data and depends on context, such as, the number of employees named John working in the organisation. If however, the email address is, for example JohnSmith@abc.ie, this is likely to be considered personal data as it sets out the full name of the individual and consequently the individual is likely to be identifiable. However, as set out in the preceding paragraph, this does not mean that the content of the emails addressed to the identified individual constitute the individual's personal data, as the emails occurred within the context of a professional working environment. However, when an employer has received a subject access request, there is an obligation on employers to investigate the content of their commercial or business emails to ascertain if the content of the email to the identifiable individual relates to the personal data of that individual in any way. In circumstances where an employee has a long employment history with an employer, it may be the case that several thousand emails have been generated during the course of the employee's employment. In cases such as these the DPC would advise the employer to ask the employee to specify in their request a particular date or time. Full Guidance for data controllers in the area of subject access requests is available here.

Outlook Calendar and Job Description

As to whether an outlook calendar and job description is personal data is best illustrated by the following example:

Case Study: An employee's incomplete access request submitted to their employer.
An employee made a complaint to the DPC as they were dissatisfied they had not been provided with a copy of their personnel file or a copy of their job description when they made a subject access request to their employer. The employer advised they had previously provided the employee with a copy of their personnel file and said that a copy of their job description would not be provided as it did not contain their personal data. The employee also sought data from their Outlook calendar as part of their subject access request. The employee believed that this data related to organised events relating to work and due to their involvement the data was personal. The employer stated to the DPC that the details of meetings in the data subject's outlook calendar would not be provided as this information is work related and is not about the data subject. The DPC was satisfied that the job description and outlook calendar do not fall under the remit of personal data as defined in Article 4(1) of the GDPR.

Employer's Obligations and Responsibilities

(a) General Principles

Employers should be aware of the principles of data protection under Article 5 of the GDPR, which provides that the processing of personal data must be lawful, fair, transparent, and comply with the principles of purpose limitation, data minimisation, accuracy, storage limitation, integrity and

confidentiality, and accountability. Employers must be also able to demonstrate compliance with all of these principles. To give an example, an employer can demonstrate transparency in the workplace by way of an easily accessible HR self-service system that would allow an employee to see what data an employer holds on them, and how it is used. This system would be documented in internal HR policies and include details in what personal data is being collected and what the purpose of the processing is. This system could include an employee's address, their current employment status, whether they are married or single, and their salary information. The system would also include an employee's performance review and any sick leave the employee has taken. Allowing an employee full access to this information demonstrates that an employer is being transparent about what information it holds on an employee.

Lawfulness, fairness and transparency

Employers must provide individuals with clear and transparent information about the purpose(s) for which they process personal data and the legal basis/bases they rely upon to do so. It should be transparent to employees when and why their personal data is collected, used, consulted or otherwise processed. This transparent information on data processing should be easily accessible and easily understood by using clear and concise language. Further obligations on the information employers need to provide to meet their transparency obligations are set out under Articles 13 and 14 of the GDPR.

Purpose limitation

The purpose for the processing of personal data should be explicit and determined at the time of the collection of the personal data. Personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. What this means is that if an employer collects personal data, such as the private email address of an employee, for the sole purpose of communicating certain HR matters to the employee prior to commencing employment, the employer cannot subsequently use that private email address of for another purpose or share that email with another organisation in the absence of a lawful basis. This is because the subsequent processing is unlikely to be compatible with the original purpose for which the data- the email address, was originally collected.

Case Study: The use of car park and building access data had been used by a manager to verify employee's time and attendance record.

In a matter where a complaint was made to the DPC in relation to the use of car park and building access data that had been used by a manager to verify employee's time and attendance record, an employer stated the company car park and building access data was collected for security purposes and for the purposes of verifying time. The employer also stated that attendance in the building was a security concern. The DPC deemed such processing incompatible further processing, as the employees had not been informed that such data would be used to verify their time and attendance. The DPC informed the employer of this and highlighted that it was concerning regardless of the proposed lawful bases relied upon. The DPC recommended the employer consider alternative an alternative way to verify time and attendance. In addition to this the employer was required to update their record retention policy to include car park and building access data and provide staff training on the GDPR.

Data minimisation

This requires employers to assess the necessity of their processing of personal data. Processing of personal data must be adequate, relevant and limited to what is necessary for the purposes of the processing. Any processing beyond what is necessary for the purpose(s) may not have a valid legal basis.

