GRA
GIBRALTAR REGULATORY AUTHORITY

(7) Guidance for SMEs: Personal Data Inventory Tool & Readiness Checklist & Policy Guide

Guidance on the General Data Protection Regulation

DISCLAIMER

Please note that, on 1st January 2021, the EU General Data Protection Regulation 2016/679 ("EU GDPR") was superseded by the Gibraltar General Data Protection Regulation. The legislation however remains largely the same, and therefore, the general principles relating to the EU GDPR as may be referenced within this Guidance Note, continue to apply to the current regime.

13th September 2018

Guidance Note IR02/18

CONTENTS

1. INTRODUCTION....3

2. WHAT IS THE GDPR & HOW DOES IT APPLY TO YOU?....4

3. GDPR & ENCOURAGING RISK-BASED COMPLIANCE....6

4. INVENTORY, READINESS & POLICY TOOLS....9

5. GLOSSARY....10

6. ANNEX A - PERSONAL DATA INVENTORY TOOL....12

7. ANNEX B – READINESS ASSESSMENT CHECKLIST....13

8. ANNEX C – DATA PROTECTION POLICY GUIDE....18

1. INTRODUCTION

As a small business you may have heard of the General Data Protection Regulation ("GDPR"), but what exactly do you need to do to comply? The GDPR was introduced on the 25th May 2018 throughout the European Union ("EU"), including Gibraltar, to strengthen the data protection rights of individuals.

Whilst the GDPR brings about changes that reflect the increased importance of data protection in society, many of the main concepts and principles remain the same as those in the previous data protection framework. The GDPR does however, introduce new elements and significant enhancements, which will require detailed consideration. The GDPR emphasises transparency, security and accountability by organisations, while at the same time standardising and strengthening the privacy rights of European citizens.

This is the seventh of a series of Guidance Notes that the Gibraltar Regulatory Authority ("GRA"), as the Information Commissioner, has published in relation to the GDPR and the revised Data Protection Act 2004 ("DPA").

This Guidance Note includes a 'Personal Data Inventory Tool', a 'Readiness Checklist', and a 'Data Protection Policy Guide' that have been designed to assist, particularly the small and medium sized enterprise ("SME"), who may not have access to extensive planning and legal resources. Using this guide, along with our first GDPR Guidance Note namely "Getting Started" (IR03/16) will help implement data-protection compliant arrangements.

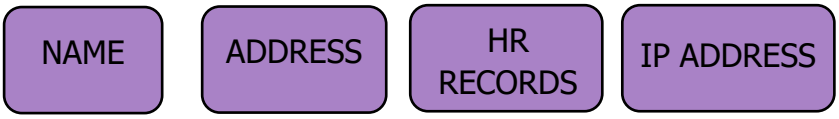
Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance notes are consistent with others made available by fellow 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 the Irish Data Protection Commissioner's office.

2. WHAT IS THE GDPR & HOW DOES IT APPLY TO YOU?

Designed to help safeguard data protection rights for individuals, the GDPR introduces a single set of rules across the EU when it comes to how organisations handle data relating to identifiable individuals. For example, if your business holds any of the following personal information, you would be subject to the requirements of the GDPR and the DPA:



Being a small business doesn't mean that you fall outside of the scope of GDPR and the DPA. All companies, regardless of their size, are urged to get on the front foot when it comes to data protection standards. Commonly, SMEs are acknowledged to have fewer resources or recognised for processing lower volumes of non-sensitive data. The standards that organisations implement should be proportionate to their data processing. This means that the Commissioner will expect more robust arrangements from organisations that process large volumes of data, and/or data of a sensitive nature, than from an SME with largely inconsequential data processing activities.

The following are ten key steps that will help towards ensuring compliance with the GDPR and the DPA:

1. **Identify the personal data that you hold**
All organisations must identify what personal data they hold. This can be achieved by setting out the information listed in Article 30 of the GDPR. Smaller companies may benefit from using the Personal Data Inventory Tool in Annex A.

2. **Conduct a risk assessment**
This should include a risk assessment of the personal data you hold and your data processing activities (Further information can be found in Article 24 and Recital 75 of the GDPR and in the subsequent section titled "risk-based compliance").

3. **Implement appropriate technical & organisational measures**
This must be done to ensure data (found on digital and paper files) is stored securely. The security measures your business should put in place will depend on the type of personal data you hold and the risk to your customers and employees should your security measures be compromised (Article 32 of the GDPR).

