GRA

GIBRALTAR REGULATORY AUTHORITY

(27) Disclosures of Personal Data to Law Enforcement and other Competent Authorities

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

30th June 2022

Guidance Note IR02/22

FOREWORD

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

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

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

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

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

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

SUMMARY

- The Gibraltar General Data Protection Regulation ("Gibraltar GDPR") does not prevent organisations from sharing personal data with authorities who are discharging their statutory law enforcement functions (known under data protection law as "*competent authorities*"). The Gibraltar GDPR and the Data Protection Act 2004 ("DPA") allow for this type of data sharing where it is necessary and proportionate.

- If an organisation wants to share personal data with such an authority, it will need a lawful basis under Article 6 of the Gibraltar GDPR.

- Where the personal data constitutes special category data, it will also need a condition for processing under Article 9 of the Gibraltar GDPR, which in some cases involve additional DPA provisions.

- If an organisation wants to share criminal offence data it will need both a lawful basis under Article 6, **and** either "*official authority*" or a separate condition for processing under Article 10 of the Gibraltar GDPR, which involves additional DPA provisions.

- Paragraph 10 of Schedule 1 of the DPA provides that special category data or criminal offence data may be disclosed where it is necessary for the prevention or detection of unlawful acts.

- Paragraph 2 of Schedule 2 of the DPA provides an exemption (the "*crime and taxation*" exemption) from the Gibraltar GDPR's transparency obligations and most individual rights, but only if complying with them would prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. This is not a blanket exemption and organisations must consider it on a case-by-case basis.

- Organisations should record the lawful bases and related provisions relied on for the disclosure of personal data, special category and/or criminal offence data.

- Organisations should only share the minimum amount of personal data necessary for the intended purpose.

- Organisations should ensure that the personal data is shared in compliance with other data protection duties and obligations, including fairness, accuracy and security.

CONTENTS

1. ACKNOWLEDGEMENTS

Where appropriate the Information Commissioner[1] 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 the UK's Information Commissioner's office.

The following documents were used in the production of this Guidance Note:

(a) Information Commissioner's Office (UK)

'Sharing personal data with law enforcement authorities'

https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/

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

2. INTRODUCTION

The Gibraltar GDPR and DPA do not prevent a data controller[2] from sharing personal data with a "*competent authority*"[3] ("Competent Authority") who is exercising its statutory law enforcement functions. The Gibraltar GDPR and DPA allow for this type of data sharing where it is reasonable, necessary and proportionate.

However, where a controller receives a request for personal data from a Competent Authority,[4] it must first identify a lawful basis under Article 6 of the Gibraltar GDPR for the disclosure of said data. If a request concerns special categories of personal data[5], a lawful basis under Article 6 of the Gibraltar GDPR must be accompanied by a condition for processing under Article 9 of the Gibraltar GDPR. Conversely, if a request concerns data relating to criminal convictions and offences[6], both a lawful basis under Article 6 and a separate condition for processing under Article 10 of the Gibraltar GDPR must be met. The DPA sets out specific conditions for the disclosure of data relating to special categories and criminal convictions.

Further, it is imperative that personal data is processed (in this case, disclosed) by a controller in accordance with the data protection principles at Article 5 of the Gibraltar GDPR, as well as respecting the data protection rights of individuals at Articles 13-21 of the Gibraltar GDPR. Notwithstanding, a controller may be able to rely on certain provisions, which may exempt them from particular obligations and data subject rights, in respect of the disclosures made to Competent Authorities, for example, that provided at paragraph 2 of Schedule 2 of the DPA. However, it is up to the controller to decide whether the disclosure of data is lawful and whether an exemption applies. Where an exemption is relied on, the controller must be prepared to justify its decision to apply the exemption.

A Competent Authority should clearly explain to the controller why it needs the personal data held by a controller. In turn, the controller must only disclose data that is limited to what is requested and what is reasonable, and may, where felt appropriate, require that the request be made in writing.

A controller should consider implementing a procedure for dealing with requests for personal data from Competent Authorities, and put mechanisms in place, including staff training, to ensure that processing of this nature complies with the Gibraltar GDPR and DPA.

