GRA
GIBRALTAR REGULATORY AUTHORITY

(23) The Rights of Individuals under the Gibraltar GDPR

Guidance on the Gibraltar General Data Protection Regulation

28 January 2021

Guidance Note IR23/20

FOREWORD

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

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

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

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

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

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

SUMMARY

This document provides detailed guidance on the rights of individuals in relation to their personal data, in accordance with the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR"). It also provides information in respect of the Data Protection Act 2004 (the "DPA") and individuals' rights in respect of the processing by 'Competent Authorities' for law enforcement purposes, as defined in the DPA.

The rights of individuals under the Gibraltar GDPR and/or the DPA include the following:

- Articles 13 and 14 - The right to be informed (section 53 of the DPA).
- Article 15 - The right of access (section 54 DPA).
- Article 16 - The right to rectification (section 55 of the DPA).
- Article 17 - The right to erasure (section 56 of the DPA).
- Article 18 - The right to restrict processing (section 56 of the DPA).
- Article 20 - The right to data portability.
- Article 21 - The right to object.
- Article 22 - Rights in relation to automated decision making and profiling (sections 58 and 59 of the DPA).

When an individual submits a request to exercise one of their above-listed rights, the relevant organisation must be able to identify such request, and comply with the request without undue delay and at the latest within one month. The position differs slightly with regards the right to be informed.

If an organisation refuses to comply with a request, they must inform the individual without undue delay and within one month of receipt of the request, including: the reasons why they are not taking action; the individual's right to make a complaint to the Information Commissioner's office; and the individual's ability to seek to enforce their right through a judicial remedy.

If a request is considered excessive or manifestly unfounded, or if an exemption (as set out within the Gibraltar GDPR and/or the DPA) applies, an organisation can refuse to comply with a request (wholly or partly). Organisations should look at each exemption carefully to see how it applies to a particular request.

Organisations may also ask for more information prior to deciding whether or not to action a request, but this should be necessary and proportionate in the circumstances. In most cases, organisations cannot charge a fee to action a request. In limited circumstances, they are able to charge a "reasonable fee" to cover administration costs.

CONTENTS

1. ACKNOWLEDGMENTS

Where appropriate, Gibraltar's Information 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 the UK's Information Commissioner's Office, and in particular their guidance on 'Individual Rights'[1].

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/# - webpages last accessed on 21st January 2021.

2. INTRODUCTION

In this Guidance Note, the Gibraltar Regulatory Authority as the Information Commissioner[2] provides guidance on the rights of individuals under the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR") and the Data Protection Act 2004 (the "DPA"), in relation to the processing of their personal data.

As detailed below, individuals are able to submit requests to organisations if they wish to exercise their rights in respect of personal data pertaining to them, that is being processed by an organisation.

This document aims to assist individuals in understanding these rights, by describing each right and providing key procedural information in respect of each. The guidance is equally useful for organisations, to assist them in determining how best to process personal data to ensure the rights afforded to individuals under applicable data protection legislation are upheld.

The document is divided into sections, providing guidance on how organisations can identify an individual's request to exercise their rights, as well as describing the timeframes in which the organisation must respond to any such requests. It also provides information on how an organisation can refuse to action these requests in certain circumstances.

Further information on whether organisations can charge a fee or request identification from individuals submitting requests is also provided.

There are some distinctions with regards the handling of rights by "*Competent Authorities*"[3] when these relate to the processing of personal for "*Law Enforcement Purposes*",[4] which falls outside the scope of the Gibraltar GDPR and is instead governed by Part 3 of the DPA. Information relating to such circumstances is provided within footnotes throughout the document. On some occasions, guidance is provided in the main body of the document. It is important to note that the right of access (see section 4 below), and the rights to rectification (see section 5 below), erasure (see section 6 below) and restriction (see section 7 below) do not apply to the processing of 'relevant personal data'[5] in the course of a criminal investigation or criminal proceedings.[6]

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

[3] Section 39 and Schedule 7 of the DPA.

[4] Section 40 of the DPA.

[5] 'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority - Section 52(4) of the DPA.

[6] Section 52(3) of the DPA.

3. ARTICLES 13 AND 14 - THE RIGHT TO BE INFORMED

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

Articles 13 and 14 of the Gibraltar GDPR, specify what information individuals must be provided with when organisations process their personal data.[7] This is known as 'privacy information', and is usually provided in a Privacy Notice[8].

The following section outlines the key aspects in respect of the right to be informed. Ensuring an effective approach in this regard, can also help organisations to comply with other aspects of the Gibraltar GDPR, foster trust amongst individuals, and assist the organisation in obtaining more useful information from individuals. Getting this wrong can leave an organisation open to fines and may lead to reputational damage.

3.1. WHAT PRIVACY INFORMATION SHOULD ORGANISATIONS PROVIDE?

The table below summarises the key information organisations must provide individuals with.[9] This differs slightly depending on whether personal data is collected from the individual it relates to or whether it is obtained from another source.

What information needs to be provided?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of the organisation	✓	✓
The name and contact details of the organisation's representative	✓	✓
The contact details of their data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓

[7] See section 53 of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes. Please refer to section 3.6 below for further information on the responsibilities of Competent Authorities processing personal data for Law Enforcement Purposes that is relevant to this section.

[8] For more detailed guidance on Privacy Notices, please refer to Guidance Note (17) "Privacy Notice" on the Gibraltar Regulatory Authority's website.

