GRA
GIBRALTAR REGULATORY AUTHORITY

(25) Data Protection in the Employment Context

Guidance on the Gibraltar General Data Protection Regulation & Data Protection Act 2004

21st December 2021

Guidance Note IR01/21

FOREWORD

Gibraltar's data protection law consists of both the Gibraltar General Data Protection Regulation ("Gibraltar GDPR") and the Data Protection Act 2004 ("DPA").

The legislation in Gibraltar maintains the data protection standards that applied in Gibraltar as a result of EU Law (i.e., the EU General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680), prior to Brexit and the end of the transition period.

Organisations involved in the processing of personal data need to be aware of the obligations that the Gibraltar GDPR and/or the DPA impose on them.

The Gibraltar Regulatory Authority, as the Information Commissioner, regularly publish guidance notes that aim to –

- *raise awareness amongst controllers and processors of their data protection obligations; and,*
- *assist them in ensuring compliance.*

Guidance notes also aim to promote public awareness of the risks to personal data that may arise from data processing activities.

SUMMARY

This document provides detailed guidance to facilitate data protection compliance in the employment context, per by the Gibraltar General Data Protection Regulation **(the "Gibraltar GDPR")** and the Data Protection Act 2004 **(the "DPA").**

Guidance on the general obligations of the employer in the field of data protection is provided, as well as guidance on specific areas that may be relevant within the employment context. This includes, **amongst other things**:

The obligations of the employer

- The Gibraltar GDPR lists **lawful bases** that organisations can rely on, depending on the 'category' of personal data concerned. **Consent can only be an appropriate lawful basis if individuals are offered control and a genuine choice.** Given the imbalance of power in the relationship between employer and employee, organisations should avoid relying on consent where possible, and to establish a different lawful basis for processing. If an employer wishes to rely on **Article 6(1)(f) of the Gibraltar GDPR** for the processing of an employee's personal data, the purpose of the processing must be legitimate, proportionate to the business needs and should be carried out in the least intrusive manner possible.

- Employers must be **transparent** about how they are using and safeguarding their employees' personal data and only process personal data that is *"**adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed."* They must be **able to demonstrate** how data protection law is observed. Employers must also implement appropriate **technical and organisational measures** at the workplace to guarantee that the personal data of their employees are protected.

- Where data sharing occurs, organisations should **comply with the Information Commissioner's Code of Practice on Data Sharing**.

Recruitment and selection

- **Advertising and applications:** Best practice recommendations are provided, including the need to ensure the company name appears in all recruitment advertisements and the need for the scope of information requested and gathered to be proportionate to what the employer is seeking.

- **Interview notes**: It may not be necessary for an employer to retain information relating to an interview if the applicant was not successful and an employment relationship was not formally initiated. Whilst personal data should not be kept for longer than is necessary, retaining interview notes for a limited period of time may help an employer protect itself from potential claims (e.g., concerns about discrimination).

- **Vetting:** Employers must be very clear as to what the objectives of any vetting process are and must only pursue avenues that are likely to further these objectives. Checks should be proportionate to the risks faced. General intelligence-gathering should be avoided.

- **Retention:** The onus is on the data controller to set retention periods in respect of recruitment records. Importantly, the personal data must not be kept for longer than is

necessary, in accordance with Article 5(1)(e) of the Gibraltar GDPR.

Employment records

- **Collecting and keeping general records:** Transparency is key. Employees should be made aware of the nature and source of any information stored about them, how it will be used, and who it will be disclosed to. It is good practice to ensure the employee understands what processing activities are being undertaken.

- **Sickness and injury:** Information about an employee's health is 'special category data' and therefore more sensitive in nature, requiring additional protection. Special category data can only be processed where a lawful basis is identified under Article 6 of the Gibraltar GDPR, and at least one further condition, as prescribed by Article 9 of the Gibraltar GDPR, is fulfilled. Article 9(2)(b) of the Gibraltar GDPR may be considered in this regard.

- **Disciplinary:** Several key points and actions an employer should properly consider include, amongst other things, that records used in the course of disciplinary proceedings must not be obtained by deception and should be accurate and sufficiently detailed to support any conclusions drawn from them.

Monitoring in the workplace

- **Lawful basis:** It is imperative that employers identify a lawful basis under Article 6 of the Gibraltar GDPR, and Article 9 of the Gibraltar GDPR where applicable, should they seek to undertake monitoring.

- **Bring your own device:** Having policies to protect work related personal data on a device owned by the individual must be implemented. Devices owned by the organisation but also used by individuals for personal matters, would benefit from a policy that ensures those sections of a device which are presumed to be only used for private use may not be accessed by the employer. Importantly, employers should implement methods by which their own data on the device is securely transferred between the device and their network.

- **Data Protection Impact Assessments:** A data protection impact assessment would allow employers to assess whether a monitoring arrangement is a proportionate response to the problem it seeks to address.

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). Whilst remote working can be a positive development, it also presents additional risks to the security of personal data. Employers will therefore need to consider the same kind of security measures for homeworking that would be used in normal circumstances.

Employees' individual rights

- It is imperative that employers ensure compliance with the rights of individuals as set out in Articles 13 to 22 of the Gibraltar GDPR. Employers should also consider whether any exemptions apply in particular circumstances. A flow-chart illustrating how best to respond to Subject Access Requests ("SARs") involving third-party data is also included, with the aim of assisting employers when faced with such requests.

CONTENTS

1. INTRODUCTION

In this guidance note, the Gibraltar Regulatory Authority as the Information Commissioner[1] provides detailed guidance to facilitate data protection compliance in the employment context, in accordance with the Gibraltar GDPR and the DPA.

Matters addressed include those relating to the legitimate expectations of workers that personal information about them will be handled properly, and those relating to the legitimate interests of employers in deciding how best, within the boundaries of data protection law, to run their organisations.

Data protection law is not limited to simply recognising an individual's right to the protection of their personal data but requires employers to uphold data protection rights and obligations in a compatible, administrative infrastructure, that allows adequate protection of such rights.

It is important for employers to be aware of matters that may arise, such as the conditions relating to an employee's right of access to their personal data, concerns about retention, employee monitoring, and record keeping even after termination of employment.

This guidance also places particular emphasis on the appropriate legal basis that applies to the processing of personal data in the employment context, as well as the imbalance of power between employers and employees, and the limits set on the processing of personal data in recruitment activities.

Notably, this guidance note is intended to serve as a reference document, to be consulted, when necessary. However, bearing in mind that data protection obligations will vary according to the size and nature of the business, not every aspect of this guidance note will be relevant to every organisation. It is therefore recommended that organisations consult the applicable legislative provisions when faced with a particular data protection concern and apply the same to their specific circumstances.

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

2. ACKNOWLEDGMENTS

Having referred to reports and other publications of several authoritative bodies and industry participants during the drafting of this document, the Information Commissioner hereby acknowledges that parts of this document reflect and incorporate the opinions of, or commentary provided by or in, the following:

1. UK Information Commissioner's Office

a. 'The Employment Practices Code,' November 2011
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

b. 'The Employment Practices Code – Supplementary Guidance,' June 2005
https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf

2. Agencia Española de Protección de Datos

a. 'La protección de datos en las relaciones laborales,' May 2021
https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

3. Article 29 Working Party (predecessor to the European Data Protection Board)

a. 'WP48: Opinion 8/2001 on the processing of personal data in the employment context,'
13 September 2001
https ://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

b. 'WP249: Opinion 2/2017 on data processing at work,' 23 June 2017
https ://ec.europa.eu/newsroom/article29/items/610169/enB

3. TERMINOLOGY

For the purposes of this guidance note, the following terms are defined in the context of employment.

'Employee(s)'

For the purposes of this guidance note, the term "employee" includes:

- applicants (successful and unsuccessful);
- former applicants (successful and unsuccessful);
- employees (current and former);
- agency staff (current and former);
- casual staff (current and former);
- contract staff (current and former);
- volunteers or work experience placements.

