GRA

GIBRALTAR REGULATORY AUTHORITY

(18) Guidance on Data Security

Guidance on the EU General Data Protection Regulation 2016/679 & Data Protection Act 2004

19th March 2020

Guidance Note IR07/19

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, the DPA and the GDPR must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased obligations that the GDPR and DPA place on organisations. The Information Commissioner's aim is to alleviate some of the concerns for businesses, public-sector and third-sector organisations and assist them ensure data protection compliance.

SUMMARY

- As electronic storage and processing becomes increasingly inexpensive and more accessible, larger amounts of information are being held and processed. This increase in personal data processing, particularly in the online environment, has given rise to new data security challenges, which pose a threat to individuals as well as organisations and society.

- The EU General Data Protection Regulation 2016/679 and the Data Protection Act 2004 require organisations to ensure the "appropriate security" of personal data. What is appropriate depends on the circumstances of the organisation and the data being processed (in particular, consideration should be given to the risks of the processing). The law is thereby flexible to accommodate different types of organisations but clear in that appropriate security measures must be implemented. Ultimately, each organisation is accountable for establishing security measures that are appropriate for their circumstances. In this regard, an evaluation of risks with regards the processing of personal data is important.

- In regard to the notion of risk, specific data protection parameters need to be considered for its assessment, in particular the nature, scope, context and purposes of the processing. Moreover, data protection law clearly relates the risk to the measures taken in order to preserve the rights and freedoms of individuals. The impact of a potential personal data breach to the data subjects is a key aspect of the risk assessment.

- To determine what security measures are appropriate you will need to carry out a risk assessment, which will involve defining the processing and its context, understanding and evaluating the impact of a breach, defining the threats and their likelihood and finally evaluating the risk.

- Security measures that you should consider implementing, as appropriate:

    - <u>Organisational measures</u>
        - Create an asset register to actively manage all hardware and software
        - Risk management – undertaking risk assessments
        - Identifying individuals responsible for, and adopting, an information security policy
        - Effective data retention policies
        - Outsourcing - use trustworthy providers and implement appropriate contracts
        - Use third-party audits to test and certify your security
        - Training staff and raise awareness of data security threats
        - Implement data breach management arrangements
        - Disciplinary measures for those who breach the policies

    - <u>Technical measures:</u>
        - Access controls
            - Use passwords/passphrases

        - Multi-factor authentication
        - Minimise access to data
        - Regularly review access permissions
        - Logging and audit trails
    - Firewalls
    - Encryption
    - Keep devices and software up to date
    - Virus and malicious software protection
    - Actively manage the configuration of devices to ensure security
    - Automatic locking/screen saver
    - Use secure configuration
    - Adopt a policy for the use of mobile devices and remote working
    - Adopt a policy to limit and/or control the use of removeable media
    - Backup and restoration arrangements
    - Manage the security and use of wireless networks
    - Disable autocomplete email function and use predetermined sharing folders to share data
    - Physical security
        - Identify and secure restricted areas
        - Implement physical access controls
        - Use secure storage for manual records
        - Setup computer screens to mitigate against the risk of unauthorised access to data
        - Secure disposal of records/equipment

CONTENTS

1. ACKNOWLEDGEMENTS 1
2. INTRODUCTION 2
3. THE LAW 3
4. RISK BASED APPROACH 6
   4.1. Risk assessment 7
      4.1.1. Define the processing and its context 7
      4.1.2. Understand and evaluate the impact 7
      4.1.3. Definition of threats and their likelihood 10
      4.1.4. Evaluate the risk 12
   4.2. Technology and costs 13
5. SECURITY MEASURES 14
   5.1. ORGANISATIONAL MEASURES 14
      5.1.1. Asset management 14
      5.1.2. Information security policy 14
      5.1.3. Data collection and retention policies 15
      5.1.4. Outsourcing 15
      5.1.5. Third-party audits/certification 16
      5.1.6. Training and awareness 16
      5.1.7. Data breach management 17
      5.1.8. Disciplinary measures 17
   5.2. TECHNICAL MEASURES 18
      5.2.1. Access controls 18
      5.2.2. Firewalls 20

5.2.3. Encryption 20
5.2.4. Keep your devices and software up to date (patch management) ... 21
5.2.5. Protecting your systems from viruses and malicious software 21
5.2.6. Secure configuration 22
5.2.7. Automatic locking/screen saver 22
5.2.8. Mobile devices and remote working 22
5.2.9. Removeable media 24
5.2.10. Backup and restoration 24
5.2.11. Wireless networks 24
5.2.12. Disable autocomplete & use shared folders 25
5.2.13. Physical security 25
Annex A - Threats 27
Annex B – Threats and likelihood assessment questions 30

1. ACKNOWLEDGEMENTS

Where appropriate Gibraltar's Information Commissioner (the "Commissioner") will seek to ensure that locally published guidance notes are consistent with those published by fellow Information Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from both the UK and Irish Data Protection Authorities. Guidelines issued by the European Union Agency for Cybersecurity is also incorporated. Other sources were also used. The following outlines key documents used in the production of this Guidance Note:

(a) European Union Agency for Cybersecurity

'Guidelines for SMEs on the security of personal data processing', December 2016 https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

(b) The UK's Information Commissioner's Office

'Information Security Checklist'
https://ico.org.uk/for-organisations/data-protection-self-assessment/information-security-checklist/

(c) Ireland's Data Protection Commission

'Data Security Guidance'
https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance

(d) The UK's National Cyber Security Centre

'10 steps to cyber security'
https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/home-and-mobile-working

'Cyber Essentials'
https://www.cyberessentials.ncsc.gov.uk/advice/

2. INTRODUCTION

As electronic storage and processing becomes increasingly inexpensive and more accessible, larger amounts of information are being held and processed.

This increase in personal data processing, particularly in the online environment, has given rise to new data security challenges, which pose a threat to individuals as well as organisations and society. Examples of high-profile data security breach related cases are British Airways and the Marriott chain of hotels.

It is important to note that data security is important for all, not just big organisations, and that it concerns manual records as well as electronic records. The General Data Protection Regulation 2016/679 ("GDPR") and the Data Protection Act 2004 (the "DPA") require organisations to ensure the "appropriate security" of personal data. What is appropriate depends on the circumstances of the organisation and the data being processed. The law is flexible to accommodate different types of organisations but clear in that appropriate security measures must be implemented.

Data security covers a broad range of aspects including, for example, the need to restrict access to data on a need to know basis; staff training; using third-party processors who have appropriate security measures; physical security; and cyber-security related measures.

To determine what security measures are appropriate, you will need to carry out a risk assessment. This guidance note includes a risk assessment methodology that you may use, followed by a list of organisational and technical security measures that you should consider implementing, as appropriate.

Note that dependent on your circumstances there may be security aspects, not referred to in this document[1], that may be relevant to the security of your processing of personal data. In the same way, the relevance of the guidance in this document will differ depending on the organisation and its data processing.

Ultimately, each organisation is accountable for establishing security measures that are appropriate for their circumstances, and can only do this by evaluating the risks involved in their own processing of personal data.

[1] For example, this includes but is not limited to the Communications (Personal Data and Privacy) Regulations 2006

3. THE LAW

(a) The principle of integrity and confidentiality - Article 5(1)(f) of the GDPR and section 49 of the DPA

Article 5(1)(f) of the GDPR deals with the principle of *"integrity and confidentiality"* i.e. security, noting that personal data should be:

> *"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".*

We refer to this as the GDPR's 'security principle'. It concerns the broad concept of information security.