Storage limitation

Employers should only keep personal data in a form that permits identification of a data subject for as long as is necessary for the purposes of the processing. Time limits should be established for the erasure of personal data to ensure data is not kept for longer than necessary and those time limits should be subject to periodic review. Further details of Retention Periods is addressed below.

Integrity and confidentiality

Employers should ensure they implement and process personal data using "appropriate security", Article 5(1)(f) of the GDPR gives examples of these security measures as *"including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".*

> ***Case study: Access and circulation of an employee's personal email.***
>
> *An employee made a subject access request as they believed they had not been supplied with all the relevant documents when they made a subject access request to their employer. The employee first contacted the DPC when they discovered their employer had printed and circulated their personal emails. The employer explained that when the emails were first accessed it was assumed they were on a work email account. The employer later discovered it was a personal email account but stated there was a business protection purpose for accessing the personal emails. The employer sought to rely on Article 6(1)(f) as a lawful basis for processing the employee's personal emails. The DPC informed the employer that such interests must be balanced with an employee's interests and rights. The DPC advised that the employer had infringed the employee's rights under Article 5(1) (a), (b) and (f) of the GDPR. The DPC recommended that the employer ensured their privacy policy and/or data protection policy is up to date and fully compliant with the GDPR.*

(b) Legal Bases

Employers must have a lawful basis to process personal data under Article 6 of the GDPR. In addition, if an employer is processing special category data such as health data (for example medical certificates or occupational health reports), the employer will also need to avail of one of the permissible exceptions for processing personal data under Article 9 of the GDPR.

Article 6 of the GDPR provides for the following legal bases:

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

(b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Employers must determine, prior to processing, which legal basis they are relying upon to ensure their processing of employee personal data is lawful. Employers may rely on different legal bases for the processing of personal data as it relates to their specific circumstances. It is a matter for the employer to make those determinations as to what personal data is required to be processed for what purpose.

The Necessity Requirement

The requirement of 'necessity' applies to all legal bases save for the consent of the data subject. Employers should assess what personal data is actually ***necessary*** for the relevant legal basis and purpose that they are relying upon in processing the personal data.

In assessing necessity, employers should consider the reasonableness and proportionality of the processing. Whether there a more reasonable or less intrusive way to achieve the stated purpose without processing personal data, or can their objectives be achieved by processing less personal data. If so, this ought to be done as otherwise there is a risk that the legal basis upon which the employer is relying will be unlawful. This necessity element will be a case-by-case assessment, depending on the circumstances of the processing.

Legal Basis: Consent

Consent is the most familiar legal basis for both data subjects and data controllers. However, it is not necessarily the most appropriate legal basis, particularly in the employment context when considered in conjunction with the conditions attached for valid consent.

Under Article 4(11) of the GDPR, consent must to be freely given, specified, informed and unambiguous, and made with a clear affirmative action or statement. Pre-ticked boxes will not comply with the requirement to be a clear affirmative action or statement. In order to meet the requirements of 'specific and informed' consent, data controllers should make efforts to present data subjects with information and choice to ensure the data subject understands what they are consenting to.

Consent may not be an appropriate legal basis for employers to rely upon for the processing of their employees personal data; this is because there is a clear power imbalance between employees and employers that undermines the level of choice an employee will have, or feel they may have, in giving consent. Where an employer attempts to rely on consent to process employee personal data, the employee must be given an option to withdraw their consent at any time. Employers need to ensure they can facilitate this withdrawal of consent and make that process easy for employees.

Legal Basis: Contract

The legal basis of contractual necessity is a common lawful basis for employers to rely upon, given a contractual relationship often exists between an employer and employee. Employers should note that the processing of personal data should be "necessary for the performance" of the employment contract, otherwise they may need to consider reliance on another legal basis. Employers should note this legal basis only applies where the contract is between the employer and employee. A contract between the employer and a third party cannot fall under contractual necessity as a legal basis for processing of employee personal data. An example of lawful basis in this context is the performance of a contract: an employer will need to process an employee's personal data to perform their obligations under a contract, such as processing the employee's bank details to pay the employee.

In assessing if the processing of personal data is necessary for the performance of a contract with the employee, employers should again consider if the processing is objectively necessary and proportionate. Are other alternative and less intrusive measures available? The contractual terms may themselves specify that certain processing activities are necessary for the contract. However, all processing activities need not be specified within the contract itself and some processing activities may be covered by the general context of the contract. That being said, an employer will still be required to meet their transparency obligations as set out under Articles 13 and 14 of the GDPR when relying on contractual necessity as a legal basis.