4. **Lawful basis**
Know the legal basis you rely on: is it consent? Is it a contractual obligation or legitimate interest? Your legal basis must justify your processing of personal data (Articles 6 to 10 of the GDPR). Please see the Information Commissioner's Guidance Note "(6) Identifying the 'Lawful Basis'" available here: https://www.gra.gi/data-protection/guidance

5

Data minimisation, storage limitation and accuracy

Ensure that –

- you are only collecting the minimum amount of personal data necessary to conduct your business;
- you only keep it for as long as necessary; and
- you use reasonable measures to keep data accurate (Article 5 of the GDPR).

6

Purpose specification, retention and transparency

Be transparent with your customers about the reasons for collecting their personal data. Inform about the specific uses it will be put to and how long you need to keep their data on file. This notice may be portrayed on your website, on forms used to collect data or using signs e.g. at points of sale (Articles 12, 13 and 14 of the GDPR).

7

Special categories of data and data relating to criminal offences

Do you process special categories of personal data and/or data relating to criminal offences? If so, you should take extra precautions and identify the appropriate lawful basis as per point 4 above.

8

Data protection officer (DPO)

Your organisation should decide whether it needs to appoint and retain the services of a DPO (Article 37 of the GDPR). Please see the Information Commissioner's Guidance Note "(3) Data Protection Officer" available here: https://www.gra.gi/data-protection/guidance

9

Rights of the data subject

All organisations must be able to facilitate requests from service-users wishing to exercise their rights under the GDPR, including rights of access, rectification, erasure, withdrawal of consent, data portability and the right to object to automated processing (Articles 12 to 22 of the GDPR).

10

Updated policies

Where appropriate, organisations should ensure that they regularly update any policy/procedure documents that detail how the organisation is meeting its data protection obligations. This will prove useful to demonstrate compliance and meet the requirements of the accountability principle under the GDPR.

Annex C provides an example of how a data protection policy may be structured. Note that Annex C may be used as guidance, but that each organisation needs to adapt it to their data processing arrangements and that adopting Annex C may not be sufficient for all organisations.

3. RISK-BASED COMPLIANCE

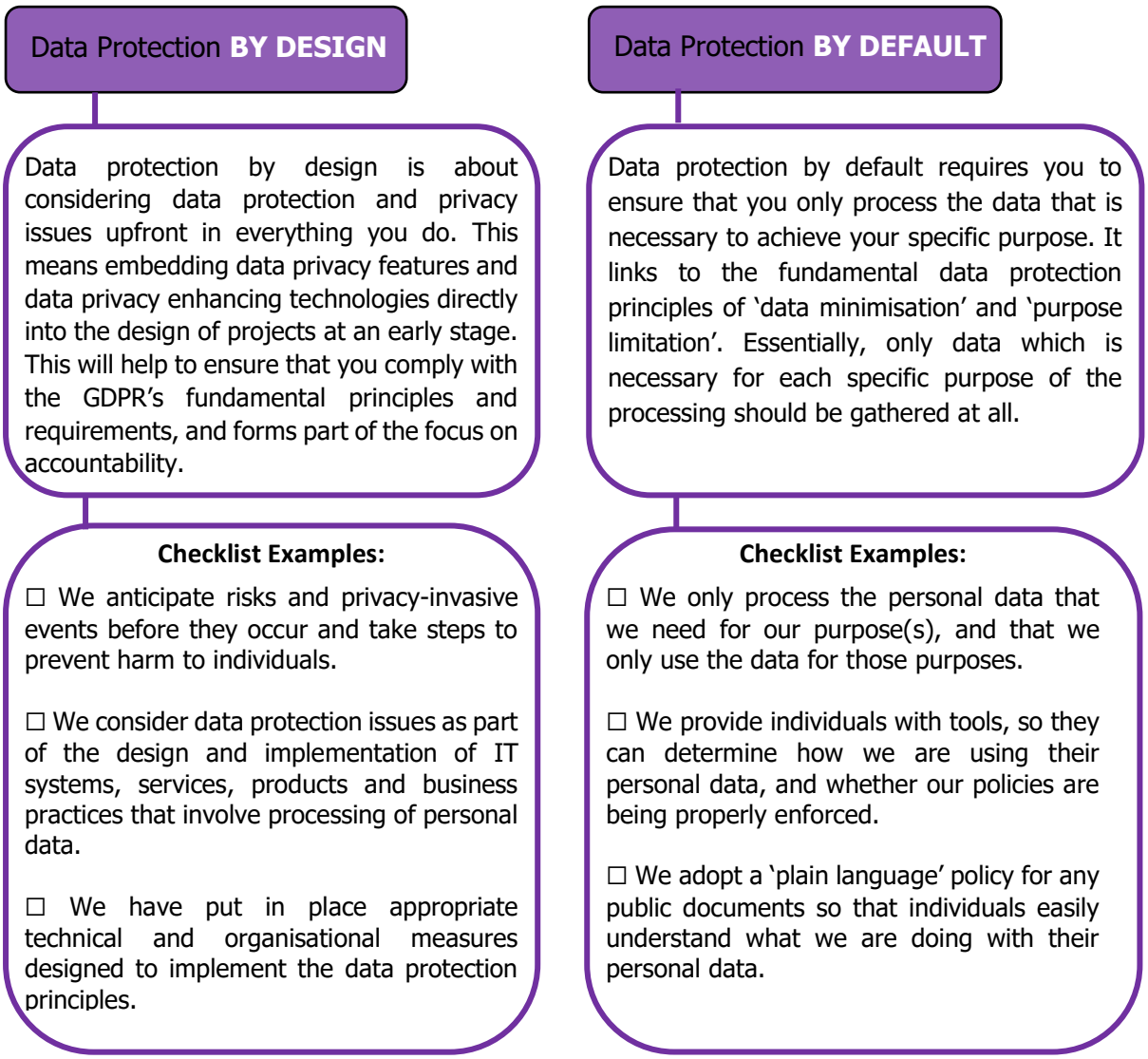
Risk analysis is contextual. The concept of risk appears in the GDPR and the DPA and it is defined by reference to the "likelihood and severity" of a negative impact on data subject rights. In such circumstances controllers should account for "the nature, scope, context and purposes of the processing." Effectively, this concept of risk analysis most notably appears in the measures controllers should implement to assure adequate data security and in doing so:

In essence, the risk-profile of the personal data your organisation processes should be determined according to the personal data processing operations carried out, taking into account the complexity and scale of data processing, the sensitivity of the data processed, and the protection required for the data being processed. For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet, health, financial or insurance company), this would attract a higher risk rating than routine personal data that relates solely to employee or customer account details.

To ensure risk-based compliance, it is useful to look at the perceptible harms to individuals that your organisation needs to safeguard against. This may include processing that could give rise to: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation; or any other significant economic or social disadvantage (as cited in Recital 75 of the GDPR).

Risk-assessments will improve awareness in your organisation, predominantly for the potential future data protection issues associated with a project. This will in turn help to improve the design of your project and enhance your communication about data privacy risks with the relevant stakeholders.

While long recommended as good practice, the GDPR provides for two crucial concepts for future project planning. Both principles are enshrined in law under Article 25 of the GDPR and are summarised as:



In regard to who, from the organisation, is responsible for complying with data protection by design and by default, accountability lies with the data controller. Depending on the circumstances and structure of the SME, there may be different requirements for different areas of organisation. For example:

- Senior management may be responsible for developing a "privacy awareness" culture and ensure that the appropriate policies and procedures are in place to comply with data protection standards;

  OR

- IT personnel may be responsible for complying with data protection requirements within the design systems, products and services afforded, maintained and/or updated by this team.

Whilst this may not apply to all organisations, data protection by design and default is about adopting an organisation-wide approach to data protection and "baking in" privacy consideration into any processing activity you undertake.

Data Protection Impact Assessment (DPIA)[1]

The GDPR introduces a new obligation to perform DPIAs. A DPIA is now a mandatory pre-processing requirement if the envisaged project/initiative/service involves data processing which "is likely to effect in a high risk to the rights and freedoms of natural persons." It is a way for organisations to systematically and comprehensively analyse the processing activities and help identify, and minimise, any data protection risks.

In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still best practice and a very useful tool to help data controllers demonstrate their compliance with data protection law.

Risk Register

The concept of risk analysis most notably appears in the measures controllers should implement to assure adequate data security. However, controllers also are required to take risk into account as part of their "general obligations." Maintaining a data protection risk register for example, may allow you to identify and mitigate against data protection risks, as well as demonstrate compliance in the event of a regulatory investigation or audit.

IMPORTANT

This document is purely for guidance and does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the General Data Protection Regulation will apply directly to them. The responsibility to become familiar with the Regulation and comply with its provisions therefore lies with the organisation. This guide is intended as a starting point only, and organisations may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries.

[1] Please see the Information Commissioner's Guidance Note "(4) Data Protection Impact Assessments" available here: https://www.gra.gi/data-protection/guidance

4. INVENTORY, READINESS & POLICY TOOLS

Whilst the GDPR and the revised DPA might seem like looming giants to SMEs, it doesn't have to be daunting. Ignoring data protection law will not make it go away, so it is important to make sure your SME understands what the GDPR and the DPA mean to your business specifically, and seek out the right resources to help you prepare and comply.