[9] See also Guidance Note (17) "Privacy Notice" as referred to above.

The legitimate interests for the processing	✓	✓
The categories of personal data obtained	X	✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right for individuals to withdraw consent	✓	✓
The right of an individual to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data	X	✓
Details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	X
The details of the existence of automated decision-making, including profiling	✓	✓

Organisations must be upfront about their use of personal data and clearly explain their purpose(s) for using such data. They should inform individuals about any new uses of personal data before they commence processing for said new purpose(s), update their privacy information accordingly, and actively communicate this to individuals.

Importantly, if an organisation **shares** personal data with other organisations:

- They must provide relevant individuals with information about who they are giving the information to unless they are relying on an exception (see section 3.3 below) or an exemption (see section 13.1 below).

- They can inform individuals of the names of the relevant organisations or can provide them with the categories in which said organisations fall if this is more appropriate in the circumstances.

If the organisation obtains personal data from **publicly accessible sources**:

- They still have to provide privacy information to individuals, unless they are relying on an exception (see section 3.3 below) or an exemption (see section 13.1 below).

- They should be very clear with individuals about any unexpected or intrusive uses of their personal data, such as combining information about them from a number of different sources.

3.2. WHEN SHOULD ORGANISATIONS PROVIDE PRIVACY INFORMATION?

Privacy information must be provided to individuals **at the time the organisation obtains the data.**[10] When this is obtained from a source other than the individual it relates to, the organisation must provide the individual with privacy information[11]:

- **within a reasonable period** of obtaining the personal data and **no later than one month** after obtaining it;
- if the organisation uses the data to communicate with the individual, at the latest, when the **first communication** takes place; or
- if organisations envisage disclosure to someone else, at the latest, **when they disclose** the data.

3.3. ARE THERE ANY EXCEPTIONS?

When collecting personal data from individuals themselves, organisations do not need to provide them with any information they already have.[12]

When obtaining personal data from other sources, organisations will not need to provide individuals with privacy information if:[13]

- the individual already has the information;
- providing the information to the individual would be impossible or would involve a disproportionate effort, in which case the organisation must carry out a Data Protection Impact Assessment ("DPIA") to find ways to mitigate the risks of the processing;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- the organisation is required by law to obtain or disclose the personal data; or
- the organisation is subject to an obligation of professional secrecy regulated by law that covers the personal data.

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

[11] Article 14(3) of the Gibraltar GDPR.

[12] Article 13(4) of the Gibraltar GDPR.

[13] Article 14(5) of the Gibraltar GDPR.

3.4. HOW SHOULD ORGANISATIONS DRAFT THEIR PRIVACY INFORMATION?

Organisations must proactively provide privacy information to individuals whose personal data they process. This requirement can be met by including the information on a website, but individuals must be made aware of it, and the information must be easily accessible.

An information audit or data mapping exercise can help organisations find out what personal data they hold and what they do with it. Organisations should think about the intended audience for their privacy information and put themselves in the audience's position.

In accordance with Article 12 of the Gibraltar GDPR, organisations must provide information in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

If an organisation collects or obtains children's personal data, they must take particular care to ensure that the information they provide them with is appropriately written, using clear and plain language.[14]

It is good practice for organisations to carry out user testing on their draft privacy information to get feedback on how easy it is to access and understand. They should also undertake regular reviews to check it remains accurate and up to date.

3.5. WHAT METHODS CAN BE USED TO PROVIDE PRIVACY INFORMATION?

There are a number of techniques that organisations can use to provide individuals with privacy information. They can use:

- **A layered approach** – short notices containing key privacy information, accompanied by additional layers of more detailed information.
- **Dashboards** – preference management tools that inform individuals how the organisation uses their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time the organisation collects individual pieces of information.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.

[14] Article 12(1) of the Gibraltar GDPR.

- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Organisations must consider the context in which they, as data controllers, are collecting personal data. It is good practice to use the same medium they use to collect personal data to deliver the privacy information. Using a combination of the above, and/or other relevant techniques, is often the most effective way to provide privacy information.

Example

An organisation uses artificial intelligence to make solely automated decisions about people with legal or similarly significant effects.

They should inform affected individuals about what information they use, why it is relevant and what the likely impact is going to be.

In such instances, the organisation may wish to consider using just-in-time notices and dashboards to keep individuals informed and let them control further uses of their personal data.

3.6. LAW ENFORCEMENT PROCESSING

Competent Authorities processing personal data for Law Enforcement Purposes must make the following information generally available to the public:[15]

- their identity and contact details;
- the contact details of their data protection officer, if applicable;
- the purposes of the processing;
- the individual's rights right of access (see section 4 below), rectification (see section 5 below), erasure (see section 6 below) and restriction (see section 7); and
- the right to lodge a complaint with the Information Commissioner and the relevant contact details.

They should supply, in specific cases, the following information to enable individuals to exercise their rights:[16]

- their legal basis for processing;
- the retention period or the criteria they used to determine the retention period;
- any recipient or categories of recipients of the personal data (including in third countries or international organisations); and

[15] Section 53(1) of the DPA.

[16] Section 53(2) of the DPA.

- any further information needed to enable individuals to exercise their rights, e.g. if information is collected without their knowledge.

The right to this information is a qualified right, subject to restrictions that prevent any prejudice to an ongoing investigation or compromise to operational techniques.