Essentially, the word "employee" does not intend to restrict the scope of the term merely to persons with an employment contract as recognised under applicable employment laws. The Information Commissioner acknowledges that new business models (e.g., freelancing) are based on different types of labour relationships, and therefore, this guidance note aims to cover all situations where there is an employment relationship, regardless of whether this relationship is based on a traditional employment contract.

'Processing'

Activities performed routinely in the employment context may involve the processing of personal data, sometimes of a sensitive nature[2]. The term 'processing'[3] includes the *"collection, recording, organisations, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure of destruction"* of personal data.

In the employment context, processing activities likely to take place may include, amongst other things -

(a) recording, disclosing, or storing details of an employee's salary and other financial details (e.g., bank account number, tax codes, social insurance contributions);

(b) e-mail correspondence concerning incidents involving one or more named employees which concern health and safety procedures;

(c) a supervisor's notebook containing information on an employee where there is an intention to put that information in the employee's personnel file;

[2] Examples may include application forms and work references, payroll and tax information, unpaid/special leave or sickness records, appraisal/assessment records, disciplinary matters, information relating to an accident at work etc.
[3] Article 4(2) of the Gibraltar GDPR.

(d) recording, disclosing, or storing information in an employee's personnel file saved on the organisation's database;

(e) recording, disclosing, or storing information in an employee's personnel file where some of the documents are filed behind sub dividers with headings, such as application details, leave records and performance reviews;

(f) the recording of annual leave charts or records of absences from work;

(g) recording, disclosing, or storing information in sets of completed application forms and interview notes for a particular vacancy.

Conversely, there may be other processing activities that are unlikely to fall within the scope of data protection law where individuals are not named **and** are not identifiable. For example –

(a) the use of a report on the comparative success of different recruitment campaigns where no details regarding individuals are held.

(b) the use of a report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals.

4. OBLIGATIONS OF THE EMPLOYER

Employers must be transparent about how they are using and safeguarding their employees' personal data, inside and outside the organisation. Employers are accountable for data processing activities and must be able to demonstrate how data protection law is observed in respect of all their personal data processing activities, including those relating to employees.

In the first instance, employers should keep an inventory of all the personal data held and consider the following -

(a) why they are holding it;

(b) how they obtained it;

(c) why it was originally gathered;

(d) how long they will retain it for;

(e) how secure is it, from a technical and organisational perspective, both in terms of encryption and accessibility;

(f) whether they ever share it with third parties, and if so, on what basis they might do so.

4.1 Lawful basis for processing personal data[4]

The processing of personal data must not take place on a "*just-in-case*" basis nor on the premise that the information "*could*" be useful in the future. Processing should be limited to what is strictly necessary to fulfil a particular purpose. Identifying the lawful basis that an employer may rely on to process personal data is a fundamental step in ensuring data protection compliance.

The Gibraltar GDPR lists the lawful bases that organisations can rely on depending on the 'category' of personal data concerned (i.e., whether the information is 'personal data', 'a special category of personal data' or 'data relating to criminal convictions and offences').

The lawful basis for the processing of personal data in the context of employment may include –

(a) the employee has given their consent to the processing[5] for one of more specific purposes (Article 6(1)(a) of the Gibraltar GDPR);

(b) processing is necessary to fulfil parts of an employee's contract (Article 6(1)(b) of the Gibraltar GDPR);

(c) the employer is complying with a legal obligation (Article 6(1)(c) of the Gibraltar GDPR);

[4] Please see the Information Commissioner's Guidance Note, (6) "Identifying the 'Lawful Basis'" available here: https://www.gra.gi/data-protection/guidance.

[5] See section 4.1(i) below.

(d) processing is necessary to comply with the employee's vital interests[6] (Article 6(1)(d) of the Gibraltar GDPR);

(e) processing is necessary for the performance of a task carried out in the public interest (Article 6(1)(e) of the Gibraltar GDPR);

(f) for the purposes of legitimate interests pursued by the employer or by a third party (Article 6(1)(f) of the Gibraltar GDPR).

Employers may rely on a different lawful basis for each category of personal data being processed but must ensure that they record the grounds on which they are processing each separate category of personal data. For example, if a company formalises an agreement in which the employee receives benefits for certain purchases, the employer may wish to rely on the employee's consent. However, the lawful basis for this processing may differ from the lawful basis relied upon in respect of compliance with other aspects of the employment contract.

With respect to the processing of special categories of personal data, employers must not only consider Article 6 of the Gibraltar GDPR but also Article 9 of the Gibraltar GDPR. Article 9(2) of the Gibraltar GDPR allows for such processing when, amongst other things, it is necessary for the fulfilment of obligations and the exercise of specific rights of the employee (e.g., in respect of disability allowances)[7].

When an organisation processes personal data relating to criminal convictions and offences, said processing must be lawful, fair and transparent and comply with all other principles and requirements of the DPA. Part 1, 2 and 3 of Schedule 1 of the DPA sets out the conditions for such processing.

(i) Overview of Consent as a Lawful Basis[8]

Whilst employees are almost never in a position to freely give, refuse or revoke consent, particularly given the dependency that results from the employer/employee relationship, in exceptional circumstances consent may be one of the lawful grounds for the processing of personal data in an employment context. For example, if the particular circumstances allow, explicit consent may be one of the lawful bases relied on to process special categories of personal data or personal data relating to criminal convictions and offences.

Importantly, for consent to be valid it must be '*freely given, specific, informed and unambiguous*'[9]. This means that the employee must be aware that they are consenting to having their personal data processed for the specific purpose(s) and should not be forced into giving consent.

For this reason, consent as a lawful basis for processing is problematic in an employment context given that "*there is a real or potential relevant prejudice that arises from not*

[6] For example, where medical history is disclosed to a hospital treating them after a serious road accident.
[7] Article 9(2)(b) of the Gibraltar GDPR.
[8] Please see the Information Commissioner's Guidance Note, (13) "Guidance on Consent" available here: https://www.gra.gi/data-protection/guidance.
[9] Article 4(11) of the Gibraltar GDPR.

consenting" if the *"consequence may be the loss of a job opportunity"*[10]. In such a case, consent would not be freely given and is therefore not valid.

Consent can only be an appropriate lawful basis if individuals are offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.

Silence, pre-ticked boxes, inactivity, or lack of complaint about the processing cannot be taken by the employer as consent, and importantly, an employee can withdraw consent at any time, and it must be as easy to withdraw consent as it is to give it.

(ii) Overview of Legitimate Interest(s) as a Lawful Basis[11]

If an employer wishes to rely on Article 6(1)(f) of the Gibraltar GDPR for the processing of an employee's personal data, the purpose of the processing must be legitimate. The processing must also be proportionate to the business needs and should be carried out in the least intrusive manner possible.

Notably, under Article 21 of the Gibraltar GDPR[12] employees have the right to object to processing of their personal data in certain circumstances, including where the employer is relying on Article 6(1)(f) of the Gibraltar GDPR with regards the processing. The chosen method with which the processing is to be undertaken must therefore ensure 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 employee[13].

4.2 Transparency Requirements

Employees have a right to know what information their employer is collecting about them (directly or from other sources) as well as the purposes of processing operations envisaged or carried out with the data, whether presently or in the future[14]. Employers should proactively provide employees with information when collecting and processing their personal data. Articles 13 and 14 of the Gibraltar GDPR provide a list of the information employers, as controllers, should provide to employees. The list includes items such as -

(a) what personal data will be collected, and the lawful basis being relied on;

(b) the period for which the personal data will be stored;

---

[10] Article 29 - Data Protection Working Party, 'WP48 Opinion8/2001 on the processing of personal data in the employment context.' - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf - (last accessed 16th December 2021)

[11]Please see the Information Commissioner's Guidance Note, (6) "Identifying the 'Lawful Basis'" available here: https://www.gra.gi/data-protection/guidance.

[12] See section 9.7 below.

[13] For an example of the balance that needs to be struck, see *Köpke v Germany*, [2010] ECHR 1725, 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.

[14] Article 13(1) of the Gibraltar GDPR.

(c) whether the personal data will be shared and/or transferred with/to a third party;

(d) the existence of automated decision-making, including profiling.