If processing of special category personal data is necessary for the performance of an employment contract, the employer should identify a separate exception to the general prohibition on the processing of special category personal data under Article 9(2) of the GDPR.

Legal Basis: Legal obligation

Where an employer is obliged to comply with EU or national law, 'compliance with a legal obligation' may be an appropriate legal basis to rely upon. However, the requirement to assess necessity of the processing still applies. The EU or national law does not have to specify the processing activity, but if the overall purpose of the processing is compliance with the law and the law has a sufficiently clear basis then this legal basis may apply.

The legal obligation must be laid down by EU or national law and this includes other forms of law, including common law or any form of soft law (for example guidelines/recommendations that are not necessarily legally binding but are adhered to generally).

However, the law must be clear and precise, ensuring its application to a data subject is foreseeable. There should be a public interest achieved by the law and it should be proportionate to that aim or goal. A single law may provide a legal basis for several processing activities. Transparency obligations remain and an employer should inform their employees of what laws they rely upon or are complying with when processing employee personal data. Further, an employer will also need to assess the necessity and proportionality of the processing to comply with a legal obligation.
An example of this legal basis used in an employment contract is where an employer will provide employee data to Revenue to comply with tax requirements or to comply with an employer's obligations under the Health, Safety and Welfare at Work Act 2005. An example of this type of

processing includes employers complying with their statutory obligations, for example, an employer is required to keep records showing their compliance with the provisions of the National Minimum Wage Act 2000. An employer can do so by retaining payslips for the specified period, showing that all employees were paid the national minimum wage.

Legal Basis: Vital Interests

Vital interests is not a commonly used legal basis and will only apply in certain limited specific situations and where another legal basis is not appropriate.

Vital interests are generally where it is "necessary to protect an interest which is essential for the life of the data subject or that of another natural person" (Recital 46 of the GDPR). So, situations involving threats to the life or health of the data subject or another person may give rise to this legal basis. This legal basis is most likely to arise in the context of medical or healthcare data, including a person's mental health. Article 9(2)(c) of the GDPR provides an exception to the general prohibition on processing special category personal data to protect vital interests. However, it is less likely to provide a legal basis outside of emergency situations.

Legal Basis: A task carried out in the public interest

Most commonly this lawful basis will be relied upon by public authorities or persons governed by public law, but can also include professional associations or controllers governed by private law.

Legal Basis: Legitimate interest

Legitimate interest is probably the broadest legal basis an employer can seek to rely upon. Legitimate interest is a versatile legal basis, often covering situations that do not fit into other legal bases. However, just because the data processing operations do not fit into the other legal bases does not mean that this legal basis will automatically apply either. Heightened considerations apply to legitimate interest as a legal basis.

Employers who seek to rely on the legitimate interest legal basis need to meet three components for this legal basis to apply:

a) identifying a legitimate interest which they or a third party pursue;
b) demonstrating that the intended processing of the data subject's personal data is necessary to achieve the legitimate interest; and
c) balancing the legitimate interest against the data subject's interests, rights, and freedoms.

Although it is a matter for the employer as data controller to set out and identify their legitimate interests, types of legitimate interest can include commercial interests, third party commercial interests, broader societal benefits or preventing fraud. The processing of personal data will only be lawful where the legitimate interest identified is not overridden by the interests, rights and freedoms of the data subjects/employees. Therefore, it may be necessary for an employer to carry out a balancing exercise between their legitimate interests and the rights and freedoms of their employees through a Data Protection Impact Assessment (DPIA). Further information on DPIAs can be accessed here. An employer should ensure this balancing exercise/ DPIA is in writing before the processing takes

place. Should a complaint be received by the DPC from an employee and the employer has relied upon this legal basis for the processing of personal data, the DPC will request sight of the DPIA.

Employers will again need to consider the necessity of the processing of personal data, the proportionality and if any less intrusive measures are available. Overall, employers need to consider if the processing activity is reasonable which will depend on the circumstances of the case. An example of this type of processing would include the use of CCTV for the purpose of monitoring building security. A DPIA in this instance should take note of the legitimate interest of the employer to ensure the security of their building whilst also noting the rights and freedoms of their employees that the CCTV is used for the specified given purpose only and not to monitor employee entry and exit times, unless specified in any internal policy.