Example

A Competent Authority has a generic privacy notice on their website which covers basic information about the organisation, the purpose they process personal data for, a data subject's rights and their right to complain to the Information Commissioner.

They have received intelligence that an individual was present when a crime took place. On first interviewing this individual, they need to provide the generic information, as well as the further supporting information, to enable their rights to be exercised. They can only restrict the fair processing information they are providing if it will adversely affect the investigation they are undertaking.

Competent Authorities may restrict the provision of further information where it is necessary and proportionate to:[17]

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

They need to justify any restriction they apply as necessary and proportionate and apply it on a case-by-case basis. It is important to balance the rights of the individual against the harm disclosure would cause.

They must also inform the individual when this limitation is in place, explaining its existence and the reasons, unless providing this information itself would undermine the purpose of imposing the restriction. Regardless, they still need to inform the individual about the process of raising a complaint with the Information Commissioner or taking matters to court.[18]

Competent Authorities should keep a record of their decisions to rely on any restriction, and provide this reasoning to the Information Commissioner if required.[19]

[17] Section 53(4) of the DPA.

[18] Sections 53(5) and (6) of the DPA.

[19] Section 53(7) of the DPA.

4. ARTICLE 15 - THE RIGHT OF ACCESS

The right of access under Article 15 of the Gibraltar GDPR, commonly referred to as a subject access request ("SAR") or data subject access request ("DSAR"), gives individuals the right to obtain a copy of their personal data that is being processed by a particular organisation, as well as other supplementary information (as set out at Article 15(1) of the Gibraltar GDPR).[20] It helps individuals to understand how and why organisations are using their personal data, and to check the processing is being done lawfully.

For further guidance, on the right of access please refer to Guidance Note (15) "Right of Access" on the Gibraltar Regulatory Authority's website.

5. ARTICLE 16 - THE RIGHT TO RECTIFICATION

Under Article 16 of the Gibraltar GDPR, individuals have the right to have inaccurate personal data rectified[21].

An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing, and may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the Gibraltar GDPR (Article 5(1)(d)). Although an organisation may have already taken steps to ensure that the personal data was accurate when they obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

5.1. WHAT DO ORGANISATIONS NEED TO DO?

If an organisation receives a request for rectification, they should take reasonable steps to satisfy themselves that the data is accurate and to rectify the data if necessary. They should take into account the arguments and evidence provided by the data subject, and have a month to respond to the request (see section 12 below.)

What steps are reasonable will in particular depend on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort that should be put into checking its accuracy and, if necessary, taking steps to rectify it.

[20] See Section 54 of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes. Further, please refer to section 10 of Guidance Note (15) "The Right of Access" on the Gibraltar Regulatory Authority's website for further information on the responsibilities of Competent Authorities processing personal data for Law Enforcement Purposes that is relevant to this section.

[21] See section 55 and section 57(7) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

Organisations should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

Organisations may also take into account any steps they have already taken to verify the accuracy of the data prior to the challenge by the data subject.

5.2. WHEN IS DATA INACCURATE?

The Gibraltar GDPR does not give a definition of the term 'accuracy'. However, the DPA states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.[22]

5.3. WHAT SHOULD ORGANISATIONS DO ABOUT DATA THAT RECORDS A MISTAKE?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate, and should be kept. In such circumstances the fact that a mistake was made and the correct information, should also be included in the individual's data.

Example

A patient is diagnosed by a doctor as suffering from a particular illness or condition, but it is proved that this is not the case. It is likely that their medical records show both the initial diagnosis (even though it was later provided to be incorrect) and the final findings.

Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is clear in the record, it would be difficult to argue that the record is inaccurate and that it should be rectified.

5.4. WHAT SHOULD ORGANISATIONS DO ABOUT DATA THAT RECORDS A DISPUTED OPINION?

Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record clearly shows that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to argue that it is inaccurate and that it needs to be rectified.

[22] Section 2(1) of the DPA.

5.5. WHAT SHOULD ORGANISATIONS DO WHILST THEY ARE CONSIDERING THE ACCURACY OF PERSONAL DATA?

Under Article 18 of the Gibraltar GDPR, an individual has the right to request the restriction of processing of their personal data where they contest its accuracy and whilst an organisation is verifying this (see section 7 below).

As a matter of good practice, and where circumstances allow, organisations should restrict the processing of the personal data in question whilst they are verifying its accuracy, whether or not the individual has exercised their right to restriction.

5.6. WHAT SHOULD ORGANISATIONS DO IF THEY ARE SATISFIED THAT THE DATA IS ACCURATE?

As the data controller, an organisation should let the individual know if they are satisfied that the personal data is accurate, and inform them that they will not be amending said data. They should explain their decision and inform the individual of their right to make a complaint to the Information Commissioner's Office and their ability to seek to enforce their rights through a judicial remedy (see section 13 below).

It is also good practice for the organisation to place a note on their system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

5.7. DO OTHER ORGANISATIONS NEED TO BE INFORMED OF ANY RECTIFIED PERSONAL DATA?

If an organisation has disclosed the personal data to others, they must contact each recipient and inform them of the rectification or completion of the personal data, unless this proves impossible or involves disproportionate effort. If asked to, they must also inform the individual about these recipients.[23]

The Gibraltar GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed.[24] The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

[23] Article 19 of the Gibraltar GDPR. This obligation exists under section 57(9) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[24] Article 4(9) of the Gibraltar GDPR.