---

[2] 'Controller' is defined at Article 4(7) of the Gibraltar GDPR and Part I, section 2(1) of the DPA. The terms 'data controller' and 'controller' within this document are interchangeable.

[3] For the definition of Competent Authority under Part III of the DPA, see section 39(1) and Schedule 7 of the DPA.

[4] With regards data processors (as defined at Article 4(8) of the Gibraltar GDPR and Part I, section 2(1) of the DPA), it is important to note that such entities process personal data on behalf of data controllers, on their written instruction and in accordance with any contract or other legal act that is binding between the controller and the data processor, as required by Article 28(3)(a) of the Gibraltar GDPR. Therefore, data processors should consider such obligations when receiving any requests for personal data from a Competent Authority and ensure that their actions (for example, their responses to said requests) do not breach these requirements. For further guidance on these concepts please see the Information Commissioner's Guidance Note, "(24) Guidance on the Concepts of Data Controller and Data Processor" available here: https://www.gra.gi/data-protection/guidance.

[5] Article 9(1) of the Gibraltar GDPR and Part II, sections 12 and 13 of the DPA.

[6] Article 10(1) of the Gibraltar GDPR and Part II, section 12 of the DPA.

3. WHAT IS A COMPETENT AUTHORITY?

Part III, section 39(1) of the DPA defines a Competent Authority as "*a person specified or described in Schedule 7*" and "*any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes*".

Several authorities and bodies are listed in Schedule 7 of the DPA, including, for example, any of Her Majesty's ("HM") Government of Gibraltar departments, the Gibraltar Courts Service, the Royal Gibraltar Police, HM Customs Gibraltar, the Environmental Agency and the Gibraltar Financial Services Commission.

Part III of the DPA sets out separate data protection rules for Competent Authorities with law enforcement functions when they are processing data for "*law enforcement purposes*".

Under section 40 of the DPA, "*law enforcement purposes*" are the purposes of the *"prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*."

4. DISCLOSING DATA TO A COMPETENT AUTHORITY

The Gibraltar GDPR and DPA provide a framework that allows a controller to disclose personal data to a Competent Authority that needs to process said data for the law enforcement purposes. However, the legislation does not force such disclosures, but allows them on a voluntary basis, provided that the disclosure is necessary and proportionate.

There are likely to be three scenarios where a controller may need to disclose personal data to a Competent Authority to enable it to carry out its law enforcement functions -

- a controller wants to proactively disclose the data (for example, to report a crime and provide relevant personal data it holds);
- a controller receives a request from a Competent Authority for personal data it holds (for example, a Competent Authority may require this for the purposes of investigating a crime); or
- a court order or another legal obligation compels the controller to share the personal data with a Competent Authority.

4.1 Identifying the Lawful Basis

A controller must be satisfied that the disclosure of personal data to a Competent Authority is lawful. This means that a controller must have a lawful basis under Article 6(1) of the Gibraltar GDPR before disclosing personal data to a Competent Authority [7].

There are six lawful bases which may be relied on. However, it is up to the controller to decide which one is the most appropriate, depending on the particular circumstances of each case. The lawful bases most likely to be applicable are the following:

Article 6(1)(c) of the Gibraltar GDPR – 'Legal obligation'

A controller may rely on Article 6(1)(c) of the Gibraltar GDPR as the lawful basis to disclose personal data to a Competent Authority where it is necessary for compliance with a legal obligation the controller is subject to. This may apply, for example, where a court order directs the controller to disclose personal data, where a warrant has been obtained or where legislation imposes an obligation on the controller to disclose the data.

Article 6(1)(e) of the Gibraltar GDPR – 'Public interest'

A controller may be able to rely on 'public interest' as a lawful basis where the "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*" Section 10 of the DPA specifies the situations when this applies. These include, but are not limited to, where the processing is necessary for the administration of justice, or where it is necessary for the exercise of a function conferred on a person by an enactment or rule of law.

A controller may rely on this lawful basis when the controller itself is exercising official authority or carrying out a specific task in the public interest. A controller cannot rely on another controller's public tasks, functions or powers as the lawful basis for disclosure, including disclosing personal data to them, as this is not a clear and foreseeable use of the information.