Organisations may adopt a layered approach to providing information, starting with basic information at the time data is collected (e.g., during the recruitment process) and followed by more detailed specific information once the individual has been recruited. The notice that organisations use to provide this information to individuals is commonly referred to as a 'Privacy Notice'[15], and in the first instance, this information may form part of or be annexed to the relevant employment contract. Employers may also for example publish the Privacy Notice on the company website, intranet or notice board. Importantly, the information provided must be concise, transparent, intelligible, and easily accessible. In addition, the information must be presented in clear and plain language[16].

Information does not have to be provided directly to an individual insofar as they already have it[17]. Notwithstanding, if an organisation intends to process personal data for a purpose other than that for which it was stated to have been collected, the new use must be brought to the attention of the respective individual(s) before the new processing takes place[18].

4.3 Principle of Data Minimisation

An employer should only process personal data that is *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"* in accordance with Article 5(1)(c) of the Gibraltar GDPR. Whilst the Gibraltar GDPR does not further define these terms, an employer's processing activities will depend on the specified purpose for collecting and using the personal data. The position may differ from one employee to another, so employers must be mindful of not processing excessive information about any of their employees.

Example

Internet misuse can be detected without the necessity of analysing website content. Furthermore, a blanket ban on communication for personal reasons may also be impractical as enforcement of such a measure may require a level of monitoring that is likely to be disproportionate. In this regard, prevention should be given much more weight than detection, as the interests of the employer are likely better served by preventing internet misuse through technical means than by detecting misuse.

Employers must not collect personal data on the premise that it might be useful in the future. However, employers may be able to hold information for a foreseeable event that may never occur **if** it can be justified.

[15] Please see the Information Commissioner's Guidance Note, (17) "Privacy Notices under the GDPR/DPA" available here: https://www.gra.gi/data-protection/guidance.
[16] Article 12(1) and Recital 58 of the Gibraltar GDPR.
[17] Article 13(4) and 14(5)(a) of the Gibraltar GDPR.
[18] Article 13(3) of the Gibraltar GDPR.

Example

An employer holds details of the blood groups of some of its employees. These employees perform hazardous work, and the information is needed in case of an accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency. If, however, the employer holds the blood groups of the rest of the workforce, such information is likely to be irrelevant and excessive if they do not engage in the same hazardous work.

If employers hold more data about their employees than is necessary for the purpose(s) identified, the processing is likely to be unlawful and a breach of the data minimisation principle.

4.4 Accountability

Article 5(2) of the Gibraltar GDPR states that *"[t]he controller shall be responsible for, and be able to demonstrate compliance with, [the principles relating to the processing of personal data as set out in Article 5(1) of the Gibraltar GDPR]"*.

Useful tools in demonstrating compliance are training, auditing and documenting processing activities, as well as implementing and regularly reviewing data protection policies.

Accountability in the workplace is essential, particularly given the nature and scope of the processing activities often surrounding personal data in this context. In terms of compliance, employers should be able to demonstrate, amongst other things, the following –

(a) what personal data is being processed;

(b) the purpose(s) for which, and method in which, the personal data is processed;

(c) the length of time for which employee data will be retained, along with reasonable justifications;

(d) documented processes and procedures to handle personal data and to tackle any data protection issues that may arise.

In addition to the above, establishing and maintaining a personal data inventory will enable employers to amend incorrect data or track third-party disclosures.

4.5 Implementing Optimal Security Measures[19]

Employers must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of their employees are protected, in accordance with Article 5(1)(f) and Article 32 of the Gibraltar GDPR.

[19] Please see the Information Commissioner's Guidance Note, (18) "Data Security" available here: https://www.gra.gi/data-protection/guidance.

Amongst other things, this includes having protection in place to prevent personal data from being accidentally or deliberately compromised. Personal data must for example remain safe from the curiosity of other employees or third parties. This may be achieved by using anonymisation and/or encryption, for example.

Importantly, data security must be appropriate to the processing risks and, whilst information security may sometimes focus on cybersecurity (the protection of networks and information systems from external attacks), it also covers matters such as physical and organisational security measures. In essence, employers must weigh up the organisation's size, nature of information processed, costs of implementation, and potential harm from security breaches as relevant factors when considering appropriate security measures[20].

To determine what security measures are appropriate, employers may be required to undertake a risk assessment, which will often involve defining the processing and its context, understanding and evaluating the impact of a potential data breach, and defining the threats at hand and their likelihood, before finally evaluating the risk. To assist, the Information Commissioner lists some of the measures an employer may consider adopting -

(a) **Organisational security measures** –

i. creating an asset register to actively manage all hardware and software;
ii. exploring risk management and undertaking risk assessments where necessary, including acting upon any outcomes as appropriate;
iii. identifying individuals responsible for adopting and implementing an information security policy;
iv. establishing and ensuring compliance with effective data retention policies;
v. outsourcing trustworthy providers and implementing appropriate contracts;
vi. using third-party audits to test and certify existing security measures;
vii. training staff and raising awareness of data security threats;
viii. implementing data breach management arrangements;
ix. establishing disciplinary measures for those who breach company policies;
x. improving physical security by identifying and securing restricted areas, implementing physical access controls, using secure storage for manual records, and securely disposing of records/equipment.

(b) **Technical security measures** –

i. access controls including the use of passwords/passphrases, multi-factor authentication, regularly reviewing access permissions, and recording logging and audit trails;
ii. introducing firewalls and the use of encryption;
iii. updating devices and software systems by, amongst other things, sourcing reputable and reliable virus and malicious software protection;
iv. actively manage the configuration of devices;
v. administer automatic locking/screen savers;
vi. adopting policies for the use of mobile devices and remote working, including limiting and/or controlling the use of removeable media;
vii. establishing backup and restoration arrangements;
viii. disabling autocomplete email function and using predetermined sharing folders to share data.

[20] Article 32(1) of the Gibraltar GDPR.

For further information, please see the Information Commissioner's Guidance Note, (18) "Data Security" available here: https://www.gra.gi/data-protection/guidance.

4.6 Data Sharing[21]

Employees must be informed about how their information is being used by their employers, including any disclosures. The term 'data sharing' includes the disclosure of data from one or more data controllers (e.g., employers) to a third party by way of the reciprocal exchange of data, the pooling of information and/or one-off disclosures in unexpected or emergency situations. Employers should distinguish between data sharing that is systematic and data sharing that is exceptional.

Recital 48 of the Gibraltar GDPR adds that *"Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected".*

Where data sharing occurs, organisations should comply with the Information Commissioner's Code of Practice on Data Sharing, which is available at www.gra.gi/data-protection/codes-of-practice.

4.7 Data Protection Officers ("DPO")[22]

As per Article 37 of the Gibraltar GDPR, some organisations must appoint a DPO. The conditions which determine when a DPO is required are outlined within the same provision.

A DPO will act as an intermediary between the employer and relevant stakeholders, such as data subjects (e.g., employees) and regulators.

When appointing a DPO, employers may either appoint an external DPO or name an employee as an internal DPO. With regards the latter, employers must ensure that an internal DPO is not subject to a conflict of interest due to for example having multiple roles (e.g. if the DPO also works in the IT Department, HR Department, or is part of senior management for example, where they would have to supervise themself). Regardless of which option is chosen, a DPO must provide expert knowledge on data protection law and on relevant considerations depending on the complexity of data processing and the size of the company.

In relation to a group of companies, Article 37(2) of the Gibraltar GDPR expressly provides that "*[a] group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment".*

[21] For further information, please refer to the Information Commissioner's 'Data Sharing Code of Practice' available here: www.gra.gi/data-protection/codes-of-practice

[22] Please see the Information Commissioner's Guidance Note, (3) "Data Protection Officers" available here: https://www.gra.gi/data-protection/guidance.

4.8 Privacy by Design and Default

'Data Protection by Design' and 'Data Protection by Default', are principles enshrined within Article 25 of the Gibraltar GDPR.

'Data Protection by Design' means that data privacy features and data privacy-enhancing technologies are embedded directly into the design of projects, which should be done at the earliest stage possible. 'Data Protection by Default' means that the user service settings must be automatically data protection-friendly and only the data which is necessary for each specific purpose of the processing should be gathered.