6. ARTICLE 17 - THE RIGHT TO ERASURE

Under Article 17 of the Gibraltar GDPR, individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.[25] **Importantly, this right is not absolute and only applies in certain circumstances.**

6.1. WHEN DOES THE RIGHT TO ERASURE APPLY?

As detailed in Article 17(1) of the Gibraltar GDPR, individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which the organisation originally collected or processed it for;
- the organisation is relying on consent as their lawful basis for holding the data, and the individual withdraws their consent;
- the organisation is relying on the legitimate interests lawful basis as their basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the organisation is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the organisation has processed the personal data unlawfully (i.e. in breach of Article 5(1)(a) of the Gibraltar GDPR) [26];
- the organisation has to do it to comply with a legal obligation; or
- the organisation has processed the personal data to offer information society services to a child.

6.2. HOW DOES THE RIGHT TO ERASURE APPLY TO CHILDREN?

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection under the Gibraltar GDPR of children's information, especially in online environments.

[25] See section 56 of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[26] Section 44(1) of the DPA.

If an organisation processes data collected from children, they should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet.

This remains the case when the data subject is no longer a child, because, as a child at the time of consent, they may not have been fully aware of the risks involved in the processing.

6.3. DOES AN ORGANISATON HAVE TO INFORM OTHER ORGANISATIONS ABOUT THE ERASURE OF PERSONAL DATA?

The Gibraltar GDPR specifies two circumstances in which an organisation, as data controller, should inform other organisations about the erasure of personal data:

- the personal data has been disclosed to the other organisation;[27] or
- the personal data has been made public in an online environment (e.g. on social networks, forums or websites).[28]

If an organisation has disclosed the personal data to others, they must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the organisation must also inform the individuals about these recipients.

Example

A recruitment agency processes an individual's personal data, and such data has been disclosed to potential employers. They receive a request from the individual to rectify personal data in relation to the qualifications held on record for that individual.

The recruitment agency should contact the employers and inform them that they have rectified such personal data.

Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of, that data. When deciding what steps are reasonable, organisations should take into account available technology and the cost of implementation.

6.4. DO ORGANISATIONS HAVE TO ERASE PERSONAL DATA FROM THEIR BACKUP SYSTEMS?

If a valid erasure request is received and no exemption applies (see section 13.1 below), then the organisation will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on the particular circumstances, the retention policy of the

[27] Article 19 of the Gibraltar GDPR. This obligation exists under section 57(9) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[28] Article 17(2) of the Gibraltar GDPR.

organisation (particularly in the context of its backups), and the technical mechanisms that are available to the organisation.

The organisation must be clear with individuals as to what will happen to their personal data when their erasure request is fulfilled, including in respect of backup systems. It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time, until it is overwritten.

The key is to put the backup data 'beyond use', even if it cannot be immediately overwritten. Organisations must ensure that they do not use the data within the backup for any other purpose, i.e. that the backup is simply held on their systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific.

6.5. WHEN DOES THE RIGHT TO ERASURE NOT APPLY?

The right to erasure does not apply if processing is necessary for one of the following reasons:[29]

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

Article 17(3)(c) of the Gibraltar GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services.

[29] Article 17(3) of the Gibraltar GDPR.

7. ARTICLE 18 - THE RIGHT TO RESTRICT PROCESSING

Article 18 of the Gibraltar GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances.[30] This means that an individual can limit the way in which an organisation uses their data. This is an alternative to requesting the erasure of their data under Article 17 of the Gibraltar GDPR.

In most cases the organisation will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time depending on the circumstances.

7.1. WHEN DOES THE RIGHT TO RESTRICT PROCESSING APPLY?

Individuals have the right to request organisations to restrict the processing of their personal data in the following circumstances: [31]

- the individual contests the accuracy of their personal data and the organisation is verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of Article 5(1)(a) of the Gibraltar GDPR), and the individual opposes erasure and requests restriction instead;
- the organisation no longer needs the personal data but the individual needs the organisation to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to the organisation processing their data under Article 21(1) of the Gibraltar GDPR, and that organisation is considering whether their legitimate grounds override those of the individual.

[32]Although the right to restrict processing is distinct from the right to rectification and the right to object, there are close links between them, as follows:

- if an individual has challenged the accuracy of their data and asked for the organisation to rectify it (see section 5 above), they also have a right to request that the organisation restrict the processing while they consider the rectification request; or

[30] See sections 56 (2)-(4) of the DPA and 57(10) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes. Please refer to section 7.6 below for further information on the responsibilities of Competent Authorities processing personal data for Law Enforcement Purposes that is relevant to this section.

[31] Article 18(1) of the Gibraltar GDPR.

[32] Section 44(2) of the DPA

- if an individual exercises their right to object under Article 21(1) of the Gibraltar GDPR (see section 9 below), they also have a right to request that the organisation restrict processing while they consider the objection request.

Therefore, as a matter of good practice, organisations should automatically restrict the processing whilst they are considering its accuracy or the legitimate grounds for processing the personal data in question.

7.2. HOW CAN ORGANISATIONS RESTRICT PROCESSING?

Organisations need to have processes in place that enable them to restrict the processing of personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data.[33] Therefore, organisations should use methods of restriction that are appropriate for the type of processing they are carrying out.