This is also a key principle in law enforcement processing and we set out in this note the DPA provisions which are relevant to law enforcement processing, including section 49[2].

(b) Appropriate technical and organisational measures – Article 32 of the GDPR and section 75 of the DPA

When implementing security measures, it is important to note that the GDPR and DPA refer to the need for "technical" or "organisational" measures. Therefore, it is important that organisations give due consideration to organisational measures, such as training and awareness, as well technical measures.

You need to consider the security principle alongside Article 32 of the GDPR, which provides more specifics on the security of your processing.

Article 32(1) reads as follows –

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

[2] **Section 49 of the DPA** (relevant to law enforcement processing) reads as follows –
"The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)".

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".

When we deal with law enforcement processing, the relevant provisions are found at section 75 of the DPA.[3]

Importantly, rather than imposing specific measures on an organisation, the GDPR and DPA allow flexibility as to what measures are to be taken. Although organisations have a legal obligation to keep personal data secure, how organisations achieve this depends on their particular circumstances.

Furthermore, it is important to recognise that some sectors may have security requirements that are specific to that sector e.g. adherence to a particular standard. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators or legislation. Although following these requirements will not necessarily equate to compliance with data protection law, the Commissioner will give these appropriate consideration.

An example of such special standards applies if you are processing payment card data, where you are obliged to comply with the Payment Card Industry Data Security Standard. The PCI-DSS outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the Commissioner will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

(c) Obligations of the controller – Article 24 of the GDPR

Further, Article 24 of the GDPR emphasises the accountability of the controller. It provides that you must implement technical and organisational measures to ensure, and be able to demonstrate, compliance with the GDPR. The measures should be risk-based, proportionate and must be reviewed and updated as necessary. For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The

[3] **Section 75 of the DPA** reads as follows –
"(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.
(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to-
(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it;
(b) ensure that it is possible to establish the precise details of any processing that takes place;
(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored; and
(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions".

GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you should take.

For law enforcement processing, the relevant provisions are found at section 65 of the DPA and mirror the requirements of the GDPR.

(d) Data protection by 'design and default' – Article 25 of the GDPR

Privacy by design is a good practice approach when designing new products, processes and systems that use personal data. Under the heading 'data protection by design and by default', the GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in data protection impact assessments) demonstrates this.

For law enforcement processing, the relevant provisions relating to data protection by design and by default are found at section 66 of the DPA.

(e) Maintaining documentation – Article 30 of the GDPR

Under Article 30 of the GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a good way to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the GDPR such as making sure that the information you hold about people is accurate and secure.

For law enforcement processing, the relevant provisions relating to the records of processing of activities are found at section 70 of the DPA.

(f) Logging – section 71 of the DPA

Specific to the law enforcement context, it is important to note the requirements in section 71 of the DPA. If you operate automated processing systems (any IT database), you must keep logs for **at least** the following processing actions:

- Collection
- Alteration
- Consultation
- Disclosure (including transfers)
- Combination
- Erasure

Logging enables you to monitor systems for inappropriate access and/or disclosure of data, to verify the lawfulness of any processing, and to ensure the integrity and security of personal data.

4. RISK BASED APPROACH

The GDPR/DPA adopts a risk-based approach to security[4], recognising that there is no "one size fits all" solution to personal data security. The law is flexible but requires organisations to consider their circumstances and implement appropriate measures. The higher the risk (for the rights and freedoms of data subjects), the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).

In the following pages a risk assessment methodology is outlined, largely based on work done by the European Union Agency for Cybersecurity ("ENISA"), which the Commissioner considers useful[5]. Organisations are nevertheless free to adopt a different approach.

As described by ENISA, a risk is often expressed as a function of the likelihood that an adverse outcome (threat) occurs multiplied by the magnitude of the adverse outcome (impact) should it occur. The risk assessment starts with the identification of threats, followed by the determination of the relevant likelihood and the impact of each risk.

In regard to the notion of risk, specific data protection parameters need to be considered for its assessment, in particular the nature, scope, context and purposes of the processing. Moreover, data protection law clearly relates the risk to the measures taken in order to preserve the rights and freedoms of individuals. The impact of a potential personal data breach to the data subjects is a key aspect of the risk assessment.

(a) The notion of impact

The impacts should be considered with regard to the freedoms and rights of individuals. For example, identity theft or fraud, financial loss, physical or psychological harm, humiliation, damage to reputation or even threat to life. When performing such analysis, the scale (e.g. number of affected individuals) may not be relevant: the impact can be high even where it may bring severe adverse effects only to a single person.

(b) The likelihood and management of risk

Even if the likelihood of a particular risk is low, a decision to accept the risk will not necessarily be right when high impacts to particular individuals may occur (e.g. if it may cause them severe physical damage or threaten their life). In such a case, avoiding the risk is recommended either by re-evaluating the overall processing operation or introducing appropriate measures to mitigate or remove the risk.

[4] See Article 32 GDPR and recital 76 on risk assessment.

[5] Although focused on cyber security, the risk assessment is also relevant for paper records.

4.1. RISK ASSESSMENT

The following is a simplified process for a risk assessment split into four phases.

4.1.1. DEFINE THE PROCESSING AND ITS CONTEXT

In this step an organisation should identify the boundaries of its data processing (e.g. the data's collection, storage, use, transfer, disposal, etc.).

Subsequently, the following questions need to be answered:

What are the types of personal data processed? The types of personal data will give an initial indication of the potential risk level.

What is the purpose of the processing? Identifying the purpose of the processing helps understand the limits of the processing as well as the associated risks.

What are the means used for the processing of personal data? The processing of personal data might take place in an automated or non-automated way or both online or offline. An organisation may rely partially or fully on a third-party (e.g. cloud services). It is important, thus, to clearly understand the means of the processing, paying particular attention to the fact that these may change in the different phases of the processing (collection, storage, use, transfer, disposal of personal data, etc.).

Where does the processing of personal data take place? The location of the personal data is also an important factor, especially when the services of data processors are used and/or when data is processed in a third (non-EU) country when additional protection mechanisms should be in place.

Which are the categories of data subjects? Identifying the categories of data subjects (e.g. clients, customers, others) will help factor in risk as these may sometimes provide an indication of the potential risk level - for example, processing of personal data of children requires special attention.

Which are the recipients of the data? Identifying the recipients of data may be useful to identify additional risks.

Further to the above, this guidance developed by ENISA in regard to data breach assessments includes an "assessment table" (see page 9) to be used in assessing the "data processing context".

4.1.2. UNDERSTAND AND EVALUATE THE IMPACT

In this step, the organisation needs to evaluate the potential impact to the rights and freedoms of individuals that a security incident (related to the data processing system) might bring.

(a) Risk and impact

In this regard, recital 75 of the GDPR provides direction as to the relevant types of impact/risk. For example -

1. tangible, physical and material harms (including financial or economic loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality and other significant economic or social disadvantage); and

2. intangible and non-material harms (such as - detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions; chilling effect on freedom of speech, association, etc.; reputational harm; personal, family, workplace or social fear, embarrassment, apprehension or anxiety; unacceptable intrusion into private life; and discrimination or stigmatisation).

(b) Level of impact and evaluation

The following outlines four levels of impact correlated to the consequences of a data breach on an individual:

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

The evaluation of the impact can only be qualitative, taking into account the specificities of a particular data processing operation. To assist, a number of parameters that need to be carefully considered (and co-related) are outlined below:

1. **Type of personal data**: This parameter can, increase or decrease the level of impact, based on the criticality of the data. For example, when the data include medical files or information on political beliefs (or any other special category of, or sensitive, data under GDPR/DPA), the impact of a security breach can be severe for the individuals. However, the assessment cannot only be based on the distinction of data between 'simple data' and special categories of data. Personal data that do not fall under a special category can reveal very critical information about an individual (e.g. location, habits, financial information) and consequently bring disastrous effects on him/her in case of a breach.

