# Explanatory Framework for Adequacy Discussions

## Section I3:

## Role of the Gibraltar Regulatory Authority and Redress

### Overview

This section explains how the GRA meets the various adequacy requirements for an independent supervisory authority for Gibraltar. It sets out the GRA's powers and responsibilities, its governance and independence, including its staffing, funding and spending, its effective enforcement and compliance regime, and the administrative and judicial redress system, which enables individuals to pursue legal remedies to enforce their rights rapidly and effectively.

## Introduction

The Gibraltar Regulatory Authority (the "GRA") is Gibraltar's Data Protection Supervisory Authority. It was established, under the Gibraltar Regulatory Act 2000 (the "GRA Act 2000"), as an independent statutory body and became the independent regulator for Gibraltar's data protection regime in 2006.

The GRA is independent of the Government of Gibraltar (the "GoG"). It reports directly to the Gibraltar Parliament and is required by law to act with complete independence in the performance of its functions. The GRA neither seeks nor accepts instructions from any outside body or government and has an excellent track record as an independent regulator for data protection since 2006, taking a proportionate approach to enforcement.

One of the GRA's main roles is to promote privacy and uphold information rights. It has a wide range of responsibilities across various sectors and sets and enforces regulatory rules in accordance with Gibraltar and EU legislation. In addition to promoting data privacy and upholding information rights, the GRA also regulates the electronic communications, broadcasting, satellites and postal industries.

This section is concerned only with the data protection aspect of the GRA's remit, setting out how the GRA meets the various adequacy requirements for an independent supervisory authority.

The remaining parts of this section cover:

- Part 1: The Role of the GRA - responsibilities and activities.
- Part 2: The GRA's independence and governance.
- Part 3: The GRA's investigation and enforcement powers.
- Part 4: Data subjects' ability to seek a judicial remedy instead of, or in addition to GRA action, and their ability to complain about GRA service.

A further section (Section I3 - Annexes A-F) contains supplementary information on these topics.

## PART I: THE ROLE OF THE GRA - RESPONSIBILITIES AND ACTIVITIES

Section 123(2) of the Data Protection Act 2004 (the "DPA 2004") designates the GRA as the Data Protection Commissioner. Therefore throughout this section, the Data Protection Commissioner is referred to as the "GRA".

The GRA is therefore the independent statutory body responsible for the enforcement of data protection law in Gibraltar. Its functions include enforcing the privacy rights of individuals, advising on data protection related matters, investigating complaints made by data subjects, and raising public awareness of privacy issues.

### The GRA's responsibilities

A key part of the GRA's regulatory responsibilities is enforcement of the DPA 2004 and the General Data Protection Regulation (the "Gibraltar GDPR", and together with the DPA 2004, "the Data Protection Legislation"). These powers and tasks are set out in Part VI of DPA 2004 and Articles 57 and 58 of the GDPR. The GRA's regulatory activity includes:

- conducting assessments of compliance with the Data Protection Legislation, and conducting data protection audits of data controllers and processors. Section 160 of the DPA 2004 provides the GRA with the power to enter, inspect, and search premises;
- issuing information notices requiring individuals, controllers or processors to provide information as part of an investigation into compliance with the Data Protection Legislation;
- issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of Data Protection Legislation and other information rights obligations;
- administering fines by way of penalty notices in the circumstances set out in section 162 of the DPA 2004;
- administering fixed penalties for failing to meet specific obligations;
- prosecuting criminal offences before the courts;
- requiring a data controller or digital service provider to inform an individual of a personal data breach.

These enforcement powers are set out in more detail in Part 3 of this section. The GRA is also empowered to take various regulatory actions for the Communications (Personal Data and Privacy) Regulations 2006 (the "Privacy Regulations").