When an employer collects, stores or uses employee data, said processing may be exposed to risk. Employers should therefore, from the outset, minimise potential risks and effectively ensure compliance with the Gibraltar GDPR. Recital 75 of the Gibraltar GDPR outlines some of the intangible harms that an employer needs to consider when processing the data of employees, including amongst others:

(a) the potential risk of discrimination;

(b) the potential for identity theft or fraud;

(c) the potential financial loss that could occur as a result of a breach;

(d) the opportunity for reputational damage as a result of a breach;

(e) the potential loss of confidentiality; and/or

(f) any other significant economic or social disadvantage.

4.9 Reporting a Data Breach[23]

As required by Article 33 of the Gibraltar GDPR, where a data protection breach presents a risk to the data subject(s) concerned, the data controller must generally report the breach to the Information Commissioner within 72 hours of becoming aware of it. This also applies to employers where personal data pertaining to their employees is affected by a data breach.

Additionally, where a breach could result in a high risk to the affected employee(s), the employer must also inform the respective employee(s) without undue delay.

[23] Please see the Information Commissioner's Guidance Note, (8) "Guidance on Personal Data Breach Notification" available here: https://www.gra.gi/data-protection/guidance.

5. RECRUITMENT AND SELECTION

5.1. Advertising and Applications

Individuals providing personal information, even if only giving their name and email address, in response to a job advertisement, should be made fully aware of who they are giving their details to, before they submit said information. Below are a few best practice recommendations employers should be mindful of when advertising jobs, to ensure compliance with data protection law -

(a) ensure the company name appears in all recruitment advertisements and that it describes the purposes for which the employer may use the personal data, particularly in cases where it is not self-evident;

(b) recruitment agencies, used on behalf of an employer, should identify themselves and explain how personal data they receive will be used and disclosed. An advertisement placed by a recruitment agency need not show the identity of the employer on whose behalf it is recruiting, and the agency may pass on information to the employer provided that the applicant understands that their details will be shared;

(c) upon receiving identifiable particulars of applicants from a recruitment agency, it is good practice to inform the applicant as soon as practically possible that their information has been received. Additional information should not be sought from applicants unless it can be justified as being necessary to enable the recruitment decision to be made;

(d) the scope of the information requested and gathered must be proportionate to what the employer is seeking to achieve. For example, the extent and nature of information sought from an applicant for the post of Head of Security at a bank would be very different from that sought from an applicant for work in the bank's staff canteen;

(e) similarly, in terms of the application process, the same information should not necessarily be required from all prospective employees, and the same should instead be tailored to the job-role being advertised. For example, an applicant for a purely administrative job should not be required to provide details of their driver's licence, whereas an applicant for a delivery job may be required to.

Ultimately, data protection law does not prevent employers from recruiting staff effectively. What it does is help strike a balance between an employer's need for information and an applicant's right to respect for their privacy and private life.

5.2. Verifications

Applicants may not always give complete and accurate answers to the questions they are asked. Employers are justified in making reasonable efforts to check the accuracy of the information they are given. The verification process should however be open. Applicants should be informed of what information will be verified and how this will be done, particularly if external sources or third parties are used. In such cases, signed approval from the individual may be sought. Gathering information about an applicant covertly is unlikely to be justified.

If the information obtained following the verification process differs from that provided by the applicant, it should not simply be assumed that the information originally provided is incorrect or misleading. If necessary, further information should be sought and a reasoned decision taken as to where the truth lies. As part of this process, the applicant should be asked to provide an explanation or make representations, as appropriate, to ensure that the information held on file is accurate and thereby processed fairly.

5.3. Short-Listing

Employers should be consistent in the way personal data is used in the process of short-listing applicants for a particular position. If an automated system is used as the sole basis of short-listing, employers must inform applicants about this and make provisions to consider representations from applicants before making a final decision.

5.4. Interview Notes

Interviewing an applicant without taking any notes is rare. In most circumstances, the personal information that is recorded and retained following an interview can be justified as relevant to, and necessary for, the recruitment process itself. In this regard, it may not be necessary for an employer to retain information relating to an interview if the applicant was not successful and an employment relationship was not formally initiated.

Generally, interview notes are not intended to be viewed by anyone other than the interviewer and interview panel. However, employers should be mindful that said information may be requested by the individual by means of a SAR (see section 9.2 below). If the notes are either transferred to computer, form part of a filing system, or are intended to form part of a filing system[24], the information may need to be provided as part of a data subject's SAR.

Compliance with the data minimisation and storage limitation principles, as per Articles 5(1)(c) and 5(1)(e) of the Gibraltar GDPR respectively, should also be considered. Whilst personal data should not be kept for longer than is necessary, retaining interview notes for a limited period of time may help an employer protect itself from potential claims (e.g., concerns about discrimination).

5.5. Vetting

Employers must be very clear as to what the objectives of any vetting process are and must only pursue avenues that are likely to further these objectives. It is prudent for the employer to make it clear early in the recruitment process (e.g., within application forms) that vetting will take place and how it will be conducted.

Checks should be proportionate to the risks faced by an employer and be likely to reveal information that would have a significant bearing on the employment decision[25]. In such cases, it is less intrusive to obtain the relevant information directly from the applicant and then verify it, than it is to obtain information about the applicant directly from third parties. The former approach should be adopted wherever practicable.

[24] Article 2(1) of the Gibraltar GDPR.

[25] The risks are likely to involve aspects of the security of the employer or of others. For example, employing unsuitable individuals to work with children.

Vetting that consists of general intelligence-gathering should be avoided. Vetting usually involves an entity asking the Royal Gibraltar Police ("RGP") directly about an individual's background in relation to a specific role, where the RGP would respond with information it deems appropriate. Data protection law does not place an obligation on the RGP to make any disclosures. This is a matter for the RGP to determine in their capacity as the only local organisation allowed to have a complete register of criminal convictions. Organisations will need to identify a lawful basis to carry out vetting and obtain/process data relating to criminal convictions. The most suitable lawful basis is dependent on the circumstances of each case. See below example relating to a local hospital.

Example

A local hospital is hiring pediatricians for its Children's Ward and requires that applicants be adequately vetted to ensure that they are suitable to work with children. In this case, such vetting is likely to be justified and proportionate to the risks, namely the safety of the children. In this context, the Information Commissioner considers Article 10 of the Gibraltar GDPR and Schedule 1, Part 2, Paragraph 18 of the DPA to be relevant as the lawful basis for the processing.

However, the hospital should still have clear internal guidelines on the procedure and inform applicants at the earliest stage possible.

Organisations must implement suitable and specific measures to safeguard the personal data of individuals undergoing vetting. Some relevant measures include:

(a) Limitations on access to data relating to vetting;

(b) Strict time limits for the erasure of personal data and mechanisms to ensure that such time limits are observed;

(c) Targeted training for those involved in the processing of data relating to vetting;

(d) The appointment of a DPO where it is not mandatory under the Gibraltar GDPR; and,

(e) Logging mechanisms to permit the verification of whether and by whom the personal data relating to vetting have been consulted and/or erased.

Given that vetting involves the processing of data relating to criminal convictions, organisations should give particular consideration to Article 24 of the Gibraltar GDPR and whether an "appropriate policy document" is required by virtue of other DPA requirements (e.g., see Schedule 1, Paragraphs 5, 38, 39 and 40 of the DPA).

It is the Information Commissioner's view that where vetting takes place, a data protection policy for vetting should be documented and regularly reviewed and updated where necessary.

5.6. Retention of Recruitment Records

The onus is on the data controller to set retention periods in respect of recruitment records. Importantly, the personal data must not be kept for longer than is necessary, in accordance with Article 5(1)(e) of the Gibraltar GDPR.

Employers should also consider the possibility that some business needs might be satisfied by using anonymised rather than identifiable records. Furthermore, some of the information gathered during the recruitment process may not be relevant to the employment situation. Employers should only retain personal data that has on-going relevance or is needed as evidence of the recruitment process. In this regard, it may be beneficial for employers to design application forms to facilitate the easy deletion of information which is irrelevant to the on-going employment relationship.