2. **Criticality of the processing operation**: It is important to assess the overall criticality of the processing operation, beyond the particular types of data.

3. **Volume of the personal data processed**: This parameter relates to the quantity of personal data that is being processed for a single individual - the greater the volume, the higher the potential for adverse effects. Volume should be considered both in terms of time (e.g. same type of data over a certain period of time) and content (complementing data of the same type).

4. **Special characteristics of the data controller/processor**: This parameter relates to the field of operation and the business activities of the organisation, which may by nature be revealing additional information for a certain data set (thus, potentially affecting the level of impact). For example, the breach of confidentiality of a customers' list may be higher if this list comes from an online pharmacy than from a stationery shop.

5. **Special characteristics of the data subjects**: The impact could also increase in cases where the data subjects belong to a social group with particular needs (e.g. minors, public figures). For example, the processing of a list of telephone numbers becomes more critical if it concerns known Members of Parliament.

Following consideration of the relevant specificities, an organisation should proceed to evaluate impact in regard to[6] –

1. loss of confidentiality,
2. loss of integrity, and
3. loss of availability.

The following table and questions will be useful in the evaluation of the above.

NO	QUESTION	EVALUATION
I.1.	**Please reflect on the impact that an unauthorised disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of confidentiality:*** · A paper file or laptop containing personal data is lost during transit. · Equipment has been disposed without destruction of the personal data. · Personal data are wrongly sent to a number of unauthorised recipients. · Some customers could access other customers' accounts in an online service. · Personal data are published on an internet message board or P2P site. · A CD-ROM with customer data has been stolen from premises. · A wrongly configured website makes publicly accessible on the internet data from internal users.	☐ Low ☐ Medium ☐ High ☐ Very high
I.2.	**Please reflect on the impact that an unauthorised alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of integrity:*** · A record that is necessary for the provision of an online social service has been changed and the individual needs to ask for the service in an offline way.	☐ Low ☐ Medium ☐ High ☐ Very high

[6] Confidentiality, Integrity and Availability are widely recognised as the key factors in regard to information security

	· A record that is important for the accuracy of an individual's file in an online medical service has been changed.	
I.3.	**Please reflect on the impact that an unauthorised destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of availability:*** · A customer database is corrupted and some processing is required to bring the service online again. · A personnel file is lost and the individual needs to provide again some information to the company. · A file is lost/database corrupted and there is no back up of this information. · A critical service (e.g. online medical record) is down and cannot be immediately recovered.	☐ Low ☐ Medium ☐ High ☐ Very high

Following the aforementioned assessment, three different levels of impact (for loss of confidentiality, integrity and availability) will be obtained. The highest of these levels should be considered as the final result of the evaluation of the impact, relating to the overall processing of personal data.

4.1.3. DEFINITION OF THREATS AND THEIR LIKELIHOOD

This step involves an organisation identifying the **threats** related to its personal data processing activities and their **likelihood**.

(a) Threats

In regard to the identification of threats, **Annex A** includes a list of threats[7] that an organisation may find useful in this exercise. Further, **Annex B** includes questions for organisations to use to assess the threat level and their likelihood. The questions are split into the following four categories:

1. Network and technical resources (hardware and software). Network connections may introduce threats both from external sources, as well as internal sources. Hardware and software resources may also introduce threats, e.g. due to poor maintenance and configuration, as well as due to bugs and backdoors related to device and software development. Common threats associated to network and technical (hardware/software) resources include eavesdropping of communication channels, unauthorised access to databases, unavailability of provided services, failure of communication links, misuse/abnormal use of information systems, etc.

[7] The list derives largely from guidance published by the French Data Protection Authority CNIL with some additions made by the Commissioner's office.

2. Processes/procedures related to the data processing operation. In many cases security threats arise from the lack of appropriate internal processes and procedures, mandating specific rules and practices within the organisation for the processing of personal data. Such threats include excessive access to data, access to the data by unauthorised persons, (un)intentional corruption of data, unauthorised modification/destruction of data, accidental disposal or loss of data processing equipment, etc.

3. Different parties and people involved in the processing operation. Security threats may also arise from those that perform the processing of personal data, i.e. the employees of the organisation involved directly in the processing, as well as other parties conducting part of the processing (data processors). Relevant threats include potential malicious internal attacks (e.g. with the support of specific employees), accidental misuse of personal data due to human mistake, unauthorised disclosure of data by external contractors, etc.

4. Business sector and scale of the processing. The business sector of an organisation, as well as the scale (volume) of the data processed, may also significantly affect the type and level of security threats. For example, if the type of personal data is considered a valuable asset and/or if the processing concerns the whole population of a country, attackers might be more interested in gaining access to these data.

It should be noted that although the aforementioned aims to cover a broad spectrum of both external and internal security threats, they cannot be considered as exhaustive but rather perceived as indicative of the practical evaluation of threats. Thereby additional factors might need to be taken into account by the organisation subject to their context.

Following the identification and evaluation of threats, the evaluation of the threat's likelihood can follow.

(b) Likelihood

Organisations may come up with their own way of classifying the likelihood of a threat. The following classification is used in this document:

1. Low: the threat is unlikely to materialise.
2. Medium: it is possible that the threat materialises.
3. High: the threat is likely to materialise.

Using the abovementioned classification (or other), the organisation should assess the likelihood of threats for each of the four different areas referred to above and detailed in **Annex B** i.e. network and technical resources, processes/procedures related to the processing of personal data, parties/people involved in the processing of personal data, business sector and scale of processing. The assessment should be as follows –

Number of positive replies in assessment area	Threat
0 - 1	Low
2 - 3	Medium
4 or above	High

Using the above assessment criteria, the following table should be completed to obtain a score for each assessment area (as mentioned in the foregoing, the questions and assessment are indicative).

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	Low	1
	Medium	2
	High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	Low	1
	Medium	2
	High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	Low	1
	Medium	2
	High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	Low	1
	Medium	2
	High	3

Having completed the table above, the final threat occurrence probability is calculated after summing up the four different scores obtained and associating the result with the following scale:

THREAT OCCURRENCE PROBABILITY SCALE	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	High

4.1.4. EVALUATE THE RISK

After evaluating the impact of the personal data processing operation and the relevant threat occurrence probability, the final evaluation of risk can be calculated as follows:

Threat occurrence probability x impact = **Risk level**

The following risk matrix may serve as a useful tool to determine the overall risk level for the data processing activity:

		IMPACT LEVEL		
		LOW	MEDIUM	HIGH/V HIGH
THREAT OCCURRENCE PROBABILITY	LOW			
	MEDIUM			
	HIGH/V HIGH			

Legend: Low risk | Medium risk | High risk

Independently of the final result of this exercise, the organisation may adjust the risk level obtained, where appropriate and justified to take account of specific characteristics relating to the data processing operation.

4.2. TECHNOLOGY AND COSTS

Further to the nature, scope, context and purposes of the processing as well as risk, Article 32 of the GDPR provides for the consideration of the state of the art and costs of implementation as factors to consider when determining the security measures that should be implemented. In this way, the law is flexible and adaptable to the circumstances of the processing, so that the security obligations are relevant and proportionate.

(a) The state of the art

To ensure the effectiveness of security measures, organisations should ensure that they are informed of updates in relation to the state of the art in respect to security measures, particularly those relevant to their data processing. This is important as threats to personal data evolve and previous security measures become obsolete.