To assist, particularly SMEs, who may not have access to extensive planning and legal resources, this Guidance Note includes the following -

1) Personal Data Inventory Tool

This tool will allow organisations to map out the personal data they hold and process. It will serve as a starting point to create an inventory in relation to the categories of the personal data processed, the lawful basis for each processing purpose(s), the retention period(s) and what, if any, remedial action is required to ensure compliance with data protection law (see Annex A).

2) Readiness Assessment Checklist

After completing using the Personal Data Inventory Tool, this checklist provides a general means for organisations to ensure that the right measures (both organisational and technical) are taken, and at the same time, get an idea about their effectiveness. Aside from being a thought-provoking exercise, this assessment will allow organisations to further analyse their data protection capabilities, establish what measures they have in place and what else they must do to ensure compliance with data protection law (see Annex B).

3) Data Protection Policy Guide

A 'Data Protection Policy' or 'Privacy Policy', is a term commonly used to describe an internal document that defines an organisation's data handling arrangements to ensure compliance with data protection law.

Annex C is an example guide of how a Data Protection Policy may be structured and what it should include. It is important to note that Annex C is to serve as guidance, but that each organisation needs to adapt it to their data processing arrangements and that adopting Annex C may not be sufficient for all organisations.

5. GLOSSARY

Consent
Article 7 of the GDPR has altered the conditions needed for consent as a legal basis for data processing to be valid. It is now necessary to consider whether consent was freely given, and the data subject must have the opportunity to withdraw consent for processing at any time. Consent should not be assumed and must be obtained before data processing begins (e.g. through Privacy Notices).

Data Controller
Data Controllers are persons or organisations who decide the purposes for which, and the means by which, personal data is processed. Further, the purpose of processing data involves 'why' the personal data is being processed and the means of the processing involves 'how' the data is processed.

Data Processor
A person or organisation that processes personal data on behalf of a data controller.

Data Protection Impact Assessment (DPIA)
A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the GDPR.

Data Subject
A Data Subject is the individual the personal data relates to.

Lawful Basis[2]
In order to process personal data, you must have a lawful basis to do so. The lawful grounds for processing personal data are set out in Articles 6, 9 AND 10 of the GDPR.

Personal Data
Personal Data refers to any information relating to a living individual who is, or can be, identified by that information, including data that can be combined with other information to identify an individual.

Processing
Processing means performing any operation or set of operations on personal data which may include (a) obtaining, recording or keeping data; (b) organising or altering the data; (c) retrieving, consulting or using the data; (d) disclosing the data to a third party (including publication) and; (e) erasing or destroying the data.

Retention Policy
How long will your organisation hold an individual's personal data?
Your retention period will be influenced by several factors. There may be legal or other requirements on your organisation, which may vary depending on your business type, but data should not be retained longer than necessary, in relation to the purpose for which such data is processed. Further, data must be stored securely while it is in your possession and you must ensure it is deleted fully and safely at the appointed time.

Special Categories (Sensitive) of Personal Data
Previously referred to as "sensitive data", this is newly defined in Article 9(1) of the GDPR. It refers to data 'which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

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

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

ANNEX A –PERSONAL DATA INVENTORY TOOL

Categories of personal data and data subjects	**Elements of personal data included within each data category**	**Source of the personal data**	**Purposes for which personal data is processed**	**Lawful basis for each processing purpose**	**Special categories of personal data/data relating to criminal convictions**	**Lawful basis for processing special categories of personal data/data relating to criminal convictions**	**Retention period**	**Accuracy**	**Remedial action required to ensure compliance with data protection law**
List categories of personal data collected & retained. *For example:* *Current employee data* *Retired employee data* *Customer data (if any)* *Marketing database to include data about other businesses* *CCTV footage.*	***List each type of personal data included within each category of personal data*** *For example:* *Name* *Address(es)* *Banking details* *Business purchases/transactions* *Medical details* *Stored video and images of events.*	***List the source(s) of the personal data*** *For example:* *Whether the data was collected directly from individuals.* *Whether the data was collected indirectly, from third parties.*	***Within each category of personal data, list the purposes for the data is collected & retained*** *For example:* *Did you collect the data for marketing purposes?* *Was the data collected and stored as part of a service enhancement or research project?* *Did you collect the data for a volunteer's programme or event?*	***For each purpose that personal data (non-special categories) is processed, list the legal basis on which it is based*** *Establish whether you are processing the data under consent for example, or whether you intend to satisfy a contractual or legal obligation.*	***If special categories of personal data are collected & retained, it is important to set out details of the nature of the data*** *For example:* *Medical/health data* *Genetic and/or biometric data* *Sexual orientation* *Politics* *Religion* *Ethnic Origin*	***List the lawful basis on which special categories of personal data are collected and retained*** *Establish whether you are processing the data with explicit consent from the data subject.*	***For each category of personal data, list the period for which the data will be retained*** *For example:* *Do you retain/store the data for a month?* *Are you required to retain the data for a year?* *As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.*	***How important is data accuracy? Where applicable, when will updates occur?***	***Identify actions that are required to ensure all personal data processing operations are GDPR compliant*** *For example, this may include deleting data where there is no further purpose for retention.*