Employers should also ensure that application forms or supplementary information collated from unsuccessful applicants are securely destroyed, if applicable. If it is common business practice to keep the names of unsuccessful applicants on file, it is important that this is communicated to them and that they are afforded the opportunity to have their details deleted.

6. EMPLOYMENT RECORDS

6.1. Collecting and Keeping General Records

Transparency is again key in this regard. Employees should be made aware of the nature and source of any information stored about them, how it will be used, and who it will be disclosed to. Whilst it is not generally necessary to seek an employee's consent to keep employment records, it is good practice to ensure the employee understands what processing activities are being undertaken.

In accordance with Article 5 of the Gibraltar GDPR, employers should consider the following -

(a) care must be taken not to use information for secondary purposes unless it is clearly lawful;

(b) they must be sure to have adequate information on which to make a judgement or decision;

(c) any personal data, including medical reports or absence management procedure records must not be kept for longer than necessary. The employer should have systems, policies and procedures in place to determine how long the data should be retained and when specific information should be destroyed;

(d) accuracy of personal data must be ensured, including giving employees the chance to challenge any alleged inaccuracy;

(e) personal data should be kept secure by restricting access, being careful how it is transferred (e.g., not scanning and emailing notes with no password or printing to open printers), sharing only on a need-to-know basis, and being particularly careful when travelling or remote working;

(f) appropriate measures should be in place for international transfers[26];

(g) agreements that meet the requirements of Article 28 of the Gibraltar GDPR should be in place with data processors (e.g., if payroll is outsourced etc.)[27];

(h) where they meet the relevant threshold, data breaches must be reported to the Information Commissioner under Article 33 of the Gibraltar GDPR.

[26]Please see the Information Commissioner's Guidance Note, (11) "International Transfers" available here: https://www.gra.gi/data-protection/guidance.

[27] Please see the Information Commissioner's Guidance Note, (24) "Guidance on the Concepts of Data Controller and Data Processor" available here: https://www.gra.gi/data-protection/guidance.

Example

An employer outsources payroll services to a firm of accountants. Amongst other things, the employer must make relevant checks before-hand, and ensure the processor has provided sufficient guarantees that they will have measures in place to comply with data protection requirements. The employer must also ensure that there is a contract in place governing such processing.

6.2. Sickness and Injury Records

Information about an employee's health is 'special category data'. This is personal data that the Gibraltar GDPR considers to be more sensitive in nature, and so, requires additional protection. Special category data can only be processed where a lawful basis is identified under Article 6 of the Gibraltar GDPR, and at least one further condition, as prescribed by Article 9 of the Gibraltar GDPR, is fulfilled.

Employers may think about relying on the consent of employees if they are processing special category data[28]. Given the imbalance in the relationship between employer and employee, organisations are however advised to avoid relying on consent where possible, and to establish a different lawful basis for processing. For example, Article 9(2)(b) of the Gibraltar GDPR, allows organisations to process such data when it is "*necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Gibraltar law…*". This may be applied in various circumstances, (e.g., the processing is necessary to enable the employer to meet the requirements imposed on them by law in relation to statutory sick pay).

With computer-based systems becoming increasingly popular, the separation of sickness and injury records from other personal data can be achieved. Although the precise content of an employee's medical file may vary according to the case, guarantees must nevertheless be in place to ensure data quality. This could take the form of a general recommendation to the employer's staff handling such data, reminding them of their general obligations, and ensuring that special category data is afforded a higher-level of protection. This may be achieved by for example restricting access (i.e., make available on a "need-to-know" basis) and adopting additional technical and organisational security measures (e.g., password protection, encryption), as appropriate.

Example

An employer offers a private medical insurance scheme. Only in exceptional circumstances should it be necessary for the employer to have access to medical information about any employee or others included in the cover. In general, medical information should be kept in confidence by those responsible for providing the healthcare. It should normally be sufficient for the employer to simply be provided with information relating to the financial or administrative aspects of said scheme.

[28] Refer to section 4.1(i) above for additional information on consent.

6.3. Disciplinaries, Grievances and Dismissals

The activity of disciplining or dismissing employees, or the handling of their grievances, will often involve the processing of personal information, for example in the consultation of records or the compilation of dossiers of information about those involved. There are several key points and possible actions an employer should properly consider in this regard, as follows –

(a) the right of access of relevant employees to their data generally applies[29]. However, access rights may be subject to an exemption under the DPA (see section 9.2 below);

(b) personal data to be used in disciplinary proceedings must not be obtained by deception;

(c) records used in the course of disciplinary and grievance proceedings must be accurate and sufficiently detailed to support any conclusions that are drawn from them;

(d) records relating to disciplinary and grievance proceedings must be securely stored. Employers should be particularly careful that such records are only made available to those whose duties require them to have access to a particular record;

(e) records of allegations about employees that have been investigated and found to be without substance should not normally be retained once an investigation has been completed. However, there may be some exceptions to this[30].

In any case, employee information should not be used in a way that is incompatible with the purpose(s) for which the information was obtained at the outset. Where the processing of employee information in disciplinary and grievance proceedings is not compatible with the original purposes of for which said data was collected, the further processing must be fair. Any unfairness would breach Article 5(1)(a) of the Gibraltar GDPR.

Further, information relating to disciplinary and grievance proceedings may 'expire' after a set period of time. Retention in this regard should be set out in an employer's policy which outlines clear procedures about data processing and retention with regards the organisation's disciplinary and grievance proceedings. During any applicable retention period, employers must not use, or allow the relevant data to be used, beyond the purpose for which it was retained.

6.4. Retention and Termination of Employment

Retention, otherwise referred to in data protection law as storage limitation, is one of the fundamental principles enshrined in the Gibraltar GDPR. It is rarely appropriate to have a 'one size fits all' storage limitation rule covering the entire contents of an employee file. What to keep, how to store it, and for how long, is heavily dependent on multiple factors, some of which are predetermined by statutory obligations (e.g., employment law). In simpler terms, information relating to your tax code may be kept for a number of years from the end of the tax year it relates to, but records relating to exposure to hazardous substances may be kept for much longer given that the damage linked to such exposure may take several years to become apparent.

[29] Article 15 of the Gibraltar GDPR.

[30] An employer may be required to keep a limited record that an allegation was received and investigated for its own protection. For example, where the allegation relates to abuse and the employee is employed to work with children or other vulnerable adults.

Although advisable to delete personal data at the end of the relevant retention period, deletion[31]/destruction of information may not always be possible. Employers should however ensure anonymisation of personal data when no longer needed as this will reduce the risk that it becomes irrelevant, excessive, inaccurate, or out of date. Anonymisation means that the personal data can be kept in a form which no longer permits identification of data subjects.

Example

An employer holds personal data relating to a former employee. The employer deletes most of the personal data following the employee's termination of employment. However, in line with their retention policy and local employment and tax legislation, the employer retains information relating to the employee's tax contributions, to comply with their statutory obligations. Upon the expiration of such obligations the employer deletes this data.

Good practice around storage limitation, with clear, regularly reviewed policies on retention periods and erasure, is likely to reduce the burden of dealing with queries about retention and individual requests for erasure. This will also help employers comply with the data minimisation and accuracy principles, which in turn, reduces the risk that the relevant employer will use such data in error – to the detriment of those concerned.

6.5. Outsourcing of Data Processing

Frequently, organisations do not process all the information they hold on employees themselves, but outsource certain processing activities to other organisations (e.g., specialist businesses which run payroll systems, sister companies which manage the centralised computer system on which group employee records are kept, or organisations providing a secure facility for the storage of archived manual records). Such organisations are 'data processors'[32].

Where an employer outsources a service to a data processor, the onus is on the employer to ensure that the data processor puts in place appropriate technical and organisational measures to comply with the Gibraltar GDPR. Such arrangement should be governed by a contract that complies with Article 28(3) of the Gibraltar GDPR. In deciding what the appropriate security measures are, account must be taken of the nature of the information being processed and the harm that might result from a security breach.