The Gibraltar GDPR suggests a number of different methods that could be used to restrict data, such as:[34]

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that organisations consider how they store personal data that they no longer need to process but that the individual has requested be restricted (effectively requesting that the organisation do not erase the data).

If they are using an automated filing system, the organisation needs to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. They should also note on their system that the processing of this data has been restricted.[35]

7.3. CAN ORGANISATIONS PROCESS RESTRICTED DATA?

Organisations must not process the restricted data in any way **except to store it** unless:[36]

- they have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or

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

[34] Recital 67 of the Gibraltar GDPR.

[35] Recital 67 of the Gibraltar GDPR.

[36] Article 18(2) of the Gibraltar GDPR.

- it is for reasons of important public interest.

7.4. DO ORGANISAITONS HAVE TO TELL OTHER ORGANISATIONS ABOUT THE RESTRICTION OF PERSONAL DATA?

Yes. Under Article 19 of the Gibraltar GDPR, if an organisation has disclosed the personal data in question to others, they must contact each recipient and inform them of the restriction of the personal data, unless this proves impossible or involves disproportionate effort. If asked to, they must also inform the individual about these recipients.[37]

7.5. WHEN CAN RESTRICTIONS BE LIFTED?

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and the organisation is investigating this;[38] or

- the individual has objected to the processing of their data by an organisation on the basis that it is necessary for the performance of a task carried out in the public interest,[39] or the purposes of their legitimate interests,[40] and the organisation is considering whether their legitimate grounds override those of the individual.[41]

Once the organisation has decided on the accuracy of the data, or whether the legitimate grounds override those of the individual, they may decide to lift the restriction. If they do this, they must inform the individual **before** they lift the restriction.[42]

As noted above, these two conditions are linked to the right to rectification (Article 16 of the Gibraltar GDPR) and the right to object (Article 21 of the Gibraltar GDPR). This means that, if an organisation is informing the individual that they are lifting the restriction (on the grounds that they are satisfied that the data is accurate, or that their legitimate grounds override those of the individual), they should also inform them of the reasons for their refusal to act upon their rights under Articles 16 and/or 21 of the Gibraltar GDPR. They will also need to inform the individuals of their right to make a complaint to the Information Commissioner's office, and their ability to seek a judicial remedy (see section 13 below).

[37] This obligation exists under section 57(9) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[38] Article 18(1)(a) of the Gibraltar GDPR.

[39] Article 6(1)(e) of the Gibraltar GDPR

[40] Article 6(1)(f) of the Gibraltar GDPR

[41] Article 18(1)(d) of the Gibraltar GDPR. Such objection to processing would be made under Article 21(1) of the Gibraltar GDPR.

[42] Article 18(3) of the Gibraltar GDPR.

7.6. LAW ENFORCEMENT PROCESSING

Competent Authorities processing personal data for Law Enforcement Purposes are required to restrict the processing of personal data in two situations:

- If they must maintain personal data for the purposes of evidence.[43]
- If an individual contests the accuracy of personal data but it is not possible to be certain about its accuracy.[44]

Example

The local police force is investigating a suspect for benefit fraud. As part of this investigation, factually inaccurate personal data about the suspect (such as an age/ethnicity) has been received from a third party. However, this inaccurate record needs to be retained as evidence to account for how the authority first carried out the investigation and the source of this information. They should not erase or rectify this information, but restrict it as it forms evidence against the suspect. They should not process this inaccurate personal data for any other purpose.

If restriction is based on the latter, they should inform the individual before they lift the restriction.[45]

8. ARTICLE 20 - THE RIGHT TO DATA PORTABILITY

The right to data portability under Article 20 of the Gibraltar GDPR, gives individuals the right to receive personal data they provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmit this data directly to another controller.

For guidance, please refer to Guidance Note (5) "Data Portability" on the Gibraltar Regulatory Authority's website.

[43] See section 56(2) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[44] See section 56(3) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[45] See section 57(10) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

9. ARTICLE 21 - THE RIGHT TO OBJECT

Article 21 of the Gibraltar GDPR gives individuals the right, **in certain circumstances**, to object to the processing of their personal data. This effectively allows individuals to stop or prevent organisations from processing their personal data.

An objection may be in relation to all of the personal data an organisation holds about an individual or only to certain information. It may also only relate to a particular purpose for which the organisation are processing the data.

9.1. WHEN DOES THE RIGHT TO OBJECT APPLY?

Whether the right to object applies depends on an organisation's purposes for processing and their lawful basis for processing under Article 6 of the Gibraltar GDPR.

Importantly, individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:[46]

- a task carried out in the public interest; [47]
- the exercise of official authority vested in a data controller; [48] or
- an organisation's legitimate interests (or those of a third party). [49]

In these circumstances the right to object is not absolute.

If an organisation is processing data for scientific or historical research, or statistical purposes, the right to object is more limited. These various grounds are discussed further below.

9.1.1. DIRECT MARKETING

An individual can object to the processing of their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.[50]

[46] Article 21(1) of the Gibraltar GDPR.

[47] Article 6(1)(e) of the Gibraltar GDPR.

[48] Article 6(1)(e) of the Gibraltar GDPR.

[49] Article 6(1)(f) of the Gibraltar GDPR.

[50] Article 21(2) of the Gibraltar GDPR.