Article 6(1)(f) of the Gibraltar GDPR – 'Legitimate interests'

In some circumstances it may be appropriate for a controller to rely on the 'legitimate interests' lawful basis. This relates to processing that is necessary for the legitimate interests pursued by a controller or by a third party, and where these do not outweigh the interests or fundamental rights and freedoms of the individuals whose personal data is being processed. For example, a controller might have a legitimate interest in disclosing personal data of an individual suspected of an offence with a Competent Authority to ensure that they have all the necessary information for a proper and fair investigation.

Notwithstanding, in relation to this lawful basis and processing undertaken by public authorities, the provision itself states that *"[p]oint (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks"*.

It is the Information Commissioner's view that a public authority ("Disclosing Party"), that is looking to disclose personal data to a competent authority ("Receiving Party"), cannot rely

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

on 'legitimate interests' where the Disclosing Party is performing their own public function. This is because Article 6 specifically states that legitimate interests "*shall not apply to processing carried out by public authorities in the performance of their tasks*". However, the Disclosing Party may rely on legitimate interests when the disclosure is not specifically related to their own public function.

A public authority may be able to rely on the legitimate interests of the Receiving Party as a third party, even if such legitimate interests are based on the Receiving Party's public function.

Further to the above, a controller may be able to rely on 'vital interests' (Article 6(1)(d) of the Gibraltar GDPR) as a lawful basis if it deems the disclosure necessary to protect someone's life. However, this lawful basis is only applicable in specific circumstances where an individual's life is at risk.

In this respect, Recital 46 of the Gibraltar GDPR specifies that the *"processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person."* However, "*processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis."*

4.2 Special Categories of Personal Data

Article 9(1) of the Gibraltar GDPR defines special categories of personal data as data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

Where a controller intends to disclose special category data to a Competent Authority, the controller must identify a lawful basis under Article 6(1) of the Gibraltar GDPR and a specific condition under Article 9(2) of the Gibraltar GDPR.

There are 10 conditions for the processing of special category data. However, if a controller wants to disclose said data for the prevention or detection of unlawful acts, the most likely applicable condition will be Article 9(2)(g) of the Gibraltar GDPR, in conjunction with section 12(3) of the DPA and paragraph 10 in Part 2 of Schedule 1 of the DPA:

- Article 9(2)(g) of the Gibraltar GDPR provides for processing that is "*necessary for reasons of substantial public interest, on the basis of Gibraltar law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".*
- Section 12 of the DPA provides the following –

  "*(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the Gibraltar GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)-*

(a) point (b) (employment, social security and social protection);
(b) point (g) (substantial public interest)

[…]

(3) The processing meets the requirement in point (g) of Article 9(2) of the Gibraltar GDPR for a basis in Gibraltar law only if it meets a condition in Part 2 of Schedule 1."

- Paragraph 10 in Part 2 of Schedule 1 of the DPA (i.e. "*Preventing or detecting unlawful acts*") provides that –

"*This condition is met if the processing-*
(a) is necessary for the purposes of the prevention or detection of an unlawful act;
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes; and
(c) is necessary for reasons of substantial public interest."

The term "*substantial public interest*" is not defined in the Gibraltar GDPR or DPA. However, the public interest can be taken to cover a wide range of values and principles relating to the public good, or what is in the best interests of society.

Substantial public interest means the public interest needs to be real and of substance. Given the inherent risks of special category data, it is not enough for a controller to make a vague or generic public interest argument. A controller should make specific arguments about the concrete wider benefits for the processing of data. For example, a controller should consider how the processing of data benefits the public in terms of both depth (i.e. how much benefit will be achieved from the processing) and breadth (i.e. the number of individuals who will benefit from the processing).

Further, a controller should ensure that the processing (i.e. disclosure) is reasonable, justified and substantiated. In this regard, a controller should demonstrate how the overall purpose of processing (i.e. the disclosure) has substantial public interest benefits, that the processing under the relevant condition is necessary for that purpose, and that it complies with the 'data minimisation' principle at Article 5(1)(c) of the Gibraltar GDPR.