[31] The word "deletion" can mean different things in relation to electronic data and the Information Commissioner recognises that it may not always be possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, it is imperative that any information stored in the back-up system is also deleted.

[32] Please see the Information Commissioner's Guidance Note, (24) "Guidance on the Concepts of Data Controller and Data Processor" available here: https://www.gra.gi/data-protection/guidance.

7. MONITORING IN THE WORKPLACE

Modern technology enables employees to be tracked over time across workplaces and their homes through the processing of personal data by devices such as smartphones, desktops, tablets, and even vehicles. If there are no limits to said processing, and if it is not transparent, there is a high risk that the interests of employers in the improvement of efficiency and the protection of assets, may turn into unjustifiable and intrusive monitoring. A further risk comes from the "over-collection" of data in such systems (e.g., collection of Wi-Fi location data).

In the absence of an easily understandable and readily accessible workplace monitoring policy, employees may not be aware of the existence and consequences of any monitoring that is taking place, and may therefore be unable to exercise their data protection rights in respect of the same.

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 processing beyond the original purposes for data collection.

Example

Using systems that are legitimately installed to protect properties (e.g., CCTV systems) to then monitor the availability, performance and customer-friendliness of employees, would constitute illegitimate further processing.

The use of CCTV to monitor employees in the workplace can be particularly intrusive so any use should in any case be carefully considered and strictly controlled.

Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organise meetings and to communicate confidentially. 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, but the analysis of metadata about a person might also allow for the privacy-invasive monitoring of an individual's life and behavioural patterns.

It is essential that any use of personal data to monitor staff complies with data protection law. Prior to any such monitoring, it is imperative that employers identify a lawful basis under Article 6 of the Gibraltar GDPR, and Article 9 of the Gibraltar GDPR where also applicable.

It is a fundamental requirement of data protection law that employees be fully aware of any monitoring being carried out and the reasons why. Simply telling employees that their emails may be monitored may not be sufficient. Employees should be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained, how it will be used, and who, if anyone, it will be disclosed to. The necessary information can be provided in a staff handbook or in a dedicated, internal, documented policy/procedure and employees should be reminded periodically about said monitoring, including, where appropriate, any

significant changes made to existing arrangements, in particular to avoid "function creep"[33] from occurring.

Personal data should only be collected for specified, explicit and legitimate purposes, and only be used for such pre-determined purpose(s). Employers must also consider the proportionality of any processing, ensuring that it only occurs when necessary. Further, security measures should be in place to protect personal data processed, by for example strictly limiting access only to individuals who need it.

Importantly, if during the monitoring process information about employees is kept or collected, this information must be made available to a respective employee if a SAR is made, unless an exemption applies (see section 9.2 below).

7.1. 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 commonly known as "bring your own device" or BYOD.

Implementing BYOD effectively can lead to benefits for employees (e.g., increased flexibility). However, use of an employee's device will also be personal in nature (e.g., during evenings and weekends). BYOD practices must therefore be carefully managed. For example, having a policy to protect work related personal data on a device owned by the individual must be implemented. In contrast, devices owned by the organisation but also used by individuals for personal matters would benefit from a policy that ensures 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 not be accessed by the employer.

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.

Importantly, employers should implement methods by which their own data on the device is securely transferred between the device and their network. For example, a device may be configured to route all traffic through a VPN back into the corporate network, so as to offer a certain level of security. If such a measure is used, the employer should however also consider that software installed for the purposes of monitoring may pose a privacy risk during periods of personal usage by the employee. Devices that offer additional protections such as "sandboxing" data[34] (i.e., keeping data contained within a specific app) could also be used. Conversely, the

[33] "Function creep" occurs when information is used for a purpose that is not the original specified purpose. For example, a workplace may install a security system that requires employees to sign-in or sign-out of the workplace. The purpose of the security system is to prevent unauthorized access to a particular workplace. However, organizations may end up using this information about individual employees to track employee attendance. This concept ties in with the purpose limitation principle (Article 5(1)(b) of the Gibraltar GDPR).

[34] A key measure in network and web security strategies which provides additional layers of security. In essence, it is a flexible permissions tool that allows employers to grant filtered access to specific information. In terms of cybersecurity for example, a sandbox provides a safe environment for opening suspicious files or running untrusted programmes without affecting the devices they are on.

employer may 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.

7.2. Processing Operations Relating to Employee Activity

(i) Biometrics

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 and the use of biometric-enabled devices has become increasingly common.

Article 4(14) of the Gibraltar GDPR defines biometric data as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [i.e., fingerprint data]*".[35] Biometric data includes, for example, facial recognition, fingerprint verification, and voice recognition.

Whilst a lawful basis under Article 6(1) of the Gibraltar GDPR would be required for such processing to be lawful, Article 9(1) of the Gibraltar GDPR includes biometric data as a 'special category of personal data' and one of the conditions under Article 9(2) of the Gibraltar GDPR must therefore also be met for such processing to be lawful. This may for example include circumstances where the data subject has explicitly consented to the said processing (Article 9(2)(a) of the Gibraltar GDPR). Again, however, the threshold for valid consent is particularly difficult to obtain in an employment relationship where there is an inherent relation of subordination between the employer and its employee.

Biometric systems can form an important component of an employer's audit trail, but they also pose the risk of providing an invasive level of knowledge and control regarding the activities of the employee whilst in the workplace. Employers need to be very cautious about the legal requirements and risks that may arise from biometric monitoring. It is recommended that employers take the following steps if considering the implementation of such monitoring –

(a) alternative, less intrusive, measures that do not require the processing of biometric data should be explored, and where possible, implemented instead of biometric data processing;

(b) the lawfulness for the processing of biometric data needs to be carefully assessed in line with Article 6 and Article 9(2) of the Gibraltar GDPR;

(c) employers should consider the need to carry out a DPIA (see section 7.3) as biometric monitoring is likely to result in "high risks to the rights and freedoms of natural persons". Furthermore, pursuant to Article 35(3)(b) of the Gibraltar GDPR, the large-scale processing of special categories of personal data will, in any case, require a DPIA;

[35] UK Information Commissioner's Office, 'What is special category data?' - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4 - (last accessed 16th December 2021)

(d) compliance with other requirements of data protection law such as the Article 5 of the Gibraltar GDPR data protection principles, must be ensured throughout.

(ii) Video Monitoring and Surveillance Systems

Video monitoring and surveillance systems **("VMSS")** also present issues for employee privacy. The most relevant changes relating to VMSS in the employment context are –

(a) the capability to easily access VMSS data remotely (e.g., via a mobile device);

(b) the reduction in the camera(s) size(s) to allow covert monitoring;

(c) the increase in VMSS capabilities (e.g., high definition); and,

(d) the processing that can be performed by new video analytics, meaning that it may be possible for an employer to monitor the worker's facial expressions by automated means.

VMSS should only be used when it is not possible to use other means that have a lesser impact on privacy.

Employers carrying out monitoring via VMSS should make it clear to the employees that monitoring is taking place, including where and why it is being carried out. This could be done by ensuring that writing notices are provided to employees e.g. via email, and that in areas subject to monitoring, a prominent sign is displayed that identifies the organisation responsible for the monitoring, why it is being undertaken and who to contact should concerns arise. Simply telling employees that they may be monitored by VMSS from time to time is not sufficient.

(iii) Covert Employee Monitoring[36]

The more intrusive the monitoring, the more precise the information given to employees needs to be, including the location of cameras and/or microphones. By its nature, covert monitoring is carried out in a manner calculated to ensure that those subject to it are unaware that it is taking place. This will only be justified if openness and transparency would likely prejudice the prevention or detection of crime, equivalent malpractice or the apprehension or prosecution of offenders[37]. It is essential that the employer makes a considered and realistic assessment of whether such prejudice is likely.

(iv) Processing Operations Involving Vehicles

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

[36] Please see the Information Commissioner's Guidance Note, (14) "Guidance on the Use of CCTV" available here: https://www.gra.gi/data-protection/guidance.Whilst such guidance relates specifically to covert CCTV recordings, it remains applicable to all forms of covert monitoring.

