GIBRALTAR REGULATORY AUTHORITY

(9) Guidance on Information Commissioner's Regulatory Action

Guidance on the General Data Protection Regulation

DISCLAIMER

Please note that, on 1st January 2021, the EU General Data Protection Regulation 2016/679 ("EU GDPR") was superseded by the Gibraltar General Data Protection Regulation.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

7 August 2020

Guidance Note IR04/18 v2

CONTENTS

1. INTRODUCTION 1
2. WHEN WE WILL ISSUE INFORMATION NOTICES 2
3. WHEN WE WILL ISSUE ASSESSMENT NOTICES 4
4. WHEN WE WILL ISSUE ENFORCEMENT NOTICES 8
5. WHEN A PENALTY NOTICE WILL BE APPROPRIATE 9
6. EFFECTIVENESS OF REGULATORY ACTION 13
7. EVALUATION AND NEXT STEPS 13

1. INTRODUCTION

The purpose of this document is to provide guidance on the regulatory action that the Information Commissioner[1] (the "Commissioner") may take under the Data Protection Act 2004 (the "DPA") and General Data Protection Regulation (the "GDPR").

Section 167 of the DPA requires the Commissioner, to produce and publish guidance about how he proposes to exercise his functions in connection with -

(a) assessment notices;
(b) enforcement notices; and
(c) penalty notices.

Also, under section 167 of the DPA, the Commissioner may produce and publish guidance about how he proposes to exercise other enforcement functions, such as the issuing of information notices. This guidance has been produced in accordance with said provisions.

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

2. WHEN WE WILL ISSUE INFORMATION NOTICES

An information notice is a formal request for a controller, processor or individual to provide us with information, within a specified time frame, to assist us with our investigations. In some circumstances it may be a criminal offence to provide a response which is false in any material respect.

We may serve an information notice at our discretion in any investigation. We will have regard to what action is appropriate and proportionate, and criteria including:

1. the risk of harm to individuals or the level of intrusion into their privacy potentially posed by the events or data processing under investigation;

2. the utility of requiring a formal response within a defined time period;

3. the utility of testing responses, by the fact that it is an offence to deliberately or recklessly make a false statement in a material respect in response; and

4. the public interest in the response.

When deciding the period for compliance with information notices, in particular whether or not to issue an 'urgent' information notice, we will have regard to what action is appropriate and proportionate and criteria including:

1. the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example, requesting an early report on a serious data security breach in order for the Commissioner to direct the controller on and validate appropriate notification to data subjects and appropriate mitigation of the breach;

2. the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;

3. the scope of the notice, that is the scope of questions or requests in an information notice;

4. the additional burden on the recipient in having to comply with a notice urgently;

5. the impact on the rights of the recipient, should the Commissioner obtain information under an urgent information notice (which may be by court order), prior to an appeal being heard by the Magistrates' Court;

6. the length of time of the investigation. For example, it may be appropriate and proportionate to issue an urgent information notice during a long running investigation where the questions are limited, and the response may bring the investigation closer to completion; and

7. the comparative effectiveness of other investigatory powers of the Commissioner.

If a recipient of an information notice does not fully respond within the applicable time period, whether urgent or not, the Commissioner will promptly apply for a court order requiring a response. The Commissioner may decide not to make such application, having regard to criteria including:

1. the reasons for non-compliance with the information notice;

2. any commitments given by the recipient to responding to the information notice;

3. whether the information has been or is likely to be obtained from another source;

4. the comparative effectiveness of other investigatory and enforcement powers of the Commissioner. For example, the Commissioner may decide it has sufficient evidence to move to an enforcement action in any event; and

5. the public interest.

The Commissioner will also consider whether or not to issue a Penalty Notice (see below).

3. WHEN WE WILL ISSUE ASSESSMENT NOTICES

The DPA contains a provision for the Commissioner to issue an 'assessment notice'[2]. This is, essentially, a notice which is issued by the Commissioner to a controller or processor to allow us to investigate whether the controller or processor is compliant with data protection legislation. The notice may, for example, require the controller or processor to give us access to premises and specified documentation and equipment.

We may serve an assessment notice at our discretion in any investigation into compliance with the data protection legislation. We will have regard to what action is appropriate and proportionate, and criteria including:

1. where we have conducted a risk assessment or other regulatory action, there is a probability that personal data is not being processed in compliance with the data protection legislation, together with a likelihood of damage or distress to individuals;

2. it is necessary to verify compliance with an enforcement notice;

3. communications with or information (e.g. news reports, statutory reporting or publications) about the controller or processor suggest that they are not processing personal data in compliance with the data protection legislation; and

4. the controller or processor has failed to respond to an information notice within an appropriate time.