ANNEX B – READINESS ASSESSMENT CHECKLIST

PERSONAL DATA

	Question	Yes	No	Comments/Remedial Action
Consent-based data processing *(Article 15 of the GDPR)*	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific and informed?			
	When seeking consent, has the individual chosen to agree to the processing of their data by way of statement or a clear affirmative action?			
	If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual's consent to ensure compliance under the GDPR?			
	Are procedures in place to demonstrate that an individual has consented to their data bring processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their data at any given time?			
Children's Personal Data *(Article 8 of the GDPR)*	Where online services are provided to a child, are procedures in place to verify the age of that child?			
	Are measures in place to get consent of a parent or legal guardian where required?			
Processing of data based on legitimate interest	If legitimate interest is a legal basis on which personal data is processed, has your organisation carried out a suitable analysis to ensure that the use of this legal basis is appropriate? *Your analysis must demonstrate that (i) there is a valid legitimate interest; (ii) the data processing is strictly necessary in pursuit of the legitimate interest and (iii) the processing is not prejudicial to or overridden by the rights of the individual.*			

DATA SUBJECT RIGHTS

	Question	Yes	No	Comments/Remedial Action
Access to persona data *(Article 15 of the GDPR)*	Is there a documented policy/procedure in place for handling Subject Access Requests (SARs)?			
	Is your organisation able to respond to SARs within the one month deadline set by the GDPR?			
	Are you aware of what information can be provided via a SAR, the set response times or way of providing the requested information to the data subject?			
Data Portability *(Article 20 of the GDPR)*	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?			
Deletion & Rectification *(Articles 16 & 17 of the GDPR)*	Are there controls/procedures in place to allow personal data to be deleted or rectified (if applicable)?			
Right to Restriction of Processing *(Article 18 of the GDPR)*	Do you have controls/procedures in place to halt the processing of personal data where an individual has, on valid grounds sought the restriction of processing?			
Right to Object to Processing *(Article 21 of the GDPR)*	Are individuals informed about their right to object to certain types of processing (i.e. direct marketing)?			
Profiling & Automated Processing *(Article 22 of the GDPR)*	Where an automated decision is made which is necessary for entering into, or performance of a contract, or based on explicit consent, are procedures in place to facilitate an individual's right to obtain human intervention and to content this decision?			

ACCURACY & RETENTION

	Question	Yes	No	Comments/Remedial Action
Purpose Limitation	Is personal data only used for the purpose(s) for which it was originally collected?			
Data Minimisation	Do you agree that the data collected is limited to what is necessary for the purpose(s) for which it is processed and nothing further?			
Accuracy	Are procedures in place to ensure personal data is kept up-to-date and accurate?			
Retention	Are retention policies/procedures in place to ensure data is held for longer than is necessary?			
Other legal obligations governing retention	Is your business subject to other rules that require a minimum retention period (e.g. medical records, tax)?			
	Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?			
Duplication of Records	Are there procedures to ensure that there is no unnecessary or unregulated duplication of records?			

TRANSPARENCY

	Question	Yes	No	Comments/Remedial Action
Being transparent with customers & employees *(Articles 12, 13 & 14 of the GDPR)*	Are your service users fully informed of how you use their data?			
	Are your employees fully informed of how you use their data?			
	Are you able to advise your customers and/or employees about how their data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data is collected directly from the individuals, are procedures In place to provide them with the information listed in Article 13 of the GDPR?			
	If personal data is collected from third parties (that is, not directly obtained from the individuals), do you have procedures in place to provide the information listed in Article 14 of the GDPR?			
	When engaging with individuals, such as when providing a service for example, do you proactively inform the individuals of their privacy rights?			
	Is information about how transparent your organisation is with regards privacy rights and compliance with GDPR principles published in an easy, accessible and readable format?			