Other key responsibilities of the GRA include:

- producing data protection codes of practice about issues such as data sharing and direct marketing;

- conducting assessments of cross-border data transfers and corporate groups' binding corporate rules and overseeing data protection impact assessments;
- overseeing the establishment of data protection certification mechanisms, encouraging the development of codes of conduct and accrediting bodies to monitor compliance with codes of conduct.

## International Activities

The GRA is an accredited member of both the European Conference of Data Protection Authorities (the "ECDPA") and the Global Privacy Assembly (the "GPA") (previously known as the International Conference of Data Protection & Privacy Commissioners (the "ICDPPC")). Members of the GRA regularly attend the annual ECDPA and GPA.

In addition, the GRA actively participates in various other international events and projects, and liaises with other regulators internationally to coordinate, cooperate and align regulatory activities to maximise its effectiveness, and contribute to developing regulatory and enforcement practices.

For example, in 2016, the GRA and INFOEM (the State of Mexico's Data Protection Authority) signed a Memorandum of Understanding ("MOU") to establish mechanisms for institutional cooperation and collaboration with regards to Data Protection and Freedom of Information. Amongst other things, this led to the participation of a member of the GRA, as an expert speaker on data protection regulation within the EU, in a data protection forum and a conference organised by INFOEM. It also facilitated the attachment of four lawyers from INFOEM to the GRA for one week to learn about Gibraltar's data protection framework and its procedures.

Significantly, on 1 November 2019, the Convention for the protection of individuals with regard to automatic processing of personal data (CETS No. 108) was extended to Gibraltar.

Other international activities by the GRA are described at Annex A.

## PART II: INDEPENDENCE AND GOVERNANCE OF THE GRA

The GRA is a fully independent body, established by the GRA Act 2000. It has an excellent track record as the independent supervisory authority for data protection in Gibraltar.

Section 11(2)[1] and (3)[2] of the GRA Act 2000 require the GRA to act with complete independence when exercising its functions and to only take into account public policy to the extent that it is lawful to do so. Section 123 of the DPA 2004 also states that the Data Protection Commissioner (i.e the GRA) shall be independent in the exercise of functions under the Act.

### Appointment and Removal of GRA board members

Under section 3 of the GRA Act 2000, the board of the GRA (the "GRA Board") is composed of:

- the Chief Executive Officer (CEO);
- the Deputy Chief Executive Officer (the "Deputy CEO"); and
- a minimum of 2, but a maximum of 3, other persons appointed by the Chief Minister.

The Chief Minister appoints the CEO of the GRA under section 6 of the GRA Act 2000. The term of office is set at five years but may be extended. This role is considered to be a quasi-judicial role in that the CEO is required to interpret the law and carry out objective investigations in regard to alleged contraventions of the law.

The Deputy CEO is appointed by the GRA, on the recommendation of the CEO, from officers employed by or seconded to the GRA. This is set out in section 7 of the GRA Act 2000.

If the CEO is absent for a period of more than fourteen days, the GRA is required to appoint the Deputy CEO as Acting CEO for a period of time not exceeding one month. Likewise, in the absence of the Deputy CEO for a period in excess of fourteen days, the CEO shall appoint another officer of the GRA to act as Deputy CEO for a period of time not exceeding one month.

Under section 3 of the GRA Act 2000, the other GRA Board members are appointed by the Chief Minister. However, there are safeguards in place to ensure that appointments are transparent. For example, rather than direct appointments by the Chief Minister, the

[1] Section 11(2): A person – (a) appointed under section 3(3); or (b) to whom functions have been delegated under section 9, shall not hold a position which is incompatible with the performance in an independent and impartial manner of such functions as he may have to discharge as a result of an appointment under section 3(2) or a delegation under section 9 as the case may be.
[2] Section 11(3): The Gibraltar Regulatory Authority shall act with complete independence when exercising its functions and shall only take into account public policy to the extent that it is lawful to do so.

process for the appointment of the GRA's board members involves an initial recommendation of candidates by the CEO and all appointments are published in the Gazette which is available on the Laws of Gibraltar website.

