GRA

GIBRALTAR REGULATORY AUTHORITY

Data Protection Impact Assessment – guidance on 'prior consultation'

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

13 November 2019

'Prior consultation' guidance in relation to Guidance Note IR04/17

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, both pieces of legislation 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

A Data Protection Impact Assessment ("DPIA") is a procedure designed to assist organisations identify and minimise the privacy risks of new projects or policies.[1]

A data controller must consult the supervisory authority prior to processing where a DPIA under the EU General Data Protection Regulation 2016/679 (the "GDPR") and the Data Protection Act 2004 (the "DPA") indicates that the intended processing would result in a high risk to the rights and freedoms of individuals and these risks cannot be adequately mitigated by the data controller.[2]

This Guidance Note aims to provide advice on the GDPR and DPA's prior consultation requirements and process, to help data controllers determine when to consult the Information Commissioner[3] (the "Commissioner"). The guidance is divided in to two sections –

- when to consult the Commissioner; and
- how to consult the Commissioner.

The information provided should be treated as guidance with appropriate consideration being given to the actual legal requirements. Footnotes referencing the legislation are included so that readers are able to link and relate the guidance to the specific provisions in the law.

Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance documents are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the UK's Information Commissioner's office.

[1] See the GRA Guidance Note IR04/17 V2 Guidance on the General Data Protection Regulation: (4) Data Protection Impact Assessment (https://www.gra.gi/dataprotection/guidance-on-the-general-data-protection-regulation/gdpr4).

[2] See Article 36(1) of the GDPR, Recital 84 and 92 of the GDPR. Note that for processing under Part III of the DPA, prior consultation in the context of DPIAs is required under Section 74(2) of the DPA, where under section 74(1) of the DPA a controller intends to create a filing system.

[3] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority. The Information Rights Division (one of the Gibraltar Regulatory Authority's four Divisions) is responsible for data protection and works on behalf of the Information Commissioner to regulate data protection in Gibraltar.

2. WHEN DO WE CONSULT THE INFORMATION COMMISSIONER?

If a data controller carries out a DPIA that identifies a high risk to the rights and freedoms of individuals that cannot be mitigated, prior consultation with the Commissioner is required.[4] The data controller cannot begin processing personal data until they have sought written advice from the Commissioner on the proposed processing operation.

The emphasis is on the '**residual risk**' after implementing any mitigating measures. If the DPIA originally identified a high risk but steps have been taken to mitigate the risk, prior consultation is not needed.

[4] Article 36(1) of the GDPR and Recital 84 of the GDPR; Section 74(2) of the DPA.

3. HOW DO WE CONSULT THE INFORMATION COMMISSIONER?

The following information should be provided to the Commissioner's office when submitting a request for prior consultation -

(a) a description of the respective roles and responsibilities of the controller, or joint controllers, and processors involved in the processing;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards taken to protect the rights and freedoms of data subjects;

(d) contact details of your data protection officer (if applicable);

(e) the DPIA, including any supplementary documents;

(f) any other information requested by the supervisory authority.[5]

3.1 What happens next?

Upon receipt of the DPIA, the Commissioner will send an acknowledgement and check that all relevant information has been provided.

Within 10 working days, the Commissioner will confirm whether the DPIA has been accepted for prior consultation, along with an explanation for this decision.

There may not be any further contact until written advice is provided. Should there be any further queries, the Commissioner may decide to arrange a telephone call or a meeting.

3.2 What happens if the DPIA is not accepted?

The Commissioner may wish to discuss the proposed processing, even if the DPIA does not meet the criteria for prior consultation. Further information will also be provided as to how the Commissioner would like to engage with you.

[5] See Article 36(3) of the GDPR and Recital 94 of the GDPR; Section 74(3) of the DPA.

3.3 How is the DPIA assessed?

If the DPIA is accepted for prior consultation, a full review of the DPIA and all documentation provided will be assessed, along with any prior contact there may have been with the Commissioner, in order to understand in detail, the context and nature of the proposed processing, including any controller–processor relationships. The extent to which compliance with the Data Protection Principles has been evidenced will also be assessed.

3.4 How long does it take?

Where advice is provided under the prior consultation process, a response will be provided within eight weeks of receipt of the DPIA. In complex cases, this period may be extended by a further six weeks, therefore allowing a maximum of 14 weeks.[6] Should an extension be required, an explanation for the delay will be provided in writing within one month of receipt of the DPIA.[7]

If more information is required, this must be provided in order to continue with the assessment. To prevent further delay, any documents the DPIA refers to, such as privacy notices, should also be included.

If the intended processing would affect data subjects in EU member states, the Commissioner may be required to liaise with other data protection authorities before providing written advice, in compliance with Chapter VII of the GDPR. This may mean that the case cannot be resolved in 14 weeks, although in this instance, updates will be provided.

3.5 What are the possible outcomes?

Upon reviewing the DPIA, it may be decided that the risks have been sufficiently identified and mitigated, and that processing can begin.

The written response could be limited to advice on how the identified risks can be further mitigated before proceeding with the processing.

It is important to note that the Commissioner may use any of his powers referred to under Article 58 of the GDPR.[8] For example, in some circumstances, an official warning may be issued[9], alongside the advice provided. Warnings may also be issued where there is concern

[6] See Article 36(2) of the GDPR. However, note that the Commissioner may extend the initial timeframe for providing advice in relation to a prior consultation request under Section 74(2) of the DPA from six weeks to a further one month, as detailed in Section 74(5) and 74(6) of the DPA.

[7] Article 36(2); Section 74(7) of the DPA.

[8] Article 36(2) of the GDPR.

[9] Article 58(2)(a) of the GDPR.

that the intended processing is likely to contravene the GDPR and/or DPA. Any warning will explain the reasons for the concerns and the recommended steps to avoid any contraventions.

Should there be any more significant concerns, a limitation or a ban may be imposed on the intended processing under Article 58(2)(f) of the GDPR.

In any event, the written response will clearly detail what may and may not be done.

3.6 Can the outcome be appealed?

Warnings are not subject to appeal, nonetheless a judicial review may be sought should there be a disagreement in the way the decision was made.

Further, a review of other corrective measures (such as limitations or bans on processing) can be sought by appeal to the Magistrates Court in accordance with the provisions of the DPA.

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 its provisions lies with the organisation.

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

CONTACT US

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

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