This is an absolute right and there are no exemptions or grounds for refusal.[51] Therefore, when an organisation receives an objection to processing for direct marketing, they must not process the individual's data for this purpose.

This does not however automatically mean that they need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

Example

An online gambling company is marketing its products to its clients when it receives a request for such marketing to cease from one individual, who wants to remain a customer.

The online gambling company should cease such processing, but would need to now include the individual's personal data on a list to ensure no more marketing is sent to that individual.

9.1.2. PROCESSING BASED UPON PUBLIC TASK OR LEGITIMATE INTERESTS

An individual can also object where an organisation is relying on one of the following lawful bases:[52]

- 'public task' (for the performance of a task carried out in the public interest),[53]
- 'public task' (for the exercise of official authority vested in a data controller), [54]or
- legitimate interests.[55]

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

In these circumstances this is not an absolute right, and an organisation can refuse to comply if:[56]

- **they can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or**
- **the processing is for the establishment, exercise or defence of legal claims.**

If the organisation is deciding whether they have compelling legitimate grounds which override the interests of an individual, they should consider the reasons why the individual has objected

[51] Article 21(3) of the Gibraltar GDPR.

[52] Article 21(1) of the Gibraltar GDPR.

[53] Article 6(1)(e) of the Gibraltar GDPR.

[54] Article 6(1)(e) of the Gibraltar GDPR.

[55] Article 6(1)(f) of the Gibraltar GDPR.

[56]Article 21(1) of the Gibraltar GDPR.

to the processing of their personal data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (e.g. the processing is causing them financial loss), the grounds for their objection will have more weight.

In making a decision on this, the **organisation needs to balance the individual's interests, rights and freedoms with their own legitimate grounds.** During this process they should remember that **the responsibility is for them to be able to demonstrate that their legitimate grounds override those of the individual.**

If an organisation is satisfied that they do not need to comply with the request, they should let the individual know. Organisations should explain their decision and inform the individual of their right to make a complaint to the Information Commissioner's office, and their ability to seek to enforce their rights through a judicial remedy (see section 13 below.)

9.1.3. RESEARCH PURPOSES

Where organisations are processing personal data for scientific or historical research, or statistical purposes, the right to object is more restricted.

Article 21(6) of the Gibraltar GDPR states that where personal data is processed for scientific or historical research purposes or statistical purposes (pursuant to Article 89(1) of the Gibraltar GDPR), the data subject has the right to object to processing of personal data concerning him or her on grounds relating to his or her personal situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Effectively this means that if an organisation is processing personal data for these purposes and they have appropriate safeguards in place (e.g. data minimisation and pseudonymisation where possible), **the individual only has a right to object if the lawful basis for processing is:**

- **Relating to a 'public task' on the basis that it is necessary for the exercise of official authority vested in the organisation**[57]**, or**
- **legitimate interests.**[58]

The individual does not however have a right to object if the lawful basis for processing is relating to a 'public task' on the basis that it is necessary for the performance of a task carried out in the public interest.

Article 21(6) of the Gibraltar GDPR therefore differentiates between the two parts of the public task lawful basis (i.e. performance of a task carried out in the public interest **or** in the exercise of official authority vested in the organisation).[59]

This may cause difficulties if the organisation is relying on the public task lawful basis for processing. It may not always be clear whether they are carrying out the processing solely as a

[57] Article 6(1)(e) of the Gibraltar GDPR.

[58] Article 6(1)(f) of the Gibraltar GDPR.

[59] Article 6(1)(e) of the Gibraltar GDPR.

task in the public interest, or in the exercise of official authority. Indeed, it may be difficult to differentiate between the two.

As such, it is good practice for an organisation who is relying upon the public task lawful basis that receives an objection, to consider the objection on its own merits and go on to consider the steps outlined in the next paragraph, rather than refusing it outright. If they do intend to refuse an objection on the basis that they are carrying out research or statistical work solely for the performance of a public task carried out in the public interest, the organisation should be clear in their privacy notice that they are only carrying out this processing on this basis.

If the organisation does receive an objection, they may be able to continue processing, if they can demonstrate that they have a compelling legitimate reason or the processing is necessary for legal claims.[60] Organisations need to go through the steps outlined in the previous section to demonstrate this.

As noted above, **if an organisation is satisfied that they do not need to comply with the request, they should inform the individual** (see section 13 below).

9.2. DO ORGANISATIONS NEED TO INFORM INDIVIDUALS ABOUT THE RIGHT TO OBJECT?

The Gibraltar GDPR is clear that organisations must inform individuals of their right to object at the latest at the time of their first communication with them where:[61]

- they process personal data for direct marketing purposes; or
- their lawful basis for processing is:
    - public task (for the performance of a task carried out in the public interest),
    - public task (for the exercise of official authority vested in them), or
    - legitimate interests.

If one of the above applies, the organisation should explicitly bring the right to object to the individual's attention. They should present this information clearly and separately from any other information.[62]

If they are processing personal data for research or statistical purposes, the organisation should include information about the right to object (along with information about the other rights of the individual) in their privacy notice (see section 3 above).

[60] Article 21(1) of the Gibraltar GDPR.

[61] Article 21(4) of the Gibraltar GDPR.

[62] Article 21(4) of the Gibraltar GDPR.

9.3. DOES THE ORGANISATION ALWAYS HAVE TO ERASE THE PERSONAL DATA TO COMPLY WITH AN OBJECTION?

Where an organisation has received an objection to the processing of personal data and they have no grounds to refuse, they need to stop or not begin processing the data.