(b) The costs of implementation

The law recognises that the costs of implementing particular security measures may in some cases be disproportionate and/or prohibitive. Latitude is thereby provided to organisations with limited financial means (depending on the data processing). The significance of this factor diminishes in value for organisations with considerable resources.

It is important to note that costs are not the determining factor.

5. SECURITY MEASURES

Having undertaken an assessment of the risks to the processing of personal data, you may proceed to select security measures that are appropriate to the risk associated with their data processing activities. Carrying out an information risk assessment as set out in the previous section is one example of an organisational measure, but you will need to take other measures as well. In effect, you should aim to build a culture of security awareness within your organisation.

This section identifies security measures that organisations should consider implementing, as appropriate. It is important to note that an exhaustive list of measures is not provided and that there may be other security measures that you should implement considering your particular circumstances.

In the following sections security measures are categorised into "organisational measures" and "technical measures".

5.1. ORGANISATIONAL MEASURES

5.1.1. ASSET MANAGEMENT

It is important that you actively manage all of the hardware and software you use. You should identify and document all office or home-based equipment, servers, and mobile devices that you are using to process or store personal data in an appropriate inventory or register. The asset register should also include information on whether the device is portable and/or a personal device. Similarly, you should also identify and document all systems and applications processing or storing personal data in an appropriate software register. The software register should include software license details, latest versions in deployment and details of all patches applied. For each of the identified assets, you should assign ownership of hardware or software processing or storing information.

You should identify, document and implement rules for the acceptable use of hardware or software processing or storing information. These inventories will assist you in creating device and application white lists for approved devices and software. Further, you should undertake periodic risk assessments of hardware and software asset inventories/registers and physical checks to ensure that the accuracy of the hardware asset inventory exercises.

5.1.2. INFORMATION SECURITY POLICY

It is good practice to identify a person or department in your business with day-to-day responsibility for developing, implementing and monitoring a documented security policy. They should have the necessary authority and resources to fulfil this responsibility effectively. For larger organisations, it is common to appoint 'owners' with day-to-day responsibility for the security and use of business systems.

An information security policy will enable you to address security risks in a consistent manner. The policy can be part of a general policy or a standalone policy statement that is supported by specific policies.

Your policy should clearly set out your approach to security together with responsibilities for implementing it and monitoring compliance.

You should have a process in place to ensure that you review and approve policies and procedures in place before implementing them and set regular review dates to ensure the policy stays up to date.

Without clear accountability for the security of systems and specific processes, your overall security will not be properly managed or coordinated and will quickly become flawed and out of date.

5.1.3. DATA COLLECTION AND RETENTION POLICIES

The most effective means of mitigating the risk of lost or stolen personal data is not to hold the data in the first place. Data retention and replication should always be assessed against business need and minimised, either by not collecting unnecessary data or by deleting data as soon as the need for it has passed. Holding any personal data presents security risks.

You should always know what data you hold, where it is held and how it flows through your organisation. Without this element of oversight, effective protection of personal data within the organisation is a difficult task.

5.1.4. OUTSOURCING

Small businesses may opt to outsource some or all their data processing requirements to hosted (including cloud based) services.

There must be a written contract between your organisation and the service provider/processor (or other legal act). These contracts must include certain specific terms, as a minimum, including security standards (see Article 28 of the GDPR and section 68 of the DPA). As a data controller, you are liable for overall compliance with the GDPR/DPA and for demonstrating that compliance. However, processors do have some direct responsibilities and liabilities of their own. You must be satisfied that any processors you use treat the personal data they process for you securely, in line with the requirements of the GDPR/DPA.

You must choose a third-party provider or processor that gives sufficient guarantees about its security measures. To make sure they have appropriate security arrangements in place, you might, for example, review copies of any security assessments and, where appropriate, visit their premises.

The contract with the processor must include a term requiring the processor either to delete or return (at your choice) all the personal data it has been processing for you. The contract must also ensure it deletes existing copies of the personal data unless its retention is required by law.

If you use a third-party service provider or processor to erase data and dispose of or recycle your ICT equipment, make sure they do it adequately. You will be held responsible if personal data collected by you is extracted from your old equipment if it is resold.

5.1.5. THIRD-PARTY AUDITS/CERTIFICATION

Certification can be a useful means of demonstrating compliance with security obligations, where certification indicates that data security controls have been subject to audit or review by a reputable third-party organisation, particularly if it is against a recognised standard.

5.1.6. TRAINING AND AWARENESS

Other than technical and physical controls to protect personal data, other measures are necessary to mitigate the human risk of information security. Human errors are always possible, whether as a result of external attackers targeting human weaknesses or innocent mistakes. To minimise human errors that can result in a data breach, organisational controls should be implemented such as training and awareness programs for employees.

Passwords should not be written down and left in convenient places; passwords should not be shared amongst colleagues; and unexpected email attachments should not be opened unless first screened by anti-malware software. Staff should be trained to recognise common threats such as phishing emails and malware infection, and how to recognise and report personal data breaches.

Staff should be briefed about their security responsibilities, including the appropriate use of business systems and ICT equipment. Effective employee training about risks of data breaches, their role in preventing it and how to respond in the event of a problem can be a very effective line of defence. Many organisations set security policies and procedures but fail to implement them consistently. Running scenario-based training sessions may assist in effective training.

Controls focused on individual and organisational accountability and ensuring that policies are carried out are an important part of any system designed to protect personal data. Identify essential controls first and ensure that these controls are implemented across the organisation without exception. Once this is in place, move on to more advanced controls designed to mitigate the risk specific to the organisation type(s) or data processed.

You must have procedures in place to manage staff turnover, including retrieval of data storage devices and quick removal of access permissions.

You must ensure that staff with specific security responsibilities or with privileged access to business systems are adequately trained and qualified.

You should schedule training to take place on or shortly after appointment with updates at regular intervals thereafter or when required. You should also reinforce training using other methods including intranet articles, circulars, team briefings and posters.

Well-designed security measures will not work if staff do not know about or follow business policies and procedures. You should make policies and procedures available to all staff using staff intranet pages, policy libraries or through leaflets and posters.

It is good practice to circulate new information or updates through bulletins or newsletters.

5.1.7. DATA BREACH MANAGEMENT

Whilst the risk of data breaches and loss may be mitigated by implementing appropriate security measures, it is important to recognise that there is always a risk of mistakes occurring. When a data breach occurs, it is important that these are dealt with effectively and efficiently, to minimise and remedy any damages or loss, and mitigate the risk of future occurrences.

The GDPR/DPA introduces a duty on all organisations to report certain types of personal data breaches to the Commissioner and, in some cases, to the individuals affected.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches may arise from a theft, an attack on your systems, the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure.

You should ensure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data. All members of staff should understand who they need to notify if they have lost control of personal data.

You should ensure that you have an internal data breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the Commissioner or affected individuals. The Commissioner has published guidance in regard to breach notification alongside a breach notification form which identifies all the information that needs to be provided in a notification.

Even where a breach does not need to be reported, you must document the breach including the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle and allows us to verify your organisation's compliance with its notification duties under the GDPR/DPA.

However, when a breach occurs it is important that you deal with it effectively and learn from it. You should have a process to investigate and implement recovery plans.

Ideally, your organisation should monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Data breaches may have significant detrimental effects on individuals. For example, they may result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Identifying and responding to data breaches is important to manage and mitigate their effect.

5.1.8. DISCIPLINARY MEASURES

A breach or loss of personal data may result in harm to individuals as well as an infringement of data protection legislation that may lead to enforcement action by the Commissioner.