OTHER OBLIGATIONS

	Question	Yes	No	Comments/Remedial Action
Supplier Agreements *(Articles 27 to 29 of the GDPR)*	Do you have agreements in place with suppliers and other third parties processing personal data on your behalf?			
	Are the above agreements reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Officers (DPOs) *(Articles 37 to 39 of the GDPR)*	Does your organisation need to appoint a DPO?			
	If your organisation has decided that a DPO is not required, have you documented the reasons why?			
	Where a DPO is appointed, are escalation and reporting lines in place and have these procedures been documented?			
	Have you published the contact details of your DPO to facilitate your customers/employees in making contact with them?			
	Have you notified the Information Commissioner of your DPO's contact details using the registration form on the website (www.gra.gi)?			
Data Protection Impact Assessments (DPIAs) *(Article 35 of the GDPR)*	Is your data processing activity considered high-risk?			
	If so, is there a process for identifying the need for, and conducting of DPIA's?			
	If you have carried out a DPIA, have you documented the procedure?			

DATA BREACHES

	Question	Yes	No	Comments/Remedial Action
Data Breaches *(Articles 33 and 34 of the GDPR)*	Does the organisation have a documented privacy & security incident response plan? Are plans and procedures reviewed on a regular basis?			
	Is the reviewing process highlighted above documented?			
	Are procedures in place to notify the Information Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach if and when applicable?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, the suppliers and third parties to help resolve data breaches?			

INTERNATIONAL DATA TRANSFERS (OUTSIDE EEA) – *IF APPLICABLE*

	Question	Yes	No	Comments/Remedial Action
Access to personal data *(Article 15 of the GDPR)*	Is personal data transferred outside the EEA?			
	Does the data transferred include any special categories of personal data?			
	Have you documented the purpose(s) of the transfer?			
	Have you created a spreadsheet containing information about such transfers to include details of the nature of the data, the purpose of the processing, from/to which country the data is exported and who the recipient of the transfer is.			
Legality of International Transfers	Is there a legal basis for the transfer?			
	Are you basing the transfer on an EU Commission adequacy decision?			
	Are you basing the transfer on standard contractual clauses?			
	Have you properly documented the legal basis for the transfer?			
Transparency	Are data subjects fully informed about any intended international transfers of their personal data?			

ANNEX C – DATA PROTECTION POLICY GUIDE

DATA PROTECTION POLICY

Document control and history			
Version	**Date**	**Comment**	**Sign off**
1.0	e.g. 01/01/18	e.g. approved/reviewed	e.g. Joe Bloggs

1. INTRODUCTION

This Data Protection Policy sets out the *COMPANY NAME*'s arrangements in place to comply with its obligations under the Data Protection Act 2004 ("DPA") and the General Data Protection Regulation ("GDPR").

Further to compliance with data protection law this policy helps to protect the organisation from other risks such as damage to the reputation of the organisation and trust in the services that it provides.

The policy provides demonstrable commitment and support from senior management to ensure compliance with data protection law.

2. Data protection policy elements

In accordance with the DPA and the GDPR *COMPANY NAME* adopts and implements the following principles across the organisation –

(a) purpose specification and purpose limitation: the purpose(s) for which *COMPANY NAME* collects and uses personal data shall be specified and legitimate. The data shall not be used for anything other than the specified purposes;

(b) transparency: clear information shall be provided to individuals about the purpose(s) for which personal data are collected and used, at the time the data is collected;

(c) data minimisation: *COMPANY NAME* shall only collect personal data that is strictly necessary for the specified purpose(s) i.e. the minimum personal data required shall be collected and used;

(d) accuracy: personal data shall be accurate and where necessary kept up to date;

(e) retention: personal data shall not be kept for longer than is necessary;

(f) security: appropriate security measures to protect personal data shall be implemented and maintained;

(g) international transfers: personal data shall only be transferred to countries outside the European Economic Area when the countries have an adequate level of data protection; and

(h) accountability: the organisation will be able to demonstrate that it has implemented measures to comply with the abovementioned principles.

Further to the above, *COMPANY NAME* shall ensure that it has measures in place to ensure that it respects and conforms with the rights of individuals under data protection law, namely -

(a) the right to be informed about the collection and use of their information;

(b) the right of access to their personal data;

(c) the right for individuals to have their personal data rectified when it is inaccurate or incomplete;

(d) the right for individuals to have their personal data erased when there is no compelling reason or it to be processed;

(e) the right for individuals to request the restriction or suppression of their personal data, when the accuracy of the data is contested, or processing is unlawful, but the individual opposes erasure and requests restriction instead;

(f) the right to data portability whereby in certain circumstances individuals can request for personal data that they have submitted via automated means and in electronic format to be moved, copied or transferred to another organisation in a safe and secure way, without affecting its usability;

(g) the right for individuals to object to processing of their personal data when it is based on "legitimate interests" or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling), or when processed for purposes of scientific/historical research and statistics; and

(h) the right not to be subjected to decisions solely on automated means without human intervention.

3. Governance and accountability

Under data protection law every person that handles personal data has some responsibility to ensure that it is used appropriately. However, the following person(s) within the organisation have key responsibilities:

(a) *[Director/Head of Organisation]* – has overall responsibility for ensuring that the organisation meets its obligations under data protection law.

(b) Data Protection Officer: *[Name]* – The Data Protection Officer shall be responsible for –

i. day to day implementation and management of this policy;

ii. advising the organisation and its employees on data protection compliance;

iii. planning and coordinating activities within the organisation to ensure the objectives of this policy are met;

iv. monitoring compliance with data protection law;

v. reporting directly to the *[Director/Head of Organisation]* on data protection;

vi. ensuring that appropriate data protection training and awareness is provided to staff;

vii. acting as the contact point for the Information Commissioner;

viii. cooperating with the Information Commissioner;

(c) The [*Director/Head of Organisation/Data Protection Officer*] shall approve this policy and periodically review its implementation and effectiveness to ensure ongoing compliance with data protection law.

(d) IT Manager: [name] is responsible for ensuring that the organisation has appropriate IT security measures in place to protect the personal data held.

4. Transparency

When *COMPANY NAME* collects information about individuals, *COMPANY NAME* provides a written notice to the individuals from whom the data is collected that includes the following information:

(a) the identity of the organisation, as the data controller, including contact details;

(b) the contact details of the Data Protection Officer;

(c) the purpose for which the information is collected and use, including the lawful basis (to also include the right to withdraw consent when the lawful basis to the processing is based on consent);

(d) the period for which the data will be kept;

(e) whether the information will be shared, and if so with who;

(f) whether the information will be transferred outside of the EEA;

(g) information about the rights of individuals under the GDPR (as identified in section 2);

(h) the right of individuals to lodge a complaint with the Gibraltar Regulatory Authority ("GRA");

(i) where applicable, inform the individual that the requirement to provide the personal data is a statutory requirement, contractual requirement, or a requirement necessary to enter into a contract;

(j) identify and inform individuals where they are obliged to provide personal information together with the possible consequences of failure to provide the information; and

(k) where applicable, the existence of automated decision-making (including profiling) including meaningful information about the logic involved and the significance and envisaged consequences for the individual.

The abovementioned information and notice is provided by *COMPANY NAME* in the following manner –

[Copies of the notice provided can be included in an Annex and referred to.

Note: the law is flexible on how organisations provide the notice, as long as it is concise, transparent, intelligible and in an easily accessible form, using clear and plain language. For

example, it can be included in its entirety in the forms (hard copy or electronic) used to collect the information from individuals or said forms can include a summary with a link to a page on a website, which provides the complete notice].

5. Purpose specification and purpose limitation

(a) *COMPANY NAME* collects and processes personal data only for –
[INSERT PURPOSES HERE – e.g. the provision of "dental care"]

(b) The lawful basis that *COMPANY NAME* relies on to process personal data for said purposes are –
[INSERT LAWFUL BASES HERE e.g.

- Necessary for the performance of a contractual service that is provided to the customer (Article 6(1)(b) of the GDPR).
- The provision of health care or treatment (Article 9(2)(h) of the GDPR and schedule 1, part 1, paragraph 2 of the DPA)]

6. Data minimisation

The Data Protection Officer will keep an inventory of all the personal data that the organisation holds and processes (the "Inventory"). The Inventory shall include a justification for the collection and use of each data set processed. Any data set, which is not strictly necessary for the purposes for which the data is collected shall be removed from the organisation's data processing activities.

The Inventory shall be reviewed on an annual basis. See current Inventory [include the Inventory below or attach as an Annex].

7. Accuracy

The Data Protection Officer shall ensure that the Inventory records the following for each data set –

(a) the data source;
(b) the organisation's need for accuracy of data; and
(c) the time sensitivity of each data set.