This may mean that they need to erase personal data as the definition of processing under the Gibraltar GDPR is broad and includes storing personal data. However, as noted above, this will not always be the most appropriate action to take.

Erasure may not be appropriate if an organisation processes the data for other purposes, as they need to retain the data for those purposes.

10. ARTICLE 22 - RIGHTS RELATED TO AUTOMATED DECISION-MAKING INCLUDING PROFILING

Automated individual decision-making is a decision made by automated means without any human involvement, and is regulated by Article 22 of the Gibraltar GDPR.[63]

Example

A bank decides to issue loans to customers using a program that decides based on information the customer inputs about themselves, without human involvement. This would constitute automated decision making.

Automated individual decision-making does not have to involve profiling, although it often will do.

Article 4(4) of the Gibraltar GDPR states that profiling is *"any form of automated processing of personal data that consists of the use of personal data to evaluate certain personal aspects relating to a natural person"*. In particular it relates to analysing or predicting aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of personal data organisations might collect.

[63] See sections 58 and 59 of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals.

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about an individuals' preferences;
- predict their behaviour; and/or
- make decisions about them.

This can be very useful for organisations and individuals in many sectors, including healthcare, education, financial services and marketing.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The Gibraltar GDPR includes provisions that are designed to address these risks.

10.1. WHAT DOES THE GIBRALTAR GDPR SAY ABOUT AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING?

Article 22 of the Gibraltar GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

Article 22(1) of the Gibraltar GDPR states that the data subject has the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects on them or significantly affects them.

For something to be solely automated there must be no human involvement in the decision-making process.

'Legal or similarly significant effects' are not defined in the Gibraltar GDPR, but are considered to be where the decision has a serious negative impact on an individual.

A legal effect can be considered as something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

10.2. WHEN CAN ORGANISATIONS CARRY OUT THIS TYPE OF PROCESSING?

Organisations can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:[64]

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If an organisation is using special category personal data, they can **only** carry out processing described in Article 22(1) of the Gibraltar GDPR if:[65]

- they have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

10.3. WHAT ELSE DO ORGANISATIONS NEED TO CONSIDER?

Because this type of processing is **considered to be high-risk, the Gibraltar GDPR requires organisations to carry out a DPIA** to show that they have identified and assessed what those risks are and how they will address them. For more information, please refer to Guidance Note (4) "Data Protection Impact Assessments", available on the Gibraltar Regulatory Authority's website.

As well as restricting the circumstances in which organisations can carry out solely automated individual decision-making (as described in Article 22(1) of the Gibraltar GDPR), the Gibraltar GDPR also[66]:

- requires organisations to give individuals specific information about the processing;
- obliges them to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision.

These provisions are designed to increase individuals' understanding of how the organisation might be using their personal data.

[64] Article 22(2) of the Gibraltar GDPR.

[65] Article 22(4) of the Gibraltar GDPR.

[66] Recital 71 of the Gibraltar GDPR.

The organisation must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual; [67]
- use appropriate mathematical or statistical procedures; [68]
- ensure that individuals can obtain human intervention, express their point of view; and obtain an explanation of the decision and challenge it; [69]
- put appropriate technical and organisational measures in place, so that they can correct inaccuracies and minimise the risk of errors; [70]
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects. [71]

10.4. WHAT IF ARTICLE 22 DOES NOT APPLY TO THE PROCESSING?

If Article 22 of the Gibraltar GDPR does not apply, then the organisation can continue to carry out profiling and automated decision-making. The organisation must still however comply with the Gibraltar GDPR principles as set out within Chapter 2 of the Gibraltar GDPR. They must for example identify and record their lawful basis for the processing and they also need to have processes in place so individuals can exercise their rights.

Individuals have a right to object to profiling in certain circumstances. Organisations must bring details of this right specifically to their attention (see section 9.1.1 above).

11. HOW CAN AN INDIVIDUAL MAKE A REQUEST?

The Gibraltar GDPR and DPA do not specify how to make a valid request in respect of the rights identified in Chapter 3 of the Gibraltar GDPR or Chapter 3 of Part III of the DPA as set out in sections 4 to 10 above. An individual can therefore make a request exercising any of these rights verbally or in writing, although it is recommended that requests be made in writing in order to ensure an audit trail.

[67] Articles 13(2)(f) and 14(2)(g) of the Gibraltar GDPR.

[68] Recital 71 of the Gibraltar GDPR.

[69] Recital 71 of the Gibraltar GDPR.

[70] Recital 71 of the Gibraltar GDPR.

[71] Recital 71 of the Gibraltar GDPR.

Requests can also be made to any part of an organisation and do not have to be to a specific person or contact point. Furthermore, a request does not need to mention the specific right, nor does it need to mention the Gibraltar GDPR, the DPA, or any specific legal provision, to be a valid request. As long as it is clear that the individual has invoked the right, the request will be valid.

This presents a challenge as any of the employees of an organisation could receive a valid verbal request. However, organisations have a legal responsibility to identify that an individual has made a request, and handle it accordingly. Organisations should therefore consider which of their staff regularly interact with individuals, and whether they may need specific training to identify a request under data protection legislation.