Additionally, a controller should note that many of the conditions under Part 2 of Schedule 1 of the DPA require them to have an 'appropriate policy document' in place. However, this is not the case when a controller relies on the condition at paragraph 10 of Schedule 1 of the DPA for the disclosure of special category data to a Competent Authority.[8]

The decision and reasoning to rely on a specific condition under Article 9(2) of the Gibraltar GDPR should be documented by a controller, in order to demonstrate compliance and accountability[9].

[8] See paragraph 10(2) of Schedule 1 of the DPA.

[9] Articles 5(1)(2) and 24(1) of the Gibraltar GDPR, and where relevant, Article 30 of the Gibraltar GDPR.

4.3 Criminal Convictions and Offences Data

Article 10(1) of the Gibraltar GDPR refers to the processing of personal data relating to criminal convictions and offences **("Criminal Offence Data")**. Criminal Offence Data includes personal data about criminal convictions and offences[10], or related security measures[11].

Where a controller intends to disclose Criminal Offence Data, the controller must identify a lawful basis under Article 6(1) of the Gibraltar GDPR and as per Article 10(1) of the Gibraltar GDPR –

- be able to rely on official authority[12] (for example, some public authorities have specific roles which give them authority to process Criminal Offence Data); or
- be authorised by Gibraltar law, namely the provisions in Part 1, 2 or 3 of Schedule 1 of the DPA.

After identifying a lawful basis under Article 6 of the Gibraltar GDPR (for example Article 6(1)(f) of the GDPR), when disclosing data to law enforcement, the most likely applicable condition to satisfy Article 10 of the Gibraltar GDPR will be paragraph 10 of Schedule 1 of the DPA (identified in the foregoing in relation to the processing of special categories of personal data). Unlike special category data, there is no need to explicitly demonstrate that the disclosure of Criminal Offence Data is necessary for reasons of substantial public interest. This is because paragraph 36 of Schedule 1 of the DPA removes this requirement for Criminal Offence Data.

Further, when relying on paragraph 10 of Schedule 1, it would not be necessary for the controller to have an appropriate policy document in place, which is a requirement when a controller relies on a condition in Part 2 of Schedule 1 of the DPA.

Notwithstanding the above, a controller must document the condition being relied on for the processing of Criminal Offence Data, including its reasoning, to demonstrate compliance and accountability[13].

4.4 Data Protection Principles and Data Subject Rights

Data controllers must comply with all the principles relating to the processing of personal data under Article 5(1) of the Gibraltar GDPR and should have appropriate and effective

[10] This covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data 'relating to' criminal convictions and offences. For example, it can also cover suspicion or allegations of criminal activity.

[11] The Gibraltar GDPR does not define 'related security measures'. However, this is likely to include personal data about penalties, conditions or restrictions placed on an individual as part of the criminal justice process, or civil measures which may lead to a criminal penalty if not followed. Examples may include police cautions, bail conditions, restraining orders, information about probation or parole, etc. Civil proceedings and orders made as a result would not usually fall within 'related security measures' unless the penalty for non-compliance carries with it a criminal sanction.

[12] Public bodies or private bodies vested with public sector tasks, may have 'official authority' laid down by law to process criminal offence data. This official authority may derive from either common law or statute. The public body is responsible for identifying the specific law that gives them the official authority to process criminal offence data.

[13] Articles 5(1)(2) and 24(1) of the Gibraltar GDPR, and where relevant, Article 30 of the Gibraltar GDPR.

measures in place to demonstrate compliance. Where a controller receives a request for personal data from a Competent Authority, it should be particularly prudent in regard to the following principles and data subject rights:

Article 5(1)(c) of the Gibraltar GDPR – 'Data minimisation'

Article 5(1)(c) of the Gibraltar GDPR refers to the 'data minimisation' principle, which requires data controllers to process personal data that is "*adequate, relevant and limited to what is necessary in relation to the purposes for which there are processed*".