Legal Basis: Article 9 Special category personal data

Article 9(1) of the GDPR defines special category personal data as:

> "*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and …the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

There is a general prohibition of the processing of special category personal data under Article 9(1) of the GDPR. However, there are exceptions to this prohibition contained under Article 9(2) of the GDPR. For example, an exception is carved out for the purposes of occupational medicine or evaluating the capacity of an employee within the workplace under Article 9(2)(h) of the GDPR. For example, an employer may be required to retain health data, which falls within the category of special category data, where an employee is pregnant to ensure that the employer complies with its obligations under the Maternity Protection Act 1994.

(c) Occupational Health

Occupational health refers to the promotion and maintenance of physical, social and mental well-being of workers in all occupations. In Ireland occupational health is underpinned by the Safety, Health and Welfare at Work Act 2005 ("the 2005 Act"). Article 8 of the 2005 Act outlines the general duties of employers when ensuring the health and safety of their employees. The 2005 Act places obligations on both employers and employees to ensure that the worker is fit to carry out their duties in the workplace. Under Article 23(1) of the 2005 Act "*an employer may require an employee of a class or classes, as may be prescribed, to undergo an assessment by a registered medical practitioner, nominated by the employer, of his or her fitness to perform work activities*". The purpose of this assessment is to ensure the employee's fitness to perform work activities. As per Article 23(3) of the 2005 Act a registered medical practitioner is obliged to notify the employer if the employee is unfit to perform work activities.

The referral of an employee to undergo an assessment by a registered medical practitioner may give rise to data protection implications under the GDPR, in particular Article 9. As previously outlined, employers must determine, prior to processing, which legal basis they are relying upon to ensure their processing of employee personal data is lawful. It is best practice for employers to outline this lawful

basis to their employees in order to ensure compliance with the data protection principles set out in the GDPR. In an occupational health context certain lawful bases for processing may apply, such as, Article 6(1)(c), Article 6(1)(d), Article 6(1)(f), and Article 9(2)(h) of the GDPR. Consent may also apply as a lawful basis for processing an employee's medical data, although limitations may apply. An employee's consent under Article 9 of the GDPR must be ***explicit*** and freely given and an employer must ensure that the employee has been properly informed prior to the assessment.

An employer's obligations under Article 24 of the GDPR includes the implementation of appropriate data protection policies which ensure lawfulness, fairness and transparency. The inclusion of an occupational health policy will allow both the employer and employee to engage with registered medical practitioners to the extent necessary to ensure the employee's fitness to work is guaranteed.

Case Study: Processing of an employee's personal data by a third party.

An employee was dissatisfied with the processing of their personal data by a third party, namely a HR investigator. With regard to the HR investigator the employer provided Articles 6(1)(c) and 9(2)(b) as their lawful basis for processing their employee's health and special category data. The employer also highlighted their legal obligations under the Safety, Health and Welfare at Work Act 2005 as outlined in their Employee Handbook. The DPC was satisfied that the employer had a lawful basis for processing their employee's personal data in this manner. The DPC recommended that the employer inform their employees in their data protection policies that they may rely on Articles 6(1)(c) and 9(2)(b) for the processing of employees personal data.

Data Protection (Access Modification) (Health) Regulations 2022

This amendment revoked and replaced the Data Protection (Access Modification) (Health) Regulations 1989 which modifies how data subject access requests received by employers can be addressed.

This modification means that an employer is no longer obliged to consult a medical practitioner before providing health data to the employee in response to their subject access request. The new Regulations provide that where the data controller/employer '*has reasonable grounds for believing that granting access to the health data concerned would be likely to cause serious harm to the physical or mental health of the data subject*' discretion can be exercised by the employer as to whether the data will be released. This refers only to the part of the data that may be '*likely to cause serious harm*' and the rest of the data must be released unless the data controller is relying on other lawful exceptions. Employers can seek medical input and opinion if required, however, consideration must be given to the principles of data minimisation and security of data as set out under section 8 of the Health Regulation (this includes providing only the data of concern to the appropriately qualified medical practitioner which must be in a pseudonymised format). If the employer is not going to release the data, under section 9 of the Health Regulations, they must advise their employee that they can request that the data be made available to a suitably qualified health practitioner and that the data can be kept available for that purpose.