Section 11 of the GRA Act 2000 covers the eligibility criteria for appointment as a member of the GRA. Specifically, it highlights that a person who holds a position that is incompatible with performing the functions of the GRA in an independent and impartial manner may not be appointed. It also states that MPs cannot be appointed to the GRA.

Section 3(5) of the GRA Act 2000 lists the circumstances under which any member of the GRA may be removed from office. These are if the person:

- has been absent from three consecutive meetings of the GRA without the CEO's permission;
- has become bankrupt;
- has been convicted of a criminal offence punishable by imprisonment of at least 3 months;
- is incapacitated by physical or mental illness;
- is in material breach of their terms of appointment; or
- is otherwise unfit or unable to discharge their GRA functions.

If the Chief Minister is satisfied that any of the above apply, then he may declare the office in question to be vacant, following consultation with other members of the GRA. This decision must be published in the Gibraltar Gazette.

In terms of salaries and remuneration, the GRA pays the CEO and Deputy CEO such salary, pension, gratuity, compensation, expenses and allowances as set out in their appointment instrument. It also pays other expenses and allowances as it deems fit.

## Sponsorship

The GRA is accountable to the Gibraltar Parliament and not to any other government department or ministry. Section 19 of the GRA Act 2000 requires the GRA to prepare a report on its activities during each financial year, which it submits to the Chief Minister, who is then required to lay the report before Parliament. The report is expected to be prepared within three months after the end of each financial year and submitted to the Chief Minister within two weeks of being finalised.

## Funding and Spending

The GRA Act 2000[3] provides that the GRA derives its revenues from fees and charges payable to it under any Act and funds allocated to the GRA through a vote by the Gibraltar Parliament. The Act also allows the GRA to secure funds accrued to it from any other source. For example monies owed by suppliers.

The GRA does not receive any significant revenue from any other source. It is required to establish and manage a general fund into which all monies received are paid and out of which it makes all payments. It may also invest any of its funds, not required for immediate use, in banks or building societies in Gibraltar. The Income Tax Act exempts the GRA from income tax[4].

In terms of spending, the GRA Act 2000 permits the GRA to borrow money as required to enable it to discharge its functions and for the purposes of meeting capital expenditure without the requirement to provide any security against such borrowings. However, the GRA does not currently have, nor has it ever obtained, any loan.

With regard to accounts and auditing, section 13 of the GRA Act 2000 requires the GRA to keep proper accounting records of its income and other receipts and expenditures during each financial year[5] and produce a statement of its accounts within three months at the end of each financial year.

The financial statements are then audited and certified within four months of the end of that year by an auditor appointed annually by the GRA. The audit is currently carried out by Deloitte. Following its audit, the auditor is required to indicate in its report whether:

(i) it obtained all relevant information and explanations for the purposes of the audit;
(ii) proper accounting records had been kept by the GRA;
(iii) the GRA's balance sheet and accounts in the report are in agreement with the accounting records;
(iv) the accounts provide a true and fair view in the balance sheet of the GRA's finances and in the income and expenditure account of the surplus or deficit for that financial year; and
(v) the GRA discharged its obligations in relation to the collection of its revenues with diligence.

In preparing the estimates, the GRA is required to supply the Chief Minister with annual estimates of income and expenditure, including capital expenditure and any additional

[3] Section 13
[4] This is provided in section 20 of GRA Act 2000 which states: "The income of the Gibraltar Regulatory Authority shall be exempt from income tax under the Income Tax Act."
[5] "Financial year" means a period of twelve months beginning on 1 April in any year.

information required by the Chief Minister, not later than 3 months prior to the commencement of each financial year.

## Staffing

The GRA is responsible for the recruitment and retention of its staff, and the determination of their pay and conditions. It currently has a total of twenty-eight staff and is divided into four regulatory Divisions working independently of each other.

The Information Rights Division (one of the four Divisions) is responsible for data protection and works on behalf of the GRA to regulate the Data Protection Legislation, the Freedom of Access to Information on Environment Regulation 2005 and the Privacy Regulations.

The Information Rights Division has the largest number of staff within the GRA, consisting of a total of ten staff working exclusively on information rights, which at this time largely consists of data protection. The staff comprises five Information Rights Officers, two Information Rights Team Leaders, one Information Rights Manager, a Deputy Head of Information Rights and an Assistant Information Commissioner. Additionally, the CEO and the Deputy CEO of the GRA are closely involved in the decision-making and oversight of the work undertaken.

The Information Rights Division works closely with other members of staff of the GRA who provide support. For example, the GRA's front desk staff assist with the day-to-day processing of incoming and outgoing correspondence whilst the Spectrum and Operations Division of the GRA provide full IT support. Further, the GRA's Legal Advisers provide the team with specialised guidance appropriate to the statutory requirements and the high standards expected from a regulatory body.

Thus, twenty one[6] staff members are involved in the effective functioning of the Information Rights Division. In relative terms, this presents higher staffing levels per capita compared to supervisory authorities in some EU Member States.

Strict rules of **confidentiality** apply to the GRA's CEO, the Deputy CEO, employees, officials seconded to the GRA and those to whom GRA functions have been delegated, including contractors to the GRA. These are set out in Section 21 of the GRA Act 2000.

With regards to **salaries**, the GRA pays its employees and those it employs on secondment such salaries, pensions, gratuities, compensation, expenses and allowances as set out in the terms and conditions of their employment or secondment. Where relevant, the GRA pays

[6] Consisting of 10 Information Rights Division, 3 IT support, 2 legal advisers, 3 Admin/front desk, 1 DCEO, 1 CEO, 1 HR/Accounts.

persons or agencies to whom functions have been delegated and other payments for which it is liable.

In terms of performance, the Information Rights Division consists of a highly qualified workforce, with most staff members involved in the Information Rights Division's work accredited with an Honours Degree or above. Several have a masters' level qualification specifically relating to information rights.

Staff in the Information Rights Division are actively encouraged by senior management to further their education with relevant qualifications and courses aimed at expanding their knowledge of information rights matters. Collectively, the team has considerable experience in data protection and have ensured that the GDPR is being applied effectively in Gibraltar.

## Priorities

The GRA's priorities are as follows:

1. To improve standards of information rights practice through clear, inspiring and targeted engagement and influence, including the issuing of effective advice, guidance and working together with key stakeholders, including other regulators, public bodies and organisations.
2. Enforce the laws that help shape and oversee by taking fair, proportionate and timely regulatory action on investigations and prioritising issues and cases of significant public impact.
3. Maintain and develop relationships for international cooperation within the global information rights regulatory community.
4. Raise awareness of data protection and the risks to privacy from digital technology, and promote its responsible use. The aim is to empower the public with sufficient knowledge and understanding for individuals to be able to exercise their rights and make informed decisions about the opportunities offered by digital technology.
5. Stay relevant, provide excellent public service and keep abreast of evolving technology.

## PART III: INVESTIGATIONS AND ENFORCEMENT

The GRA has a strong delivery record as an independent regulator.

The GRA's investigative tasks and powers are found under Articles 57 and 58 of the Gibraltar GDPR. In particular, Article 57(1)(h) of the Gibraltar GDPR refers to investigations. Additional powers are conferred and duties imposed on the GRA by following provisions:

- Schedule 12 of the DPA 2004 – powers of the GRA (as Data Protection Commissioner).
- Schedule 13 of the DPA 2004 – other general functions of the GRA (as Data Protection Commissioner).

The GRA is empowered to carry out investigations to verify compliance with the DPA 2004 and the Gibraltar GDPR, **irrespective of whether a complaint has been made**. Matters are escalated to the GRA Board by the CEO and Deputy CEO as they consider necessary. Since 2014, the Information Division has seen an increase in its involvement in investigations, and the GRA has regularly issued decisions on investigations conducted, detailing whether or not there has been a breach of Data Protection Legislation.