As part of your arrangements to protect personal data, you should supplement security measures with disciplinary procedures to ensure that employees adhere to the organisation's information security policies.

For example, staff could be informed that unjustified access or other use (e.g. viewing, copying, disclosing) of the personal data is considered a disciplinary matter and that such instances may be reported to the Commissioner. In this respect, it may be useful to inform staff that in addition to your organisation, individuals can be personally liable for accessing or using personal data without consent.

5.2. TECHNICAL MEASURES

We often think of technical measures as relevant to the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security. These are some of the technical measures you can implement.

5.2.1. ACCESS CONTROLS

Access controls for electronic records will normally play an important role in your measures to ensure personal data in electronic records are only accessed by authorised individuals, when necessary, and prevent unauthorised and wrongful access.

Each system user should be assigned a unique "key" to ensure accountability e.g. username and password, and user permissions should be restricted to the absolute minimum required for each role. Greater access limitation should be adopted in respect of special categories of personal data.

The access allowed to users should be reviewed on a regular basis to ensure that they remain consistent with the responsibilities and requirements of the user.

(a) Passwords/passphrases

A measure which you should consider implementing is the use of unique identifiers (such as passwords, passphrases, smart cards etc.) for each user before they can access any personal data held. The use of shared credentials (multiple individuals using a single username and password) should be prohibited.

Strong passwords are strongly encouraged to ensure that they are effective. A strong password for example is one that possesses 10 or more characters and contains one or more of each of the following:

- Letters (upper and lower case)
- Symbols (e.g. @, #, [, % etc)
- Numbers (0-9)
- Punctuation (;, ?, !)

Passphrases are like passwords but serve as a sentence or sequence of words. It is recommended that they should include at least twenty characters, and much like passwords, include symbols, numbers and punctuation marks.

You need to ensure that users do not disclose their passwords or passphrases to anyone else under any circumstances, in order to keep the integrity of the mode of access authentication. Additionally, passwords should not be written down and kept in 'convenient places'.

Further to the strength of passwords, you should consider implementing rules relating to the frequency of password changes and limits related to the number of login attempts allowed. You should enforce password complexity and length and should also require a password to be changed if there is evidence it has been compromised.

A brute force attack is a common threat. Using strong passwords and limiting the number of failed login limits are particularly important to protect against this threat.

Further, you may look to implement monitoring of user activity to detect anomalous use as this is also important for password security.

(b) Multi-factor authentication

Multi-factor authentication ("MFA") means there is more than one identity factor employed for access authentication. A commonly used option is '2FA', which means that two factors for authentication are used. For example, instead of just using a password, a user may also need to enter a code which is sent to their email address/mobile number to gain access.

Devices such as smart cards or tokens, as well as standalone mobile apps, can also be used as part of MFA. They may generate a PIN number that is valid for a very short period and is used in conjunction with a username and password to authenticate the user and allow access.

(c) Minimise access to data and services

In order to minimise the potential damage that could be done if an account is misused or stolen, you should ensure that staff have the minimum access necessary to personal data, software, settings, online services and device connectivity, for them to carry out their role.

Administrator accounts can be used to check what privileges employee accounts have. Accounts with administrator privileges should only be used to carry out administrative tasks. That is to say that those with administrator privileges should ensure that they do not browse the internet or check emails when using an administrator account as you may increase the chance of an administrator account becoming compromised.

(d) Regular and ongoing management and review

The access allowed to users should be reviewed on a regular basis to ensure that they remain consistent with the responsibilities and requirements of the user.

Specific policies and procedures for circumstances sometimes referred to as "movers, leavers and joiners" should be considered to increase or restrict previous access where a user's role changes.

(e) Logging and audit trails

The implementation of mechanisms that log user activity is an important measure to identify inappropriate use of information by staff as well as external attacks. Where you process large volumes of data, in particular sensitive data, it is advisable that you introduce an alarm system that reports on suspicious or malicious activity on a computer or network. Alerts should be examined in a timely manner to ensure unauthorised activity is promptly identified and corrective action taken.

Without appropriate mechanisms to monitor use activity by assessing logs and audit trails, access controls can be undermined. Therefore, you should ensure that a system is able to identify the user that accessed a file and the time of the access. In addition, the system should log alterations made to a file, along with its author/editor.

Further, you should be transparent and should inform staff of logging and audit trails as well as any monitoring activity. In addition, notifying users of logging and audit trails is likely to deter staff abuse.

User access controls should be supported by periodic reviews of logs that document actual access to personal data, to ensure that all access to personal data is strictly necessary and justifiable for the performance of a function.

Particular care should be taken where IT administrator accounts are able to access all data in an unrestricted manner, and there should be policies in place to oversee activity in these accounts.

5.2.2. FIREWALLS

External attacks to a computer system or network are a threat to information security, as attackers can gain unauthorised access to personal data. You should therefore implement an appropriate firewall to protect the boundary between its computers and the internet.

The firewall creates a 'buffer zone' between your IT network and other, external networks. Within the 'buffer zone', any incoming traffic can be analysed and reviewed to establish whether or not it should be allowed to enter your network.

There are two types of firewall that you can implement; personal firewalls or dedicated boundary firewalls. A personal firewall can be used on an internet connected device such as a laptop. However, for larger organisations with multiple different devices connected to the internet, you might require a dedicated boundary firewall, which places a protective buffer around the network as a whole.

You may also mitigate threats by segmenting and limiting access to network components that contain personal data. For example, your web server should be separate from your main file server. If your website is compromised, the attacker will not have direct access to your central data store.

5.2.3. ENCRYPTION

Encryption is a mode of protection that encodes information so that only authorised individuals can access the data. It is considered a necessary precaution where personal data is stored on

a mobile device (e.g. USB, smartphone etc.) or transmitted over a public network. The person looking to open the encrypted document or device will require a password or code to access it. As with passwords generally, this form of security loses its integrity when the key to decrypt the data is not kept secure.

Encryption is particularly useful when data is transferred or communicated between individuals (e.g. via email) or stored in removable devices (e.g. USB flash drives). It does not prevent the information from being intercepted but prevents the data from being accessed unless the secret key or password is obtained. Further to the use of encryption when data is transferred or stored in removable devices, data stored in a computer can also be encrypted for additional security.

Further to the encryption of data when stored on a device, it is also important to encrypt data when it is being transmitted over the internet.

It is important to note that encryption is specifically listed in Article 32(1)(a) of the GDPR as a security measure that should be considered to protect personal data.

5.2.4. KEEP YOUR DEVICES AND SOFTWARE UP TO DATE (PATCH MANAGEMENT)

Regardless of the type of computers, laptops, tablets or smartphones that your organisation is using, it is important to ensure that they are kept up to date at all times. This includes operating systems, applications and software used.

Manufacturers and developers release regular updates which not only add new features to your software, but also fix any security vulnerabilities that may have been discovered.

You should ensure that you apply these updates (a process known as patching) in order to improve security. Operating systems, phones and applications should all be set to 'automatically update' whenever this option is available. This way your systems and devices will be protected as updates are released.

5.2.5. PROTECTING YOUR SYSTEMS FROM VIRUSES AND MALICIOUS SOFTWARE

You should consider the risks to your networks and systems should they not have adequate measures in place to minimise the likelihood of a virus or a malicious software attack. There are various ways that malware can find its way onto a computer system. A user might open an infected email attachment, open a malicious website, or use a removable storage device carrying malware without realising that what they are opening is infected.