[37] See judgement in *Lopez Ribalda and Others v. Spain [GC] – 1874/13 and 8567/13 (2019).*

(and, hence, the employee) collected by basic GPS tracking systems, but, depending on the technology, a wealth of other information including driving behaviour.
In the interest of transparency, employers must clearly inform employees if a tracking device has been installed in a company vehicle that they are driving, 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. This information could be displayed prominently in every car within eyesight of the driver for example.

An employer should investigate whether it is demonstrably necessary to monitor the exact locations of employees for a legitimate purpose and weigh that necessity against the fundamental rights and freedoms of the employees. In such cases where the necessity can be adequately justified, the legal basis for such a processing could be based on the legitimate interests of the employer[38] for example. It should however first be assessed whether the processing is necessary, and whether the actual implementation complies with the principle of data minimisation[39]. The employer should seek to use the least intrusive means of processing, and where possible, avoid continuous monitoring.

Where private use of a professional vehicle is allowed, in addition to informing individuals about the existence of tracking devices in an expressly transparent manner, the employer should consider offering an opt-out mechanism in certain circumstances. In principle, the employee 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 their own initiative, protect certain location data as private.

7.3. Data Protection Impact Assessments[40]

A data protection impact assessment ("DPIA") is a procedure designed to assist organisations in identifying and minimising the privacy risks of new projects or policies, and can be a helpful tool in identifying and justifying the benefits of processing operations such as employee monitoring.

In terms of employee monitoring, a DPIA would allow employers to assess whether a monitoring arrangement is a proportionate response to the problem it seeks to address. Whilst it is an important tool for accountability, the outcome, and overall advantages of a DPIA will vary depending on the particular circumstances of the case.

Example

A delivery company installs GPS equipment in vehicles which are privately owned by the company's employees. The system is installed to ensure that deliveries are done in a timely manner and that customers can track their items. The company believe this will greatly improve their service.

Whilst such a system may be in the legitimate interests of the delivery company, amongst other things, they should limit the use of the GPS equipment and data to when a vehicle is in service, and not when the employee is not undertaking active work, to ensure the least intrusion possible. Further, the delivery company should clearly inform their employees of

[38] Article 6(1)(f) of the Gibraltar GDPR.
[39] Article 5(1)(c) of the Gibraltar GDPR.
[40] Please see the Information Commissioner's Guidance Note, (4) "Data Protection Impact Assessments" available here: https://www.gra.gi/data-protection/guidance.

such processing of personal data before making the system live.

A DPIA involves –

(a) clearly identifying the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver;

(b) identifying any likely adverse impact of the monitoring arrangement;

(c) considering alternatives to monitoring or different ways in which it might be carried out; and

(d) taking into account the obligations that arise from monitoring.

8. 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). In general, and depending on the implementation, this may involve the employer issuing IT equipment or software which, once installed in an employees' home or on their own devices, enables them to have the same level of access to the employer's network, systems and resources as they would have if they were in the workplace.

Whilst remote working can be a positive development, it also presents additional risks to the security of personal data. Such risks include, for example, the loss of personal data on portable working devices, insecure Wi-Fi arrangements, and unauthorised access to work folders on an unprotected mobile device.

Employees that have remote access to the employer's infrastructure may not be bound by the physical security measures that may be in place at the employer's premises. However, 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. Employer's will therefore need to consider the same kinds of security measures[41] for homeworking that would be used in normal circumstances.

[41] Please see the Information Commissioner's Guidance Note, (18) "Data Security" and (22) "Video Conferencing" both available here: https://www.gra.gi/data-protection/guidance.

9. Employees' Individual Rights[42]

The rights of individuals under the Gibraltar GDPR apply to future, current and former employees, as data subjects. When processing employee personal data, it is imperative that employers ensure compliance with the principles of processing as set out within Article 5 of the Gibraltar GDPR, as well as the rights of individuals as set out in Articles 13 to 22 of the Gibraltar GDPR. Employers should also consider whether any exemptions apply in the particular circumstances[43].

9.1 Right to be Informed

(Article 13 and 14 of the Gibraltar GDPR)

The right to be informed covers the key transparency requirements of the Gibraltar GDPR. It aims to ensure that individuals are provided with clear and concise information about what data controllers do with their personal data and why.

9.2 Right of Access[44]

(Article 15 of the Gibraltar GDPR)

Individuals have a right to obtain information that organisations hold about them, exercised through a SAR. This is an important right, aimed at ensuring individuals have control over their information, and to enable them to be "*aware of and verify the lawfulness of processing*"[45].

An individual is only entitled to their own personal data and the right cannot be used to access information relating to other persons (unless the information is also about them or they are acting on the other person's behalf). An individual's right to obtain a copy of their personal data must however not adversely affect the rights and freedoms of others.

Please refer to Appendix 1 which shows how to deal with SARs when the identity of a third party might form part of the information to be disclosed to the employee making the request.

Notwithstanding the above, there are some exemptions that are particularly relevant to employment –

(a) information held for management forecasting (i.e., information about plans for promotion, transfer or redundancy) may be withheld to the extent to which access would be likely to prejudice conduct of the employer's business[46];

---

[42] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.

[43] Please see the Information Commissioner's Guidance Note, (21) "Guidance on Exemptions" available here: https://www.gra.gi/data-protection/guidance.

[44] Please see the Information Commissioner's Guidance Note, (15) "The Right of Access" available here: https://www.gra.gi/data-protection/guidance.

[45] Recital 63 of the Gibraltar GDPR.

(b) information consisting of records of the intentions of the employer in relation to negotiations with an employee may be withheld to the extent to which access would be likely to prejudice those negotiations[47];

(c) information that consists of a reference given or to be given in confidence by the employer for the education, training or employment of the employee, the appointment of the employee to any office, or the provision by the employer of any service may be withheld[48];

(d) certain information may be withheld if access would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders and/or the assessment or collection of any tax or duty or any other imposition of a similar nature[49].

9.3 Right of Rectification[50]

(Article 16 of the Gibraltar GDPR)

Individuals have the right to have inaccurate personal data rectified or incomplete personal data completed by their employer. This right is closely linked to the accuracy principle of the Gibraltar GDPR[51], and although an organisation may have already taken steps to ensure that the personal data was accurate when they obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

9.4 Right of Erasure[52]

(Article 17 of the Gibraltar GDPR)

Individuals have the right to have personal data erased. This right is also known as the 'right to be forgotten' and only applies in certain circumstances. In the employment context for example, the end of an employment relationship may necessitate the erasure of data, but only if no other legislative obligations apply that require retention. Additionally, if an exemption applies[53], an organisation can refuse to comply with an erasure request (wholly or partly). Importantly, not all exemptions apply in the same way, and the organisation should look at each exemption carefully to see how it applies to a particular request.

The right to request the removal or erasure of personal data may be applicable in circumstances where the personal data is no longer necessary, the individual objects to such processing, and/or the individual withdraws consent (where this was the lawful basis for processing). Not only will employers need to comply with such requests, but they will need to

---

[46] Schedule 2 Part 4 Paragraph 17 DPA.
[47] Schedule 2 Part 4 Paragraph 18 DPA.
[48] Schedule 2 Part 4 Paragraph 19 DPA.
[49] Schedule 2 Part 1 Paragraph 2(1) DPA.
[50] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.
[51] Article 5(1)(d) of the Gibraltar GDPR.
[52] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.
[53] Please see the Information Commissioner's Guidance Note, (21) "Guidance on Exemptions" available here: https://www.gra.gi/data-protection/guidance.

ensure that any third party with whom such employee data was shared, also deletes such data. Employers should however be aware of the circumstances in which such right does not apply.

9.5 Right to Restrict Processing[54]

(Article 18 of the Gibraltar GDPR)

Individuals have the right to restrict processing of their personal data in certain circumstances, which means that an individual can limit the way in which an organisation uses their data.

In most cases the employer will not be required to restrict an employee's personal data indefinitely but will need to have the restriction in place for a certain period of time depending on the circumstances. Employers must have processes in place that enable them to restrict the processing of personal data if required. Such restriction may be applied to a broad range of operations including collection, structuring, dissemination and erasure of data. Employers should therefore use methods of restriction that are appropriate for the type of processing they are carrying out[55].