Additionally, it is good practice to have a policy for recording details of requests received, particularly those made by telephone or in person, and that a log be kept. As a matter of good practice, the organisation should also check with the requester that the request has been properly understood, as this can help avoid later disputes about how they have interpreted the request.

12. COMPLYING WITH A REQUEST

When an individual submits a request exercising one of their rights under Chapter 3 of the Gibraltar GDPR as set out in sections 4 to 10 above,[72] organisations in receipt of the request must **comply without undue delay and at the latest within one month of receipt of the request.** [73]

If the organisation is seeking to verify the requester's identity (see section 15 below), or is changing a fee in accordance with the provisions of the Gibraltar GDPR and/or DPA (see section 14 below), they must reply within one month of receipt of any information requested to confirm the requester's identity or the relevant fee.

Organisations should calculate the time limit from the day they receive the request (whether it is a working day or not), until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, they have until the next working day to respond.

[72] See section 57(1)(a), (2) and (9) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes. This is relevant for the rights under sections 5,6 and 7 above.

[73] Article 12(3) of the Gibraltar GDPR.

This means that the exact number of days they have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Organisations can extend the time to respond to a request by a further two months if the request is complex or a number of requests have been received from the individual. Organisations must let individuals know within one month of receiving their request and explain why the extension is necessary.

13. REFUSING TO COMPLY WITH A REQUEST

If an organisation seeks to refuse a request submitted by an individual exercising one of their rights under Chapter 3 of the Gibraltar GDPR as set out within sections 4 to 10 above,[74] the organisation must inform the individual without undue delay and within one month of receipt of the request of the following:[75]

- **the reasons they are not taking action;**
- **their right to make a complaint to the Information Commissioner's Office; and**
- **their ability to seek to enforce their right through a judicial remedy.**

The organisation should also provide this information if they request a reasonable fee or need additional information to identify the individual (see sections 14 and 15 below).

[74] Please see section 57(1)(b) and section 57(2)-(6) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes. This is relevant for the rights under sections 5,6 and 7 above.

[75] Article 12(4) of the Gibraltar GDPR.

13.1. DOES AN EXEMPTION APPLY?

If an exemption applies, an organisation can refuse to comply with a request (wholly or partly). Not all of the exemptions apply in the same way, and the organisation should look at each exemption carefully to see how it applies to a particular request. For more information on exemptions under applicable data protection legislation, please refer to Guidance Note (21) "Exemptions", available on the Gibraltar Regulatory Authority's website.

13.2. WHAT DOES MANIFESTLY UNFOUNDED MEAN?

An organisation can also refuse to comply with a request if it is:[76]

- manifestly unfounded; or
- excessive.

A request may be **manifestly unfounded** if:

- the individual clearly has no intention to exercise their right to object. For example, if an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
    - the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
    - the request makes unsubstantiated accusations against an organisation or specific employees;
    - the individual is targeting a particular employee against whom they have some personal grudge; or
    - the individual systematically sends different requests to an organisation, as part of a campaign, e.g. once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. **Organisations must consider a request in the context in which it is made, and they are responsible for demonstrating that it is manifestly unfounded.**

Also, organisations should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. Organisations should consider the specific situation and

[76] Article 12(5) of the Gibraltar GDPR. See section 62 of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

Example

An individual believes that information held about them is inaccurate. They repeatedly request its correction but the organisation has previously investigated and told them that they regard it as accurate.

The individual continues to make requests along with unsubstantiated claims against the organisation as the controller.

They refuse the most recent request because it is manifestly unfounded and they notify the individual of this.

13.3. WHAT DOES EXCESSIVE MEAN?

A request may be **excessive** if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- makes a request about the same issue. An individual may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the controller has not handled previous requests properly;
- makes an overlapping request, if it relates to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

14. CAN AN ORGANISATION CHARGE A FEE?

In most cases, organisations cannot charge a fee to comply with a request from an individual exercising one of the rights under Chapter 3 of the Gibraltar GDPR as set out in sections 4 to 10 above, or provide the information that they are required to provide individuals with (the 'privacy information') under the right to be informed, as described in section 3 above.[77]

[77] Article 12(5) of the Gibraltar GDPR. See section 61(5) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

However, organisations can charge a "reasonable fee" for the administrative costs of complying with a request if it is manifestly unfounded or excessive, as defined in section 13 above.[78] Organisations should base the reasonable fee on the administrative costs of complying with the request.

If the organisation decides to charge a fee, they should contact the individual promptly and inform them. Organisations do not need to comply with the request until they have received the fee. Alternatively, an organisation can refuse to comply with a manifestly unfounded or excessive request.

15. CAN AN ORGANISATION ASK FOR PROOF OF IDENTITY?

If an organisation has doubts about the identity of the person exercising a right under Chapter 3 of the Gibraltar GDPR as set out in sections 4 to 10 above, the organisation can ask for more information.[79] However, it is important that they only request information that is necessary to confirm who the individual is. The key to this is proportionality. The organisation should take into account what data they hold, the nature of the data, and what they are using it for.

Organisations must let the individual know as soon as possible that they need more information from them to confirm their identity before responding to their request. The period for responding begins when the organisation receives the additional information.

[78] Article 12(5)(a) of the Gibraltar GDPR. See section 62(1)(a) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

[79] Article 12(6) of the Gibraltar GDPR. See section 61(4) of the DPA for Competent Authorities processing personal data for Law Enforcement Purposes.

IMPORTANT NOTE

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

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