To comply with this principle, a controller should only provide personal data that is adequate, relevant and limited to the purpose of disclosure. How much personal data is necessary will depend on the circumstances of the case.

A controller must be satisfied that the personal data requested by a Competent Authority is necessary for said authority to fulfil its statutory functions for the law enforcement purposes. A Competent Authority should explain and provide reasons as to why it needs the data held by a controller. Further, a controller must only disclose personal data that is limited to what is requested and what is reasonable. For example, if a controller receives a court order to disclose personal data, the court order should detail what personal data is necessary for the investigation and what data should be disclosed.

If a controller intends to disclose personal data to a Competent Authority on a systematic basis (i.e. routine data sharing), it should have measures in place to control the data sharing and implement a data sharing agreement to ensure compliance with the Gibraltar GDPR and DPA[14].

Article 5(1)(b) of the Gibraltar GDPR – 'Purpose limitation'

The 'purpose limitation' principle at Article 5(1)(b) of the Gibraltar GDPR stipulates that personal data must be collected for a specified, explicit and legitimate purpose, and not further processed in a manner that is incompatible with said purpose.

Therefore, if a controller's original purpose for the processing of personal data included disclosure to a Competent Authority, then the lawful basis relied on should reflect said purpose. For example, if a controller installed a CCTV system for the purpose of the prevention and detection of crime, it is likely that the controller intends to disclose evidence of criminal activity with a law enforcement authority such as the police.

However, if a controller does not envisage disclosing personal data to a Competent Authority, then disclosing the data may result in its processing for a new purpose. For example, this may be the case where a controller processes employee data for HR purposes and then receives a request for said data from a law enforcement authority as part of an investigation into suspected criminal activity.

In this regard, it is important to note that a controller may only process personal data for a new purpose, which it did not originally anticipate, if -

- the new purpose is compatible with the original purpose;
- it obtains the individual's explicit consent for the new purpose; or

[14] Please see the Information Commissioner's "Data Sharing Code of Practice" available here: https://www.gra.gi/data-protection/codes-of-practice.

- it can identify a clear legal provision which requires or allows the new processing in the public interest.

If the new purpose of processing is compatible with the original purpose, the controller may not need a new lawful basis to further process the data. However, this will not be the case where the controller has relied on consent, and in such circumstances, it will be required to obtain fresh consent from individuals for the new purpose of processing[15].

Notwithstanding the above, a controller may be exempt from the 'purpose limitation' principle if one of the exemptions available under Schedules 2 and/or 3 of the DPA[16] apply. If a controller can rely on an exemption, it will not need to consider whether the disclosure of personal data to a Competent Authority is compatible with the original purpose of processing. However, a controller will still have to identify a lawful basis for any disclosure of data to a Competent Authority. A controller must carefully consider what lawful basis is most appropriate in each case and should document the lawful basis relied on to demonstrate compliance and accountability[17].

Articles 13 and 14 of the Gibraltar GDPR – 'The right to be informed'

The Gibraltar GDPR requires data controllers to be transparent with individuals regarding the processing of their personal data. Articles 13 and 14 of the Gibraltar GDPR specify what information individuals should be provided with when a controller processes their personal data. This information includes, amongst other things, the purposes of the processing, the lawful basis for the processing and the recipients or categories of recipients of personal data.

However, as noted above, there are provisions which may exempt controllers from providing individuals with information concerning the disclosures made to Competent Authorities, as required by Articles 13 and 14 of the Gibraltar GDPR[18].

Where an exemption is relied on, controllers must be prepared to justify their decision to apply the relevant exemption. The Information Commissioner recommends that any decisions to apply an exemption are taken at an appropriate senior level and that the reasoning for the decision is documented. Controllers should also seek advice from their Data Protection Officer, where one has been appointed[19].

Paragraph 2 of Schedule 2 of the DPA – 'Crime and taxation: general exemption'

One of the most relevant provisions exempting controllers from the above-mentioned obligations under the Gibraltar GDPR is set out under Paragraph 2 of Schedule 2 of the DPA.

---

[15] Please see the Information Commissioner's Guidance Note, "(6) Identifying the 'Lawful Basis'" and "(13) Guidance on Consent" available here: https://www.gra.gi/data-protection/guidance.