If an employer has disclosed personal data to other data controllers, the organisation must contact each recipient and inform them of the restriction of the personal data, unless this proves impossible or involves disproportionate effort.

9.6 Right to Data Portability[56]

(Article 20 of the Gibraltar GDPR)

The right to data portability gives individuals the right to receive personal data they provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmit this data directly to another controller.

In the employment context, this may be applicable following a change of employment in such cases where an individual wishes to have their personal data transmitted from an old employer to a new employer.

9.7 Right to Object[57]

(Article 21 of the Gibraltar GDPR)

In certain circumstances, individuals have the right to object to the processing of their personal data. This effectively allows individuals to stop or prevent organisations from processing their personal data.

---

[54] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.

[55] Article 4(2) of the Gibraltar GDPR.

[56] Please see the Information Commissioner's Guidance Note, (5) "Data Portability" available here: https://www.gra.gi/data-protection/guidance.

[57] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.

An objection may be in relation to all the personal data an organisation holds about an individual or only to certain information relating to a specific aspect of their employment (e.g., it may only relate to a particular purpose for which the organisation is processing the data).

9.8 Rights related to Automated Decision-Making, including Profiling[58]

(Article 22 of the Gibraltar GDPR)

Automated individual decision-making is a decision made by automated means without any human involvement, and, although it does not have to involve profiling, it often will do.

Even in the employment context, organisations may obtain personal information about prospective or existing employees from a variety of different source (e.g., internet searches and social media presence) to make decisions about them, find something out about an individual's preferences, or possibly, to predict habits and/or behaviour.

Organisations can only carry out solely automated decision-making with legal or similarly significant effects if the decision is necessary for entering into or for the performance of a contract between an organisation and the individual, is authorised by law (e.g., for the purposes of preventing fraud or tax evasion), or is based on the individual's explicit consent.

[58] Please see the Information Commissioner's Guidance Note, (23) "Guidance on the Rights of Individuals Under the Gibraltar GDPR" available here: https://www.gra.gi/data-protection/guidance.

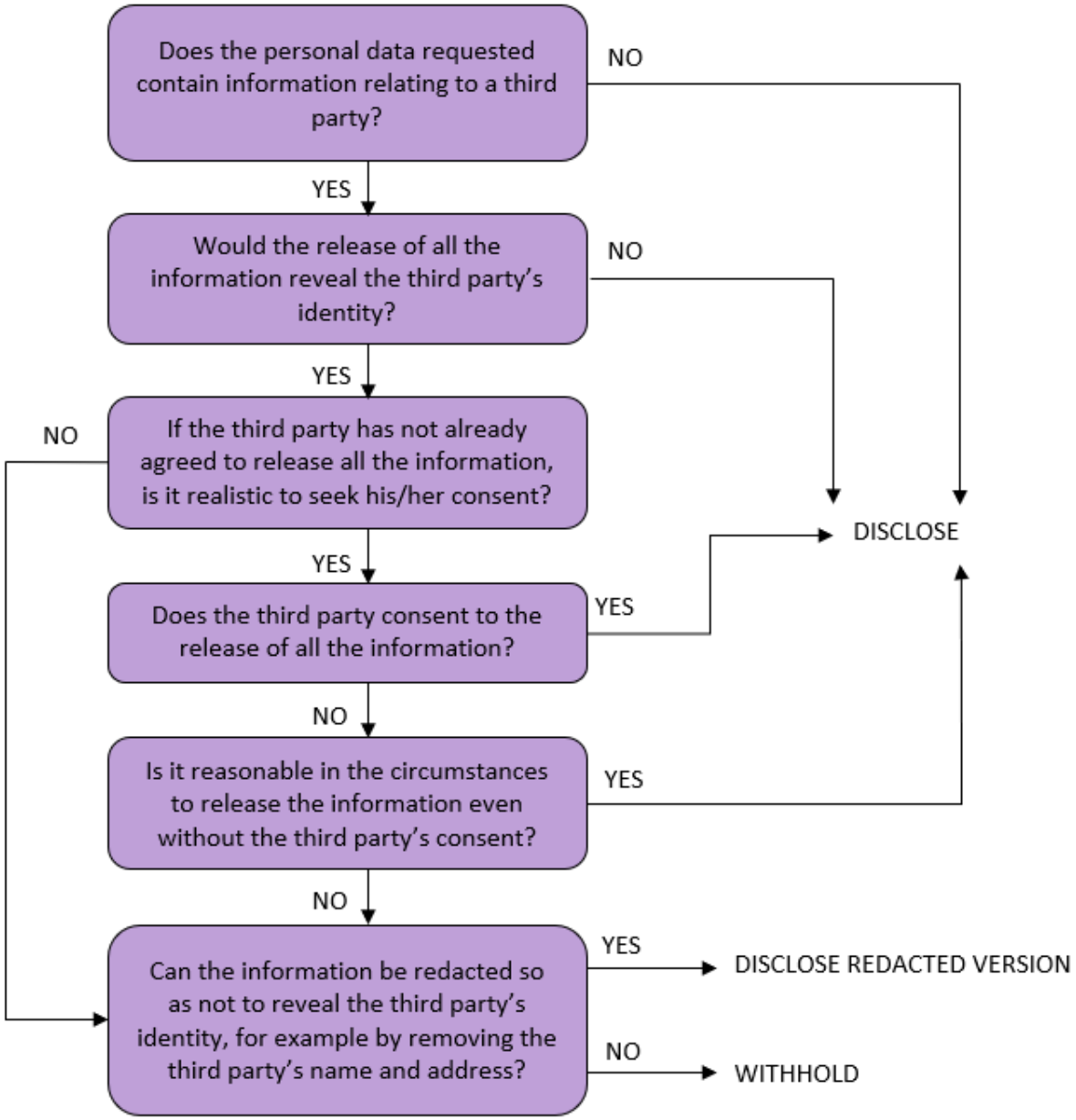
10. Appendix 1

The following diagram[59] explains how employers can deal with SARs when the identity of a third party might be revealed within the personal data being released to the employee making the request.

Ultimately, the employer must decide whether the balance weighs in favour of the employee's right to know what information is held about them or in favour of the right to privacy of the third party who can be identified through releasing the information. Factors to consider may include –

- whether it would take a disproportionate effort to edit or remove the part that reveals the identity of a third party without significantly changing its likely value to the employee;
- whether releasing the information would breach a duty of confidence owed by the employer to the third party;
- whether the third party has expressly refused consent to release of the information and the reasons given, if any;
- what the third party was told when the information was supplied about its possible release or, if told nothing, what the third party's reasonable expectations would be;
- the impact the information has had or might have in the future in respect of actions or decisions affecting the employee;
- whether the nature of the information, upon its release, could be damaging to the third party, or whether the same would reveal sensitive data about the third party;
- the extent to which the employee is already likely to be aware of the information;
- whether the information includes facts which the employee ought to be made aware of because he or she might dispute them;
- whether the information identifies the third party in a professional or personal capacity.

[59] UK Information Commissioner's Office, 'The Employment Practices Code - Supplementary Guidance' - https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf - (last accessed 16th December 2021)


Does the personal data requested contain information relating to a third party?
NO
YES
Would the release of all the information reveal the third party's identity?
NO
YES
If the third party has not already agreed to release all the information, is it realistic to seek his/her consent?
NO
YES
DISCLOSE
Does the third party consent to the release of all the information?
YES
NO
Is it reasonable in the circumstances to release the information even without the third party's consent?
YES
NO
Can the information be redacted so as not to reveal the third party's identity, for example by removing the third party's name and address?
YES
DISCLOSE REDACTED VERSION
NO
WITHHOLD

IMPORTANT NOTE

The document is purely for guidance purposes and does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the Gibraltar GDPR and the DPA will apply directly to them. The responsibility to become familiar with the Gibraltar GDPR and the DPA and comply with their provisions lies with the organisation.

Where necessary, the Information Commissioner will review this guidance note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this guidance note and the Gibraltar GDPR and/or the DPA, the Gibraltar GDPR and/or the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi