GRA

GIBRALTAR REGULATORY AUTHORITY

(17) Privacy Notices under the GDPR/DPA

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

16th March 2020

Guidance Note IR06/19

FOREWORD

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

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

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

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

CONTENTS

1. INTRODUCTION

To process personal data legitimately under the EU General Data Protection Regulation 2016/679 ("GDPR") and the Data Protection Act 2004 ("DPA"), you have to be transparent about when and how you use the personal data. This requires you to proactively provide respective individuals with certain information when collecting and processing their personal data. The notice that organisations use to provide this information to individuals is commonly referred to as a 'Privacy Notice'.

A 'Privacy Notice' should not be confused with a 'Privacy Policy', which is a term commonly used to describe an internal document that details an organisation's internal personal data handling arrangements to ensure compliance with data protection law.

This document provides guidance on the information that should be provided to individuals i.e. 'transparency requirements', when collecting and processing their personal data. The guidance is divided into four sections –

1) general guidance;
2) information that should be provided to individuals when their personal data is collected directly from them;
3) information that should be provided to individuals when you obtain the personal data from third party sources; and
4) a guide 'Privacy Notice', at Annex A.

The information provided within this document should be treated as guidance, with appropriate consideration required to be given by the reader to the actual legislative provisions. Footnotes referencing the legislation are included so that readers are able to link and relate the guidance to the specific provisions within the law.

Note: *There are some differences between the 'transparency requirements' that apply to law enforcement bodies under part 3 of the DPA and the 'transparency requirements' that apply to all other organisations under the GDPR. However, many of the requirements in both regimes are similar. Footnotes are used throughout the document to refer to the relevant provisions in the GDPR and the DPA, which readers may find useful to identify the requirements that apply to law enforcement bodies (i.e. where references to the DPA are made) and those that apply to all other entities (i.e. where references to the GDPR are made).*

2. GENERAL GUIDANCE

2.1. The information that you should provide individuals in respect of the collection and processing of personal data must be concise, transparent, intelligible, and easily accessible. In addition, the information must be presented in clear and plain language, in particular for any information that is specifically addressed to a child[1].

2.2. The information must be provided in writing, or by other means, including, where appropriate, by electronic means[2].

2.3. If you intend to process the personal data for a purpose other than that for which it was stated to have been collected, the new use must be brought to the attention of the respective individual(s) before the new processing takes place[3].

2.4. The information does not have to be provided if the individual already has it[4].

2.5. The 'Privacy Notice' can be included on any paper-based or electronic forms used to collect the personal data or can be provided alongside it. Sometimes, it can be most effective to provide the information using a combination of methods e.g. including a brief statement on the form, which refers to more detailed information on a website, and using just-in-time 'pop-up' notices.

[1] Article 12(1) of the GDPR (For further guidance on required transparency see also Recital 58 of the GDPR); section 61 of the DPA.

[2] Article 12(1) of the GDPR; section 61 of the DPA.

[3] Article 13(3) of the GDPR.

[4] Articles 13(4) and 14(5)(a) of the GDPR.

3. INFORMATION THAT SHOULD BE PROVIDED TO INDIVIDUALS WHEN THEIR PERSONAL DATA IS COLLECTED DIRECTLY FROM THEM

The following points outline the information that should be provided to individuals when their personal data is collected directly from them -

3.1. identity of the organisation, as the data controller, including contact details[5];

3.2. contact details of the Data Protection Officer (where one is appointed)[6];

3.3. purpose for the collection and use of the personal data[7];

3.4. 'lawful basis' for the collection and use of the personal data[8]. See our Guidance Note on 'Identifying the Lawful Basis';

3.5. period during which the personal data will be kept[9];

3.6. whether the information will be shared, and if so, with who and why[10];

3.7. whether the information will be transferred outside of the European Economic Area, and if so-

3.7.1. the country(ies) or international organisation(s) to which the information will be sent;

3.7.2. the existence or absence of an adequacy decision by the EU Commission (click here); and

3.7.3. in the case of transfers referred to in Article 46 of the GDPR (Transfers subject to appropriate safeguards), Article 47 of the GDPR (Binding corporate rules), or Article 49(1)(b) of the GDPR (Derogations for specific

[5] Article 13(1)(a) of the GDPR; section 53(1)(a) of the DPA.

[6] Article 13(1)(b) of the GDPR; section 53(1)(b) of the DPA.

[7] Article 13(1)(c) of the GDPR; section 53(1)(c) of the DPA.

[8] Articles 13(1)(c) of the GDPR; section 53(2)(a) of the DPA.

[9] Article 13(2)(a) of the GDPR; section 53(2)(b) of the DPA.

[10] Article 13(1)(e) of the GDPR; section 53(2)(c) of the DPA.

situations), reference to the appropriate or suitable safeguards including the means by which to obtain a copy of them or where they have been made available[11];

3.8. individual's rights under the GDPR/DPA, namely -

3.8.1. right of access to their information under Article 15 of the GDPR (or section 53(1)(d)(i) of the DPA);

3.8.2. right to request for their information to be rectified under Article 16 of the GDPR (or section 53(1)(d)(ii) of the DPA);

3.8.3. right to request for their information to be erased under Article 17 of the GDPR (or section 53(1)(d)(iii) of the DPA);

3.8.4. right to request for restrictions to the collection and/or use of their information under Article 18 of the GDPR (or section 53(1)(d)(iii) of the DPA);

3.8.5. right to object to the collection and/or use of their information under Article 21 of the GDPR; and

3.8.6. right to data portability under Article 20 of the GDPR;

3.9. right of individuals to withdraw consent at any time[12] where the lawful basis to the processing identified (i.e. point 3.4 above) is Article 6(1)(a) or Article 9(2)(a) of the GDPR;

3.10. right of individuals to lodge a complaint with the Information Commissioner i.e. the Gibraltar Regulatory Authority[13];

3.11. where applicable, information in respect to the requirement for individuals to provide their personal data due to a statutory requirement, contractual requirement, or a requirement necessary to enter into a contract[14];

3.12. whether individuals are obliged to provide personal data, and if so, details of where the obligation stems from, together with the possible consequences of failure to provide the information[15];

3.13. where applicable, the existence of automated decision-making (including profiling) including meaningful information about the logic involved and the significance and envisaged consequences for the individual[16].

[11] Article 13(1)(f) of the GDPR.

[12] Article 13(2)(c) of the GDPR.

[13] Article 13(2)(d) of the GDPR; section 53(1)(e) of the DPA.

[14] Article 13(2)(e) of the GDPR.

[15] Article 13(2)(e) of the GDPR.

[16] Article 13(2)(f) of the GDPR; section 59(2)(a) of the DPA.

4. CIRCUMSTANCES WHERE THE ORGANISATION DOES NOT OBTAIN PERSONAL DATA DIRECTLY FROM THE INDIVIDUAL

4.1. When you do not obtain the information directly from the individual, the following information must be provided to them -

4.1.1. all the information identified in section 3 above other than the information within sections 3.11 and 3.12;

4.1.2. the source from which the data was obtained, and if applicable, whether it came from publicly available sources[17].

4.2. The information must be provided[18] –

4.2.1. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

4.2.2. at latest at the time of the first communication with the individual if their personal data are to be used for communication with the individual; or

4.2.3. at latest when the personal data are first disclosed if a disclosure to another recipient is envisaged.

4.3. Paragraphs 4.1 and 4.2 above do not apply when[19] –

4.3.1. the individual already has the information[20];

4.3.2. the provision of the information would prove impossible or involve a disproportionate effort, in particular when data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[21]

[17] Article 14(2)(f) of the GDPR; section 53(3) of the DPA.

[18] Article 14(3) of the GDPR.

[19] Article 14(5) of the GDPR.

[20] Article 14(5)(a) of the GDPR.

[21] Article 14(5)(b) of the GDPR.

4.3.3. the obtaining or disclosure of the information is expressly laid down in a law to which the organisation is subject;[22] and

4.3.4. when the personal data must remain confidential subject to an obligation of professional secrecy regulated by law (including a statutory obligation of secrecy)[23].

[22] Article 14(5)(c) of the GDPR.

[23] Article 14(5)(d) of the GDPR.

ANNEX A- PRIVACY NOTICE GUIDE AND TEMPLATE

In the following a 'Guide to Complete' a 'Privacy Notice' alongside a template is provided.

You should treat the below as guidance only and not as an absolute measure to comply with the law. You should ensure that your Privacy Notice complies with the law in accordance with your data processing activities.

Organisation Sample Privacy Notice-
Guide to complete

Our contact details

Insert the contact details for your business. Include postal address, any main email addresses, phone numbers or web addresses.

Also include the name and contact details for your main point of contact for data protection matters. This does not have to be a designated 'Data Protection Officer'

What type of information we have

Tell people what type of personal information you collect and hold. Personal Information is any information that can be used to identify a living person. For example members' email addresses, customer financial information, employee data or website user stats.

How we get the information and why we do we have it

Tell people how you collect the information and where you collect the information from.

Tell people the reasons why you need to collect or hold their information. Include your lawful basis for doing this in this section (please see this Guidance Note for further information).

You may collect personal information because you have a legal or contractual obligation. You should inform people here if this is the case.

If you are relying on consent to process individual's information, then you should also tell people about their right to withdraw consent and how they can do this in this section.

What we do with the information

Tell people what you do with the information.

Include if you share information with anyone, or any other business. Make sure you include how you do this and any sharing you do outside the EU.

If applicable, include any automated decision making that is made using the information, or any profiling you undertake.

How we store your information

Tell people how or where you keep their information, how long you intend to keep their information for and then how you intend to securely destroy or dispose of it. You need to do this for every type of information you hold.

Your data protection rights

Tell people about their data protection rights. Their rights will differ depending on your lawful basis for processing, so once you know this then you can select the relevant sections from the text in the template below to include in your Privacy Notice.

How to complain

Tell people how to make a complaint to you here. Include the address of the Gibraltar Regulatory Authority.

Include the date you completed the privacy notice.

Organisation Sample Privacy Notice

Our contact details

Name:

Address:

Phone Number:

E-mail:

What type of information we have

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name and contact details)
- [Add to this list as appropriate]

How we get the information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- [Add the reasons you collected personal information]

[If applicable] We also receive personal information indirectly, from the following sources in the following scenarios:

- [Add the source of any data collected indirectly and why you collected the information]

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are: **[delete as appropriate]**

(a) Your consent. You are able to remove your consent at any time. You can do this by contacting [contact details]

(b) We have a contractual obligation.

(c) We have a legal obligation.

(d) We have a vital interest.

(e) We need it to perform a public task.

(f) We have a legitimate interest.

What we do with the information we have

We use the information that you have given us in order to [list how you use the personal information].

We may share this information with [enter organisations or individuals]

How we store your information

Your information is securely stored [enter location].

We keep [type of personal information] for [time period]. We will then dispose your information by [explain how you will delete their data]

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal data in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at [insert email address, phone number and or postal address] if you wish to make a request.

How to complain

You can also complain to the Gibraltar Regulatory Authority (the "GRA") if you are unhappy with how we have used your data.

The GRA's address:

Gibraltar Regulatory Authority,
2nd Floor, Eurotowers 4,
1 Europort Road, Gibraltar
Tel: (+350) 20074636
Email: info@gra.gi

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 GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with their provisions lies with the organisation.

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

CONTACT US

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

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