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

[17] Articles 5(1)(2) and 24(1) of the Gibraltar GDPR, and where relevant, Article 30 of the Gibraltar GDPR.

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

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

This exemption can apply if a controller is sharing personal data with a Competent Authority for any one of the following purposes -

- to prevent or detect crime;
- to apprehend or prosecute offenders; or
- to assess or collect a tax, duty or similar imposition.

Further, it exempts a controller from the Gibraltar GDPR's provisions on individuals' data protection rights[20], such as -

- the right to be informed (described above);
- all the other individual rights, except rights related to automated individual decision-making, including profiling;
- notifying individuals of personal data breaches[21];
- the lawfulness, fairness and transparency principle[22], except the requirement for processing to be lawful;
- the purpose limitation principle (described above); and
- all the other principles, but only so far as they relate to the right to be informed and the other individual rights.

However, it is not a blanket exemption. It applies only to the extent that complying with these provisions would be **likely to prejudice** the purposes listed above. If a controller can comply with the obligations under the Gibraltar GDPR without causing prejudice, it must do so.

Further, to comply with accountability obligations, a controller must be able to -

- explain the nature of the prejudice to the purpose or purposes listed above; and
- show a direct causal link between compliance and the prejudice to the purpose or purposes.

It is important to note that the potential prejudice must be real and substantial rather than just a remote possibility. A common example might be where complying with an individual's rights could prejudice the purposes of preventing or detecting crime by alerting them to the fact that a controller has shared their personal data with the police as part of an investigation.

4.5 Other Considerations

In addition to other obligations under the Gibraltar GDPR and the DPA, relating to the general processing of personal data, when disclosing personal data to Competent Authorities, controllers should -

- process personal data fairly[23];
- ensure the accuracy of the personal data being disclosed[24];

[20] Articles 13-21 of the Gibraltar GDPR.

[21] Article 34 of the Gibraltar GDPR.

[22] Article 5(1)(a) of the Gibraltar GDPR.

[23] Article 5(1)(a) of the Gibraltar GDPR.

[24] Article 5(1)(d) of the Gibraltar GDPR.

- ensure appropriate security measures are in place[25];
- carry out a Data Protection Impact Assessment beforehand if the disclosure is likely to result in a high risk[26];
- only retain personal data for as long as necessary[27].

5. LAW ENFORCEMENT AUTHORITIES

Where a law enforcement authority wants to disclose personal data to another law enforcement authority, for law enforcement purposes, it will have to comply with the same rules governing the disclosure of personal data between a data controller and a Competent Authority, as noted in section 4 above.

The Gibraltar GDPR and DPA do not prevent a law enforcement authority from disclosing personal data to another law enforcement authority for further processing under Part III of the DPA.[28] However, any disclosure of personal data will still need to be necessary, proportionate and appropriate. Further, if a law enforcement authority processes personal data under the Gibraltar GDPR and Part II of the DPA, it may reuse said data for further processing under Part III of the DPA if it is a Competent Authority for those purposes. However, it will still need to identify a lawful basis, and where relevant, a condition for the processing of special category or Criminal Offence Data, and comply with other data protection requirements.

[25] Articles 5(1)(f) and 32 of the Gibraltar GDPR. Disclosures of special category data or data relating to criminal convictions and offences require more protection and a higher level of security. Please see the the Information Commissioner's Guidance Note, "(18) Guidance on Data Security" available here: https://www.gra.gi/data-protection/guidance.

[26] Articles 35 and 36 of the Gibraltar GDPR. Please see the Information Commissioner's Guidance Note, "(4) Data Protection Impact Assessments'" available here: https://www.gra.gi/data-protection/guidance.

[27] Article 5(1)(e) of the Gibraltar GDPR.

[28] See Chapter 2 of Part III of the DPA for the relevant data protection principles. See Chapter 3 of Part III of the DPA for the relevant data subject rights, including duties concerning the provision of information. See Chapter 4 of Part III of the DPA for relevant data controller and data processor obligations.

IMPORTANT NOTE

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

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