There are a number of ways of minimising the risk of a virus or a malicious software attack. Anti-malware measures are often included for free with popular operating systems. These should be used on all computers and laptops. Smartphones and tablets should be kept up to date, password protected, and where possible, you should turn on the ability to track and erase any lost devices. Further, you should avoid connecting to any unknown Wi-Fi networks as this will help to keep your devices free of malware too.

Whitelisting can also be used to prevent users installing and running applications that may contain malware. Whitelisting involves an administrator creating a list of applications allowed on a device. If an application does not appear on the list, the user will not be allowed to install it onto their device.

Further, an administrator may look to use versions of applications that support the use of sandboxing. A sandboxed application is run in an isolated environment with very restricted access to the rest of your device and the network.

Any anti-virus software utilised should be updated regularly in order to ensure its efficiency and policies should be introduced to support vigilance regarding potential threats.

Further, you should look to adopt periodic testing to scan computer networks for any malicious software that could compromise the networks integrity.

It is also important that you carry out training and awareness to educate users about common threats that they might face.

5.2.6. SECURE CONFIGURATION

The default installation of ICT can include vulnerabilities such as unnecessary guest or administrator accounts, default passwords that are well known to attackers, and pre-installed but unnecessary software. These vulnerabilities can provide attackers with opportunities to gain unauthorised access to personal data held in business systems.

You should securely configure ICT equipment on installation to reduce information security vulnerabilities. Maintaining an inventory of ICT equipment will help you identify and remove unnecessary or unauthorised hardware or software.

5.2.7. AUTOMATIC LOCKING/SCREEN SAVER

You should ensure that computers are locked when unattended to minimise any unauthorised access to personal data. It is pointless to implement an access control system if unattended computers can be accessed by any member of staff.

If you haven't got an automated screen lock set up on a computer, it could be at risk of unauthorised access. Most operating systems allow an automatic screen lock after a period of inactivity on a computer, requiring a password to re-gain access. The automatic lock feature is useful as the only other alternative is the manual locking of a computer which requires a positive action by the user every time they leave their computer unattended. The auto-lock function should also be implemented on mobile devices.

5.2.8. MOBILE DEVICES AND REMOTE WORKING

Mobile working and remote system access provides flexibility and other benefits but also exposes personal data to risks that need to be managed.

Where mobile devices are used and/or remote working is allowed, you should establish appropriate risk-based policies and procedures that are applicable to users, as well as service providers. If you do not establish adequate mobile working and remote access practices, you might be vulnerable to the following risks:

1. Loss or theft of the device: Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.

2. Being overlooked: Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.

3. Tampering: An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

Consider the following measures to mitigate against the abovementioned risks –

1. Assess the risks and create a mobile working policy: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed.

2. Educate users and maintain awareness: All users should be trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate securely by following clear procedures. This should include direction on -
   a. secure storage and management of user credentials;
   b. incident reporting; and
   c. environmental awareness (the risks from being overlooked, etc.).

3. Apply the secure baseline build: Develop and apply a secure baseline build and configuration for all types of mobile device used by the organisation.

4. Protect data at rest: Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.

5. Protect data in transit: If the user is working remotely the connection back to the corporate network will probably use the Internet. All information exchanged should be appropriately encrypted.

6. Review the corporate incident management plans**:** Mobile working attracts significant risks and security incidents will occur even when users follow the security procedures. The incident management plans should be sufficiently flexible to deal with the range of security incidents that could occur, including the loss or compromise of a device. Ideally, technical processes should be in place to remotely disable a device that has been lost or at least deny it access to the corporate network.

5.2.9. REMOVEABLE MEDIA

Removable media such as CDs and USB drives are highly vulnerable to theft or loss. Removable media are also an easy way in which an employee may obtain information from you, without consent or authorisation.

If there is a business need to store personal data on removable media, you should implement a software solution that can set permissions or restrictions for individual devices as well as entire classes of devices.

You should implement documented policies and procedures to control or prohibit the use of removable media. Further, you should minimise and encrypt personal data in order to reduce information security vulnerabilities.

5.2.10. BACKUP AND RESTORATION

Implementing back-up policies and procedures are important to help restore personal data in the event of data loss as a result of equipment failure or other incident.

Regular back-ups should be made to help restore personal data in the event of disaster or hardware failure. While back up arrangements will differ depending on the sensitivity of the personal data, the extent and frequency of the back-ups should reflect the sensitivity and confidentiality of the personal data and how critical it is to your business being able to operate. Ideally you should keep backups in a secure location away from the business premises, and regularly test the restoration of personal data to check the effectiveness of the back-up process.

5.2.11. WIRELESS NETWORKS

Whether at home or in the office, access to a server through a wireless connection can increase the risk of a network being attacked. Notwithstanding convenience, wireless networks should be assessed on security grounds and adequate security measures should be implemented.

In respect of the use of unsecured third-party wireless connections, such as those provided in cafes, airports, and hotels, it is important to recognise the risk of an attack from another device on the unsecured network. It is therefore advisable that appropriate security measures are in place when the use of such networks is allowed e.g. implementing a firewall on portable devices.

As with remote access, wireless networks should be assessed on security rather than solely on the ease of use. You must ensure that appropriate security precautions are in place on the network through, for example, appropriate encryption measures or specification of authorised devices.

You can also increase their protection while using wireless networks by notifying wireless network users that devices should only connect to the network when necessary. Further, when using unsecured Wi-Fi to transmit personal or sensitive data, a secure web session should be in place to protect the data.

A Virtual Private Network (VPN) could also be set up. This encrypts all your data that passes through the network and is therefore useful in helping prevent cybercriminals from intercepting it.

5.2.12. DISABLE AUTOCOMPLETE & USE SHARED FOLDERS

Misdirected emails are a known threat to the security of personal data. You should disable the autocomplete function on email applications to mitigate the risk of breaches as a result of misdirected emails.

In addition, you could prohibit the transfer/sharing of information as an attachment to an email and could instead save the relevant documents in a predetermined shared folder, which can then be referred to in an email. If the email is sent to an incorrect recipient, the data remains secure as the incorrect recipient would not have access privileges to the link/folder referred to.

5.2.13. PHYSICAL SECURITY

Personal data can easily be compromised through security incidents stemming from inadequate physical security. These incidents may, for example, consist of uncontrolled access to equipment or files containing personal data, the theft or loss of the equipment or files, or the incorrect/inadequate disposal of equipment or files. You should have robust physical security measures in place to protect the personal data that you process. The physical security measures should be proportionate to the risks associated with unauthorised access, damage or interference with the personal data.

In the following, guidance is provided on physical security measures that controllers/processors should consider using, as appropriate, to protect the personal data that they process.

(a) Secure and restricted areas

You should look to establish access controls for restricted areas and the personal data therein on a need-to-know basis, to prevent unauthorised physical access, damage and interference with personal data. This may include, amongst other things, introducing measures such as establishing secure and restricted areas, limiting, controlling and monitoring access to these areas; ensuring the restricted areas are locked and alarmed when not in use; checking the quality of the doors and locks and the protection of premises by security lighting.

The measures should ensure that only staff who need to access certain areas (and the personal data therein) for their duties can do so.

In regard to visitors, appropriate measures should be implemented to ensure that their access is supervised and controlled.

(b) Physical access controls

To secure and control access to restricted areas in practice you may want to implement physical access controls. Access to areas within an organisation's premises may be controlled by traditional locks and keys. The use of traditional locks and keys may provide appropriate

security when the policy and procedure regarding the locking of doors is effectively implemented and enforced. Developing and maintaining an appropriate policy on access controls to restricted areas, including locking and securing doors, can minimise the risk of these remaining unlocked, particularly, when areas are left unsupervised.