(d) Employer Policies and Monitoring Employees

Introduction

Article 24(1) of the GDPR requires data controllers to "*implement appropriate technical and organisational measures"* for compliance with Article 5(1)(f) of the GDPR. Examples of technical and organisational measures within the employment context include measures such as, but not limited to, pseudonymisation, anonymisation, limiting access to personal data to authorised people, encryption, backups and testing, file access audit logs.

Article 24(2) of the GDPR details that appropriate technical and organisational measures "*shall include the implementation of appropriate data protection policies by the controller*". Employers may wish to implement data protection policies specifically for the processing of employee data and a separate policy for the processing of any personal data of clients or members of the public. Employers may also wish to have separate data retention and storage, internet usage, use of personal device and CCTV policies for employees and clients or members of the public. Those policies will need to meet the transparency obligations set out under Articles 13/14 of the GDPR and must *"be easily accessible and easy to understand, and that clear and plain language be used"* (Recital 39 of the GDPR).

In addition to employer policies, employers are required to consider their relationship with any third parties who process data on their behalf in connection with them. In this regard, appropriate agreements need to be in place between data controllers and processors or between joint controllers.

CCTV

For information and case studies on CCTV in the workplace please see our extensive guidance here.

Computer Networks, Internet and E-mail

The DPC accepts that organisations have a legitimate interest in protecting their business, reputation, resources and equipment. To achieve this, organisations may decide to monitor their staff's use of the internet, email and telephone. However, it should be noted that the collection, use or storage of information about workers, the monitoring of their internet access or email or their surveillance by video cameras (which process images) involves the processing of personal data and, as such, data protection law applies. In addition, individuals have a right to private life at work under the European Convention on Human Rights (*Barbulescu v. Romania* (application no. 61496/08)) which highlights the necessity for appropriate care in monitoring employees and setting clear policies. Therefore, such practices and policies should reflect an appropriate balance between the legitimate interests of the employer, and the data protection rights and right to private life of the employees. The EDPB's Guidelines 3/2019 on processing of personal data through video devices acknowledges that while some individuals may be comfortable with the use of video surveillance for security purposes, it states that '*guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g…..employee performance monitoring*….)'. Further it states that '*an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer*.' An individual does not lose their privacy and data protection rights just because they are

an employee. Any limitation of the employee's right to privacy should be proportionate to the likely damage to the employer's legitimate interests. An acceptable usage policy should be adopted reflecting this balance and employees should be notified of the nature, extent and purposes of the monitoring specified in the policy.

In principle, there is nothing to stop an employer specifying that use of equipment is prohibited for personal purposes but the likelihood is that most employers will allow a limited amount of personal use. In the absence of a clear policy, employees may be assumed to have a reasonable expectation of privacy in the workplace.

The following points need to be addressed by data controllers/employers:

- The legitimate interests of the employer to process personal data that is necessary for the normal development of the employment relationship and the business operation.
- Monitoring, including employees' email or internet usage, surveillance by camera, video cameras or location data must comply with the transparency requirements of data protection law. Staff must be informed of the existence of the surveillance, and also the purpose for which personal data are to be processed. If CCTV cameras are in operation, and public access is allowed, a notice to that effect should be displayed. Any monitoring must be carried out in the least intrusive way possible. Only in exceptional circumstances associated with a criminal investigation, and in consultation with An Garda Siochána, should resort be made to covert surveillance
- Monitoring and surveillance, whether in terms of email use, internet use, video cameras or location data, are subject to data protection requirements. Any monitoring must be a proportionate response by an employer to the risk they face, taking into account the privacy and other interests of workers.
- Staff should be aware of what data an employer is collecting on them in line with the transparency principles in Articles 12-14 of the GDPR. Staff have a right to access a copy of their personal data under Article 15 of the GDPR.
- Any personal data processed in the course of monitoring must be adequate, relevant, not excessive and not retained for longer than necessary for the purpose for which the monitoring is justified.
- Appropriate safeguards ought to be in place but particularly if the monitoring is intrusive. The European Court of Human Rights in *Barbulescu v. Romania* held that such safeguards ought to ensure 'that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality'.

Internet

Private use of the internet in the workplace and the monitoring of private emails pose certain challenges. A workplace policy should be in place in an open and transparent manner which should ensure that:

- An impartial balance is struck between the legitimate rights of employers and the personal privacy rights of employees;

- Any monitoring activity is transparent for all workers;
- Monitoring is fair and proportionate with prevention being more important than detection.

Employers should consider whether they would obtain the same results with less intrusive measures of supervision.