The organisation has established appropriate measures to ensure that the data that it processes is accurate and up to date. These measures are –
[e.g. the details of dental patients are verified and where updated on every visit/consultation]

8. Retention

The Data Protection Officer shall ensure that there is a clear policy on how long each data item in the Inventory are to be retained including the reason(s) for doing so, such as any legal requirements to retain data for a certain period.

[Insert period here e.g. on a yearly basis] the organisation purges its filing systems (manual and/or electronic) of personal data that is no longer required, in accordance with the retention periods established in the Inventory.

Details of the purges carried out including how it was carried out and by whom are recorded and signed off by the Data Protection Officer. The record of purges carried out to date is detailed in [e.g. include as an Annex or table].

9. Security

To ensure that the organisation has appropriate security measures in place to protect the personal data that it processes from being accidently or deliberately compromised, the organisation has established the following –
[Include details below or attach and refer to an Annex. Examples of aspects to consider/include:
Management & organisational information security measures - Risk Management, documentation and implementation of security measures, accountability**,** outsourcing**,** data breach management**,** disciplinary measures.
Training and awareness – staff training & awareness.
Physical security - secure areas (e.g. locked doors, CCTV), secure storage (e.g. lockable filing cabinets).
Computer security - mobile devices & remote working, modify & secure IT settings, removable media, user access controls, password security, malware protection, backing up data, logging and audit trails, patch management, boundary firewalls, encryption, wireless networks]

10. Data breach management and notification

As part of its data breach management procedure, *COMPANY NAME* shall notify the GRA[3], without undue delay and where feasible within 72 hours, after becoming aware of a data breach, unless it is determined that the breach is unlikely result in a risk to the individuals affected. If it is determined that the breach is likely to result in a high risk to the individuals affected, *COMPANY NAME* shall notify those individuals of the breach without undue delay[4].

COMPANY NAME shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (including whether it has been notified to the GRA and/or the individuals affected. The record of breaches to date is detailed in [e.g. include as an Annex or table].

11. Data subject's rights

As described in section 4 (i.e. Transparency), *COMPANY NAME* informs all individuals about their data protection rights. Any requests from individuals are internally directed to the Data Protection Officer who ensures that the request is processed and responded to without undue delay and in any event within one month of receipt of the request.

[Further information about procedures implemented to uphold the rights of individuals and facilitate their requests can be included here and/or referred to as an Annex]

12. Data protection by design by default

COMPANY NAME will consider the data protection and privacy implications of any project proposal that involves the use of personal data, prior to its implementation.
Further, periodic/yearly reviews shall be undertaken to make appropriate adjustments to the data processing with the aim of improving data protection and privacy, taking into account technological developments.

The organisation will –
[Include details of technical and organisational measures used to implement the data protection principles. For example –

[3] In accordance with Article 33 of the GDPR
[4] In accordance with Article 34 of the GDPR

- require the advice of the Data Protection Officer before progressing on a new data processing activity, particularly when it involves special categories of data, data relating to criminal convictions, and/or new technology. A record of the advice is kept;
- continuously strive to minimise the data that the organisation processes by carrying out periodic audits;
- implement pseudonymisation to the maximum extent possible;
- limit staff access to personal data to only the information that is strictly necessary for them to carry out their tasks]

13. Data protection impact assessments

Where a data processing activity is likely to result in a high risk to individuals, *COMPANY NAME* shall carry out a Data Protection Impact Assessment[5] ("DPIA"), particularly when –

- new technologies are used,
- systematic and automated processing resulting in decisions that affect individuals take place,
- special categories of personal data and/or data relating to criminal convictions are processed on a large scale, or
- systematic monitoring of a publicly accessible area on a large scale occurs.

COMPANY NAME shall:

- Seek the advice of the Data Protection Officer in regard to DPIAs.
- Include the following in its DPIAs -
    - a description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued;
    - an assessment of the necessity and proportionality of the processing in relation to the purposes;
    - an assessment of the risks to the rights and freedoms of individuals; and
    - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.

A log of all the DPIAs conducted are detailed in [e.g. include in a table or refer to an Annex].

14. Data Processors

COMPANY NAME only uses third parties to carry out an activity on the personal data that we hold, when the third party provides sufficient guarantees that it will process the data in compliance with the GDPR and the DPA.

Further, all activities on the personal data that we hold carried out by third parties on our behalf, shall be governed by a written contract as per Articles 28 and 29 of the GDPR. The following are the list of data processers contracted by *COMPANY NAME:*
[include list of data processors here and/or refer to an Annex e.g. list payroll services, cloud service providers, etc…]

[5] In accordance with Article 35 of the GDPR

CONTACT US

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

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