Further, you may look to implement an alternative method of door access controls, such as electronic door lock systems, which may include automated locking and logging of staff access to restricted areas. In these cases, an access card may serve the dual purpose of being an electronic access card that permits and logs access to certain areas, as well as an employee identification card that allows physical identification/checks of individuals accessing restricted areas.

Physical access controls should include measures to monitor and control visitor access to controlled areas, as appropriate.

(c) Secure storage

You should ensure that you implement storage arrangements with appropriate security to protect equipment and files containing personal data. For example, you may implement a 'clear desk policy' and lockable storage facilities (such as lockable draws and cabinets) to store records, with access limited to staff that requires it for their role.

(d) Computer screens

You should take necessary precautions to ensure that computer screens cannot be viewed by unauthorised individuals (e.g. members of the public). For example, computer privacy screens should be set up so that they cannot be viewed by unauthorised individuals e.g. the general public. On a similar note, privacy screens for mobile devices should also be considered.

(e) Secure disposal

You have an obligation to ensure that secure arrangements to dispose of records and equipment used to process personal data are made. In regard to paper records, it is advisable that these are shredded.

If a third-party provider is used to dispose of or recycle records and/or computers, the organisation should ensure that this is done securely, with an adequate written contract in place that fully protects personal data by ensuring compliance with the provisions of data protection legislation. Without appropriate arrangements in place, you may be held responsible if personal data collected is not disposed of properly and is somehow obtained by a third-party.

ANNEX A - THREATS

1. Threats to confidentiality

The following table presents the generic threats that can lead to illegitimate access to personal data and/or data being compromised.

Generic threats	Examples of threats
C01. Abnormal use of hardware	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.
C02. Hardware espionage	Watching a person's screen without them knowing while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals, etc.
C03. Hardware alteration	Tracking by a hardware-based keylogger; removal of hardware components; connection of devices (such as USB flash drives) to launch an OS or retrieve data, etc.
C04. Hardware loss	Theft of a laptop from a hotel room; theft of a professional mobile phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc.
C05. Software function creep	Content scanning; illegitimate cross-referencing of data; raising of privileges, wiping of usage tracks; sending of *spam* via an e-mail program; misuse of network functions, etc.
C06. Software analysis	Scanning of network addresses and ports; collection of configuration data; analysis of source codes in order to locate exploitable flaws; testing of how databases respond to malicious queries, etc.
C07. Software alteration	Tracking by a software-based key logger; infection by malicious code; installation of a remote administration tool; substitution of components, etc.
C08. Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.
C09. Remote espionage of individuals	Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings, etc.
C10. Manipulation of individuals	Influence (phishing, social engineering, bribery, etc.), pressure (blackmail, psychological harassment, etc.), etc.
C11. Acquisition of individuals	Employee poaching; assignment changes; takeover of all or part of the organisation, etc.
C12. Viewing of paper documents	Reading, photocopying, photographing, etc.
C13. Theft of paper documents	Theft of files from offices; theft of mail from mailboxes; retrieval of discarded documents, etc.
C14. Espionage of paper transmission channels	Reading of signature books in circulation; reproduction of documents in transit, etc.
C15. Misdirected data transfer	Misdirected email etc.
C16. Staff snooping	Staff access to records without justification.

C17. Excessive access	Allowing unnecessary access to data undermines confidentiality.

2. Threats to integrity

The following table outlines threats that can lead to changes in processing, unwanted changes to personal data, and/or alterations to legal processes.

Generic threats	**Examples of threats**
I01. Hardware alteration	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of an application, etc.
I02. Abnormal use of software	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.
I03. Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.
I04. Man-in-the-middle attack via computer channels	*Man-in-the-middle attack* to modify or add data to network traffic; replay attack (resending of intercepted data), etc.
I05. Work overload	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc.
I06. Manipulation of individuals	Influence (rumor, disinformation, etc.), etc.
I07. Forgery of paper documents	Changes to figures in a file; replacement of an original by a forgery, etc.
I08. Manipulation of paper transmission channels	Changes to a memo without the author's knowledge; change from one signature book to another; sending of multiple conflicting documents, etc.

3. Threats to availability

The following table outlines threats that can lead to the unavailability of processes, disappearance of personal data and/or unavailability of processing.

Generic threats	**Examples of threats**
A01. Hardware function creep	Storage of personal files; personal use, etc.
A02. Hardware overload	Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, etc.
A03. Hardware alteration	Addition of incompatible hardware resulting in malfunctions; removal of components essential to the proper operation of the system, etc.
A04. Hardware damage	Flooding, fire, vandalism, damage from natural wear and tear, storage device malfunction, etc.
A05. Hardware loss	Theft of a laptop or mobile phone; disposal of a device or hardware, etc.
A06. Abnormal use of software	Erasure of data; use of counterfeit or copied software; operator errors that delete data, etc.
A07. Software overload	Exceeding of database size; injection of data outside the normal range of values, etc.

A08. Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.
A09. Deletion of all or part of a software program	Erasure of a running executable or source codes; logic bomb, etc.
A10. Loss of software	Non-renewal of the license for software used to access data, etc.
A11. Computer channel overload	Misuse of bandwidth; unauthorised downloading; loss of Internet connection, etc.
A12. Computer channel damage	Cut wiring, poor Wi-Fi reception, etc.
A13. Computer channel disappearance	Theft of copper cables, etc.
A14. Work overload	High workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc.
D15. Personal injury	Occupational accident; occupational disease; other injury or disease; death; neurological, psychological or psychiatric ailment, etc.
D16. Departure of a person	Reassignment; contract termination or dismissal; takeover of all or part of the organisation, etc.
A17. Erasure of paper documents	Gradual erasure over time; voluntary erasure of portions of a document, etc.
A18. Damage to paper documents	Aging of archived documents; burning of files during a fire, etc.
D19. Disappearance of paper documents	Theft of documents; loss of files during a move; disposal, etc.
A20. Overload of paper transmission channels	Mail overload; overburdened validation process, etc.
A21. Damage to paper transmission channel	End of workflow following a reorganisation; mail delivery halted by a strike, etc.
A22. Alteration of paper transmission channels	Change in how mail is shipped; reorganisation of paper transmission channels; change in working language, etc.
A23. Disappearance of paper transmission channels	Elimination of a process following a reorganisation; loss of a document delivery company, etc.