Employee Monitoring Software- Keystroke Logging or "Tattleware"

It should be noted that monitoring software is extremely intrusive and that any attempt to use it must be objectively and demonstrably justified and proportionate. In light of the highly intrusive nature of such monitoring applications, in the ordinary course of an individual's employment, employers should implement other less intrusive means by which to monitor employee attendance and productivity. It should also be noted that such monitoring may be subject to employment law. If an employer wants to install covert software, by way of keystroke logging, "tattleware" or other monitoring software programmes on an employee's PC or laptop to investigate possible misconduct, or to monitor an employee's activity when working or working from home, it should be borne in mind that the use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. All employees should be given a policy on email and internet use in the workplace, known as an Acceptable Usage Policy (AUP). This should clearly set out an employer's policy on internet usage, including the use of social media on an employer owned PC or laptop.

Covert Surveillance in a Workplace Setting

Covert surveillance should be avoided where at all possible and is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies that a written specific policy be put in place detailing the purpose, justification, procedure, measures and safeguards that will be implemented with the final objective being an actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a consequence of an alleged committal of a criminal offence(s).

Any case for covert surveillance must be justified prior to it occurring and should only be done on a case by case basis. The following issues would need to be fully considered:-

- What is the specific purposes that the covert surveillance is trying to achieve? If it is to gather evidence then there must first be a substantive factual circumstance(s) that identifies an area of concern that needs to be further investigated by covert monitoring.
- Is this purpose a lawful objective? For example are there any laws that prohibit such surveillance?
- Are there any alternative options to covert surveillance? For example blocking access on work computers to social media or other non-work related sites?
- Is there any circumstantial evidence to support covert monitoring of an employee(s)? If so how serious an issue is it? There should be a risk analysis done as to the scale of inappropriate employee behaviour ranging from the most serious i.e. a criminal offence of fraud/ stealing/ gross negligence that could warrant an action for dismissal from employment to the less

serious issues, such as timekeeping/ personal emails, SMS or phone calls, that usually only warrant a manager's supervision.

- Relevant written company policies should be in place on workplace practices expected of employees.
- Article 6(1)(f) of the GDPR provides that a data controller, may process personal data in relation to a data subject / employee if;- "the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…". For this to occur any processing that is to be considered a 'legitimate interest' must also balance the employment rights of the employee and their fundamental rights to privacy, data protection, fair procedures etc.
- Prior to any covert surveillance or monitoring senior management should write a detailed policy that sets out the following:-

  - Full details as to why the covert surveillance is required and why identified individuals are being targeted.

  - Objective to be achieved. What type of evidence is being searched for and is it relevant, proportionate and not excessive?

  - How will this evidence be used? Will it be disclosed to an enforcement agency or is there potential for civil litigation?

  - What happens to irrelevant data collected? Deletion policy must be in place for such data.

  - Who in the organisation has overall responsibility for covert surveillance or monitoring and who else has authorised access to the data collected?

  - It is recommended that an independent review of data collected by solicitor / legal adviser or trusted third party is carried out.

  - It is recommended to set a short time period for surveillance or monitoring i.e. one month or less if sufficient evidence collected in a shorter period.

  - An organisation should undertake to present copy of full data set collected to each affected individual employee on completion of project together with copy of Policy justifying it.

Vehicle Tracking

In order for in-vehicle tracking to be lawful under GDPR, strict requirements must be met by the employer. Vehicle tracking should not be used for the general monitoring of staff. For further and more extensive information Guidance on this topic can be accessed here.

Retention Periods

The length of time an employer can hold an employee's data is influenced by a number of factors, for example, there may be statutory obligations or industry guidelines which dictate the retention periods. Compliance with the principle of storage limitation mandates that the data is retained for the least amount of time required to achieve the objective while ensuring that it is stored securely and is subsequently destroyed securely at the appointed time.