When determining the risks of non-compliance, we will consider one or more of the factors for regulatory action. We will also consider other relevant information, such as reports by whistle-blowers, and any data privacy impact assessments that may have been carried out.

When deciding the period for compliance with assessment notices, in particular whether or not to issue an 'urgent' assessment notice, we will have regard to what action is appropriate and proportionate, and criteria including:

1. the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy;

2. the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;

3. the scope of the notice, that is the scope of our requests in an assessment notice;

4. the additional burden on the recipient in having to comply with a notice urgently;

[2] See section 153 of the DPA.

5. the impact on the rights of the recipient should the Commissioner gain access to its premises and data processing activities urgently and without the opportunity to appeal and/or for an appeal to be heard by the Magistrate's Court;

6. the length of time of the investigation. For example, it may be appropriate and proportionate to issue an urgent assessment notice during a long running investigation where the requests are limited, and the response may bring the investigation closer to completion; and

7. the comparative effectiveness of other investigatory powers of the Commissioner.

Assessments of documents, including handling of health and social care records

We may require access to the specified documents and information, or classes of documents and information, which define and explain how obligations have been met under the legislation, and the governance controls in place to measure compliance.

Although not an exhaustive list this could include, for example:

(a) Strategies

(b) Policies

(c) Procedures

(d) Guidance

(e) Codes of practice

(f) Training material

(g) Protocols

(h) Frameworks

(i) Memoranda of understanding

(j) Contracts

(k) Privacy statements

(l) Privacy impact assessments

(m) Control data

(n) Job descriptions

We may also need access to specified personal data or classes of personal data, and to evidence that it is being handled in compliance with the policies and procedures which ensure compliance with the legislation. The level of access will only be enough to assess compliance.

We do not require access to information which:

1. is subject to legal professional privilege (see below);

2. has a high level of commercial sensitivity; or

3. is exempt from the DPA, by virtue of a security certificate[3].

We recognise that there might also be legitimate concerns about other information which relates to issues of security or sensitive activities. In these cases, it will generally be possible to audit data protection compliance without access to such information. Where it is necessary and appropriate, we will ensure that properly vetted members of staff inspect such information. Where possible and appropriate, the Commissioner will seek to establish memoranda of understanding with relevant agencies to provide access and understanding of this type of material.

Individuals can contact us to request that, if an assessment notice requires access to such information, this access be limited to the minimum required to adequately assess their compliance with the legislation. They may also request other access conditions. Such requests must be made within 28 days of the notice, unless the assessment is to be conducted on shorter notice, in which case, as soon as reasonably possible.

We may need to view health and social care records. If we do, we will respect the confidentiality of this data, and will limit access to the minimum required to adequately assess compliance. Unless necessary, we will not take the content of these off-site, or copy or transcribe them into working notes, and will not include them in any reporting of the assessment.

Inspection and examinations during assessments

Inspections and examinations are key review elements of the assessment. They help us to identify objective evidence of compliance, and how policies and procedures have been implemented.

These reviews of personal data, and associated logs and audit trails, may consider both manually and electronically stored data, including data stored centrally, locally and on mobile devices and media.

We use these reviews to evaluate how an organisation:

1. obtains, stores, organises, adapts or alters information (e.g. policies and procedures) or personal data;

2. ensures the confidentiality, integrity and availability of the data or service it provides;

3. retrieves, consults, or uses the information or personal data;

4. discloses personal data by transmitting or disseminating or otherwise making the data available; and

5. purges and destroys personal data.

[3] See section 29 of the DPA.

The review may also cover management/control information, to monitor and record how personal data is being processed, and to measure how a controller meets their wider obligations under the legislation.

The review may evaluate physical and IT-related security measures, including how personal data is stored and disposed of.

The review and evaluation process may take place on site as part of a discussion with staff to demonstrate 'practice', or independently by way of sampling by auditors. If information is held electronically, we may require the controller to provide manual copies or facilitate direct access. Any direct access would be limited to the identified records, would only be done locally and would be for a limited and agreed time.

Data reviewed as part of the review and evaluation process, but not specifically identified in the assessment notice, may only be taken off the controller's site with the controller's permission.

Interviews carried out during assessments

Interviews will consist of discussions with:

1. staff and contractors;

2. any processor's staff; and

3. staff of relevant service providers as specified in the assessment notice.

We conduct interviews to develop further understanding of working practices and/or awareness of regulatory obligations. Departmental managers, operational staff, support staff (e.g. IT staff, security staff) as well as staff involved with information and information governance may be interviewed.

Where possible we will schedule and agree interviews with the controller or processor before the on-site audit. We will give a schedule of areas to be covered before the audit and will discuss and agree the level and grade of staff to be interviewed (e.g. managers, operational staff etc.). Individuals should be advised by the target organisation in advance of their required participation.

We will use questions to understand individual roles and processes followed or managed, specifically referring to the handling of personal data and its security.

Interviews may be conducted at an individual's desk or in a separate room dependent upon circumstances, and whether there is a need to observe the working environment or examine information and records. Interviews will normally be 'one-to-one', but sometimes it may be appropriate to include a number of staff in an interview – where, for example, there are shared responsibilities. We will take notes during the interviews.

We will make every effort to restrict interviews to staff identified within the agreed schedule. But when it becomes clear during an audit that access to additional staff may be necessary, we will arrange this with the consent of the controller. Similarly, the schedule will not prevent us having confirmatory conversations with a consenting third party, for example where the third party is close to a desk-side discussion.

Interviews are to help in assessing compliance. They do not form part of, or provide information for, any individual disciplinary or criminal investigation.

Individuals' names may be used in distribution lists and the acknowledgements sections of reports, but they will not be referenced in the body of any report. Job titles may be used where appropriate.

If a controller or processor fails to comply with an Assessment Notice, the Commissioner will consider whether or not to issue a Penalty Notice (see below).

4. WHEN WE WILL ISSUE ENFORCEMENT NOTICES

Enforcement notices may be issued in the circumstances set out in section 155 of the DPA. For example, where a controller or processor has breached one of the data protection principles or rights of individuals.

The purpose of an enforcement notice is to mandate action (or halt action, such as processing or transfer) to bring about compliance with information rights and/or remedy a breach. Failure to comply with an enforcement notice invites further action, including the possibility of the Commissioner issuing a civil monetary penalty.

Enforcement notices will usually be appropriate where specific correcting action (or its prevention) may be required. Although this is not an exhaustive list, an enforcement notice may be required in such circumstances as:

1. repeated failure to meet information rights obligations or timescales for them (e.g. repeatedly delayed subject access requests);

2. where processing or transfer of information to a third country fails (or risks failing) to meet the requirements of the data protection legislation;

3. there is a need for the Commissioner to require communication of a data security breach to those who have been affected by it; or

4. there is a need for correcting action by a certification body or monitoring body to ensure that they meet their obligations.

The notice will set out:

1. who is required to take the action and why;

2. the specifics of the action to be taken;

3. how to report that the action has been taken;

4. the timescales that apply for that action; and,

5. any appeal/challenge process that applies.

When deciding whether to issue an enforcement notice, we will have regard to the factors set out above, including the presence of any mitigating or aggravating factors.

Timescales set out in an enforcement notice will usually reflect the imminence of proposed action that could lead to a breach of obligations, the severity and scale of any breach/failings, and the feasibility (including lead times) of any correcting measures or technology.

In addition, when deciding whether or not to issue an 'urgent' enforcement notice, and in deciding the period for compliance with such notice, we will consider whether urgent action by the recipient (to take specific steps or to stop specific processing of personal data) is appropriate and proportionate having regard to criteria including:

1. the extent to which such urgent action may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example, requesting a controller stops using personal data for a specific purpose or takes action to protect personal data from security breaches;

2. the scope of the enforcement notice;

3. the additional burden or impact on the recipient in having to comply with an urgent enforcement notice within the period specified; and

4. the comparative effectiveness of other enforcement powers of the Commissioner.

If a controller or processor fails to comply with an enforcement notice, the Commissioner will also consider whether or not to issue a Penalty Notice (see below).

5. WHEN A PENALTY NOTICE WILL BE APPROPRIATE

The Commissioner's aim in applying penalty notices is to ensure compliance with legislation and information rights obligations. To do this, penalties must provide an appropriate sanction for any breach of information rights or legislation, as well as act as an effective deterrent.

Our decision whether to impose a penalty at all and the decision as to the amount of the penalty in a case will involve consideration of the following factors:

1. the nature, gravity and duration of the failure;

2. the intentional character of the failure or the extent of negligence involved;

3. any action taken by the controller or processor to mitigate the damage or distress suffered by the data subjects;

4. the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with the GDPR and sections 66, 75, 112 and 116 of the DPA;

5. any relevant previous failures by the controller or processor;

6. the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse risks of the failure;

7. the categories of personal data affected by the failure;

8. the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

9. the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

10. adherence to approved codes of conduct or certification mechanisms;

11. any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly); and

12. whether the penalty would be effective, proportionate and dissuasive.

In the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations. These will typically involve wilful, deliberate or negligent acts, or repeated breaches of the law, causing harm or damage to individuals. In considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial and may require a sanction.

This means that each case will be assessed objectively on its own merits. But our hierarchy and risk-based approach mean that it is more likely that a penalty will be imposed where, for example:

1. a number of individuals have been affected;

2. there has been a degree of damage or harm (which may include distress and/or embarrassment);

3. sensitive personal data has been involved;

4. there has been a failure to comply with an information notice, an assessment notice or an enforcement notice;

5. there has been a repeated breach of obligations or a failure to rectify a previously identified problem or follow previous recommendations;

6. wilful action (including inaction) is a feature of the case;

7. there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it); and

8. there has been a failure to implement the accountability provisions of the GDPR.

When oral representations will be appropriate

Before issuing a penalty, we will advise the target that we intend to levy a penalty by issuing a notice of intent ("NOI"). The NOI will set out the circumstances of any breach, our investigation findings and the proposed level of penalty, along with a rationale for the penalty and any proposed enforcement notice requirements.

Representations will be taken from the proposed target about the imposition of the penalty and its level. The target will be allowed at least 21 calendar days to make these representations.

In addition, we may allow an organisation or individual subject to an NOI to submit representations orally during a face-face meeting at our office. However, this is discretionary and only relevant in cases that are considered by us to be exceptional. It is likely that these could be appropriate in circumstances where:

1. the central facts of any breach or failing are in dispute;

2. the integrity of any technical witness evidence is in dispute;

3. there is a requirement to make reasonable adjustments on grounds of equality; or

4. the consideration of 'harm' elements of a case would benefit from evidence from those affected.

During these meetings, representatives of the target of the NOI are able to explain in person how the privacy concerns and breaches occurred, submit mitigating factors, what they have (or plan to do) to achieve compliance and the reasons why they believe that the Commissioner should not take the intended regulatory action. A request for a reduction in the size of the penalty may also be submitted during the oral representations.

If an organisation or individual thinks that their circumstances warrant oral representations of this nature, they can explain why they think this extra step is justified in their written representations. In particular, the Commissioner will need to understand what oral representations will add to the regulatory process. We will then decide whether or not to invite the target to a face-face meeting.

However, it is unlikely that we will agree to take oral representations in a case that is principally technical in nature. In such cases, it is normally more appropriate to consider complex technical representations in writing.

Where appropriate, we will also have regard to representations (including from any Concerned Supervisory Authorities in the EU where the Commissioner is the Lead Supervisory Authority

or the Data Protection Board[4] itself) under the cooperation and consistency mechanisms of the GDPR in setting the final amount of any penalty. These representations will be taken after the consideration of representations of the target of the penalty but before the final setting of any penalty level and following the procedures set out in relevant Data Protection Board rules of procedure.

For very significant penalties (expected to be those over the threshold of £1M) a panel may be convened by the Commissioner to consider the investigation findings and any representations made, before any penalty level is applied. Where relevant and considered appropriate, external experts may also be invited to form part of the panel. It will be the Commissioner's final decision as to the level of penalty applied.

Once all representations have been fully considered we will confirm any penalty notice in writing. We will also advise those subject to penalties of any relevant rights of appeal that apply to their case.

What will be the amount of any penalty

Where we have discretion to set the amount of any penalty in the context of our regulatory work, we will approach setting any penalty level, within the legislative bands, on the basis of the following mechanism:

Step 1. An 'initial element' removing any financial gain from the breach.

Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 162(2)-(4) of the DPA.

Step 3. Adding in an element to reflect any aggravating factors.

Step 4. Adding in an amount for deterrent effect to others.

Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).

In data protection cases involving failures to meet data security obligations we will consider the breach separately from the failure to report. In all other cases we will adopt a 'whole case' approach when setting the penalty level.

Generally, the amount will be higher where:

1. vulnerable individuals or critical national infrastructure are affected;

2. there has been deliberate action for financial or personal gain;

3. advice, guidance, recommendations or warnings (including those from the Data Protection Officer or the Commissioner) have been ignored or not acted upon;

4. there has been a high degree of intrusion into the privacy of a data subject;

[4] European Data Protection Board established under Article 68 of the GDPR

5. there has been a failure to cooperate with an investigation or enforcement notice; and

6. there is a pattern of poor regulatory history by the target of the investigation.

Fixed penalties

Certain legislation provides for set penalties to be applied for failing to meet specific obligations. Where those provisions apply, we will levy those penalties in accordance with the law.

Cost recovery

We will not consider our own investigative or regulatory costs in the application of a penalty calculation. Monetary penalties will be payable to the Gibraltar Regulatory Authority as required by the DPA.

6. EFFECTIVENESS OF REGULATORY ACTION

We will report annually to Parliament about our work, including our regulatory activity and, where needed, our formal enforcement actions. This may also include reporting on specific issues identified with individual organisations.

7. EVALUATION AND NEXT STEPS

We will keep this Policy under review and evaluate it regularly and at least every three years.

We will update it to reflect any amendments to legislation, including any implementation of an updated e-Privacy Regulation, and once the final settlement between the EU and the UK post-Brexit is confirmed.

CONTACT US

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

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