ANNEX B – THREATS AND LIKELIHOOD ASSESSMENT QUESTIONS

A. NETWORK AND TECHNICAL RESOURCES		
1	**Is any part of the processing of personal data performed through the internet?** *Examples:* · An e-marketplace offering the possibility of online purchase of goods · An e-news portal providing personalised information for registered users · A CRM system offered through a cloud as a service solution.	When the processing of personal data is performed fully or partially through the open Internet, possible threats from external online attackers increase (e.g. Denial of Service, SQL injection, Man-in-the-Middle attacks), especially when the service is available (and, thus, traceable/known) to all internet users.
2	**Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?** *Examples:* · An insurance company allows remote access (through the internet) for managers to the clients' files. · A consulting company allows staff to access the internal system for managing leaves and missions through the internet. · A company provides remote access to the system to external contractors for IT maintenance and support.	When access to an internal data processing system is provided through the internet, the likelihood of external threats increases (e.g. due to external online attackers). At the same time the likelihood of (accidental or intentional) misuse of data by the users also increases (e.g. accidental disclosure of personal data when working in public spaces). Special attention should be given to cases where remote management/administration of the IT system is allowed.
3	**Is the personal data processing system interconnected to another external or internal (to your organisation) IT system or service?** *Examples:* · An e-bookshop is connected to an online payment system (to support electronic purchases). · A small clinic finance IT system is connected to the IT system of national insurance scheme (to validate insurance status of the patients). · A CRM system interconnected with the IT system processing orders and systems supporting payments and invoice issuing.	Connection to external IT systems may introduce additional threats due to the threats (and potential security flaws) that are inherent to those systems. The same applies also to internal systems, taking into account that, if not appropriately configured, such connections may allow access (to the personal data) to more persons within the organisation (which are not in principle authorised for such access).
4	**Can unauthorised individuals easily access the data processing environment?** *Examples:* · An SME does not have a dedicated computer room for administering the IT system used for the processing of personal data. · An SME has outsourced the storage of its data to a company offering remote data storage. It is not clear what security measures have been applied by the company to safeguard the premises of the data centre.	Although focus has been put on electronic systems and services, the physical environment (relevant to these systems and services) is an important aspect that, if not adequately safeguarded, can seriously compromise security (e.g. by allowing unauthorised parties to gain physical access to the IT equipment and network components or failing to provide protection of the computer room in the event of a physical disaster).
5	**Is the personal data processing system designed, implemented or maintained without following relevant documented best practices?** *Examples (of best practices in the field):*	Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. To this end, best practices accumulate the experience of prior events and can be regarded as practical

	· The different network and system components are based on standard IT technologies and protocols (contrary to ad-hoc solutions). · Hardware and software is obtained by trusted providers and following formal contractual procedures. · A proper maintenance plan is in place, including regular maintenance of network and system devices and applications.	guidelines of how to avoid exposure and achieve certain levels of resilience.
B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA		
6	**Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?** Examples: · Assistants in the financial department cannot only enter information, but also modify and delete it, same as managers. · The nurses in a medical clinic can modify the patient's medical file, although only doctors should be able to do so.	When roles and responsibilities are not clearly defined, access (and further processing) of personal data may be uncontrolled, resulting to unauthorised use of resources and compromising the overall security of the system.
7	**Is the acceptable use of the network, system and physical resources within the organisation ambiguous or not clearly defined?** *Examples:* · It is not clear if employees can use their professional email address for personal communications. · There is no policy in place mandating the level of bandwidth usage that employees are allowed to on a daily basis.	When acceptable use of resources is not clearly mandated, security threats might arise due to misunderstanding or intentional misuse of the system. The clear definition of policies for network, system and physical resources can reduce potential risks.
8	**Are the employees allowed to bring and use their own devices to connect to the personal data processing system?** *Examples:* · Employees can connect to the company's network with their tablets or other smart devices. · Employees are allowed to process data using specific applications installed in their personal tables/smart devices.	Employees using their personal devices within the organisation could increase the risk of data leakage or unauthorised access to the information system. Moreover, as devices are not centrally controlled, they may introduce additional bugs or viruses into the system.
9	**Are the employees allowed to transfer, store or otherwise process personal data outside the premises of the organisation?** *Examples:* · A travel agency allows employees to use their professional laptops outside the premises of the organisation in order to process clients' data. · A delivery company allows employees to use dedicated tablets while making the delivery to validate details of the recipient.	Processing of personal data outside the premises of the organisation can offer a lot of flexibility, but at the same time introduces additional risks, both related to the transmission of information through possibly insecure network channels (e.g. open Wi-Fi networks), as well as unauthorised use of this information.
10	**Can personal data processing activities be performed without log files being created?** *Examples:* · There is no list of persons accessing the computer room of a company on daily basis. · Access to the medical files of patients in a clinic is not registered. · There is no policy in place mandating how the logs are monitored and what actions should be taken in case of repeated abuse of the system.	The lack of appropriate logging and monitoring mechanisms can increase intentional or accidental abuse of processes/procedures and resources, resulting to the subsequent abuse of personal data.
C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA		
11	**Is the processing of personal data performed by an undefined number of employees?** *Examples:* · The HR ticketing system of a company can be viewed by all staff members.	When access (and further processing) of personal data is open to a large number of employees, the possibilities of abuse due to human factor increase. Clearly defining who really needs to access the data and limiting

	· Medical records of patients can be processed by secretaries although only treating medical staff should have access.	access only to those persons can contribute to the security of personal data.
12	**Is any part of the data processing operation performed by a contractor/third-party (data processor)?** *Examples:* · The IT system of a private school is hosted at an external data centre. · The client files of an insurance company are being processed by external associates of the company · A specialised company is contracted for the destruction of patient files in a medical clinic. · A company uses a Cloud as a Service solution to manage internal resources.	When the processing is performed by external contractors, the organisation may lose partially the control over these data. Moreover, additional security threats may be introduced due to the threats that are inherent to these contractors. It is important for the organisation to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control.
13	**Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?** *Examples:* · Employees are not clearly informed that they are processing confidential information which may not be disclosed to unauthorised parties. · External associates of a company are not given clear instructions regarding the required level of security of personal data processed by them.	When employees are not clearly informed about their obligations, threats from accidental misuse (e.g. disclosure or destruction) of data many significantly increase.
14	**Is the personnel involved in the processing of personal data unfamiliar with security matters?** *Examples:* · Not all persons involved in data processing are informed about possible security threats and proper use of resources. · The staff handling the telephone centre of a company has not been informed about possible phishing and targeted attacks.	When employees are not aware of the need of applying security measures, they can accidentally pose further threats to the system. Training can greatly contribute in making employees aware both of their data protection obligations, as well as the application of specific security measures.
15	**Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?** *Examples:* · HR data of employees are not kept in locked file cabinets. · Copies of received invoices with credit card and bank account details are not being destroyed with paper shredders, after being processed.	Many personal data breaches occur due to the lack of physical protection measures, such as locks and secure destruction systems. Paper based files are usually part of the input or the output of an information system, can contain personal data and should also be protected from unauthorised disclosure and re-use.
D. BUSINESS SECTOR AND SCALE OF PROCESSING		
16	**Do you consider your business sector as being prone to cyberattacks?** *Examples:* · A number of companies (of the same sector) were attacked during the last year. · Publicity has been given to possible security threats and vulnerabilities of the particular business sector (e.g. as a result of a study).	When security attacks have already taken place in a specific business sector, there is an indication that the organisation would probably need to take additional measures to avoid a similar event.
17	**Has your organisation suffered any cyberattack or other type of security breach over the last two years?** *Examples:* · The IT department has discovered an increased number of unsuccessful attempts from external systems to gain unauthorised access to the database. · Locks in the central data centre have been violated.	If the organisation has already been attacked or there are indications that this might have been the case, additional measures need to be taken to prevent similar events in the future.

18	**Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?** *Examples:* · Users of the online service of an e-shop have notified that they could accidentally access accounts of other users. · Auditors have found that the password policy utilised by an online service is weak.	Security bugs/wholes can be exploited to perform attacks (cyber or physical) to systems and services. Information regarding such cases should be considerably considered.
19	**Does your processing operation concern a large volume of individuals and/or personal data?** *Examples:* · An online patient record application of a hospital which stores data of chronic disease patients all over the country. · An online dating site which stores profiles of hundreds of users.	The type and volume of personal data (scale) can make the processing operation attractive to attackers (due to the inherent value of these data).
20	**Are there any security best practices specific to your business sector that have not been adequately followed?** *Examples (of possible sector specific practices):* · A company subject to specific security measures for medical devices, financial services or telecommunication services.	Sector specific security measures are usually adjusted to the needs (and risks) of the particular sector. Lack of compliance with relevant best practices might be an indicator of poor security management.

IMPORTANT NOTE

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

Where necessary, the 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 GDPR and the DPA, the GDPR and 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