The following are examples, but not an exhaustive list, of some retention periods which apply to employers:

Employee details	3 years	Section 25 Organisation of Working Time Act 1997
Payslips	3 years	Section 22 National Minimum Wage Act
Parental leave/Force Majeure	8 years	Section 27 Parental Leave Act 1998
Taxation	6 years	Companies Act 2014 and Taxes Consolidation Act 1997
Workplace accidents	10 years	Section 60 S.I. No. 44/1993 Safety health and Welfare at Work (General Applications) Regulation 1993

(e) Employee Rights

Individuals have a number of specific rights under data protection law to keep them informed and in control of the processing of their personal data. It is important that employers are aware of these rights as they have certain obligations and time frames to adhere to should an employee wish to exercise any of these rights. While data protection rights are sourced under Articles 15-22 and 34 of the GDPR, the most commonly exercised rights of individuals within the employment context are the right to access personal data (Article 15) and the right to rectification (Article 16). Under Article 12(3) of the GPDR, employers have up to one month from the date of receipt of the request to respond to requests made under Articles 15-22. This time frame can be extended by up to two further months, taking into account the complexity of the request. The employer must let the employee know before the expiry of the one month deadline, that an extension of time is required to deal with the request and they must state why. Extensive subject access request guidance can be found for employers here and for employees here.

Although these rights exist, no right is absolute and employers can lawfully restrict the data protection rights of individuals in line with various provisions, such as Article 23 of the GDPR and/or Section 60 of the Data Protection Act, 2018. If an employer is relying on these provisions to restrict the data protection rights of an employee who has sought to exercise their rights, they must set out which provision is being relied upon.

Right to Access Personal data

Article 15 of the GDPR provides individuals with the right to request a copy of their personal data. They are also entitled to receive the information set out under Article 15(1) as part of their Article 15 request. These requests must be responded to free of charge and in an accessible form within the specific time frame.

If an employer engages the services of a data processor and an employee makes an access request to the employer/controller for access to a copy of the personal data the processor holds on them, the responsibility for fulfilling the access requests rests with the data controller and not the processor.

Right to Rectification of Personal Data

Article 16 of the GDPR provides the right to have inaccurate data rectified. This is in line with the principle under Article 5(1)(d) of the GDPR that data shall be accurate and up to date.

However, the right to rectification is not an absolute right and depends on the circumstances of the request. Article 16 provides for the 'purposes of processing'; in other words, when considering a request for rectification, the request must be considered in line with consideration of the purposes for which the data was processed at the time.

Case Studies

Processing an employee's personal data in relation to an incident that occurred during working hours.

An employee objected to their employer viewing and using CCTV footage which they had obtained from a third party in order to investigate an incident. The employer stated their legal basis for processing was Article 6(1)(b), (c), (e) and (f) of the GDPR for processing the personal data contained in the CCTV footage for the purpose of grounding disciplinary proceedings. The DPC found that the processing of the CCTV footage, collected from the third party, for use in connection with its investigation was not incompatible with the purposes for which the footage was originally collected by the third party, their purpose was security of the building, employees or visitors.

Retention of records on an incident log maintained by their employer.

The incident involved the employee contacting a member of staff on their personal private number (having obtained this number from the staff members' personal Facebook page). The employee sought erasure of the incident report. The employer relied on both Articles 17(3)(b) and 17(3)(e) of the GDPR, namely that under Safety, Health and Welfare legislation they were obliged to keep a risk register as an employer and "for the establishment, exercise or defence of legal claims", including any possible claim the staff member might make against the employer. The DPC recommended that the employer informs employees of the retention period for such incident reports in the future.

Installation of CCTV cameras in the workplace without prior notification.

The employee was concerned that their personal data was not being processed in a fair and transparent manner. The employee felt their employer did not have a legitimate purpose for their new CCTV usage. The DPC had to examine whether the employer carried out a balancing test before installing the cameras. The employer in this case had conducted a balancing test prior to installation and informed the DPC of the purpose of the CCTV system, namely Health & Safety and the protection of customers, employees and property. The DPC advised the employee that their employer had a legitimate interest in processing the personal data and the employer had taken reasonable steps to ensure their employees were aware of this.

Installation of CCTV cameras in the workplace.

CCTV cameras had been installed by an employer in the employee base area. The employee felt the CCTV cameras were excessive and they had concerns about the live-monitoring and further processing of footage to monitor employees. The employer provided a description of each camera and the requirement for each. The employer informed the DPC there had been theft of company property. The employer engaged with staff through the WRC to rectify the misbehaviour and although the behaviour continued it stopped when the CCTV system was installed. The DPC considered the legitimate interest of the employer to protect their property, the alternative measures considered and tried by the employer and that no cameras were installed in the break room or canteen. The DPC recommended to the employer not to utilise live monitoring of the system, as the stated misbehaviour stopped without the need for live monitoring, and further recommended that the employer did not further process the footage to monitor the performance of their staff.