Generally, the GRA's approach is to issue decisions on whether the Data Protection Legislation has been breached, taking further action where considered necessary. In this respect, it has at times taken enforcement action, either issuing an information notice or enforcement notice, and/or instigating legal proceedings.
The following sections outline the various enforcement powers available to the GRA.

### 1. Information Notices

The GRA has the power to issue information notices under Section 150 of the DPA 2004. An information notice is a formal request for a controller, processor or individual to provide the GRA with information, within a specified time frame. It is used to obtain information to assist in an investigation, usually in response to an unresponsive organisation or individual.

An information notice may require:

- a controller or processor to provide the GRA with information reasonably required for the purposes of carrying out the GRA's functions under the Data Protection Legislation; or
- any person to provide the GRA with information that the GRA reasonably requires for the purposes of-
    - investigating a suspected failure of a type described in section 155(2) of the DPA 2004 [see Enforcement Notices below] or a suspected offence under this Act, or

- determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.

The GRA has the power to issue **urgent** information notices, under which the requested information is required in no less than 24 hours.

The GRA may serve an information notice at its discretion in any investigation where it considers that action is appropriate and proportionate, having regard to the following criteria[7]:

- the risk of harm to individuals or the level of intrusion into their privacy potentially posed by the events or data processing under investigation;
- the utility of requiring a formal response within a defined time period;
- 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
- the public interest in the response.

When deciding the period for compliance with information notices, in particular the urgency, the GRA will consider:

- 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 GRA to direct the controller on, and validate, appropriate notification to data subjects and mitigation of the breach;
- the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;
- the scope of the notice, that is the scope of questions or requests in an information notice;
- the additional burden on the recipient in having to comply with a notice urgently;
- the impact on the rights of the recipient, should the GRA obtain information under an urgent information notice (which may be by court order), prior to an appeal being heard by the Magistrates' Court;
- 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
- the comparative effectiveness of other investigatory powers of the GRA.

[7] The relevant criteria is set out in the GRA's "(9) Guidance on Information Commissioner's Regulatory Action Guidance on the General Data Protection Regulation".

If a recipient of an information notice does not fully respond within the stipulated time, the GRA will consider applying for an Information Order under section 152A of the DPA 2004 or issuing a penalty notice under section 162 of the DPA 2004.

## 2. Assessment Notices

The GRA has the power to issue assessment notices under Section 153 of the DPA 2004. An assessment notice is a notice issued by the GRA to a controller or processor requiring them to allow the GRA to carry out an assessment of their compliance with Data Protection Legislation. The notice may, for example, require the controller or processor to give the GRA access to premises and specified documentation and equipment.

The GRA may serve an assessment notice at its discretion in any investigation into compliance with Data Protection Legislation. In doing so, the GRA will have regard to what action is appropriate and proportionate, and the following criteria:

- whether the GRA have conducted a risk assessment or other regulatory action and found that 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;
- where it is necessary to verify compliance with an enforcement notice;
- where 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 Data Protection Legislation;
- where the controller or processor has failed to respond to an information notice within an appropriate time.

When determining the risks of non-compliance, the GRA will consider 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, the GRA will have regard to what action is appropriate and proportionate, and criteria including:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy;
- the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;
- the scope of the notice; including the scope of the requests in an assessment notice;
- the additional burden on the recipient in having to comply with a notice urgently.

- the impact on the rights of the recipient in the event that the GRA urgently gain access to its premises and data processing activities, without the opportunity to appeal and/or for an appeal to be heard by the Court;
- 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;
- the comparative effectiveness of other investigatory powers of the GRA.

Where an assessment notice has not been complied with, section 160 of the DPA 2004 provides, by direct reference to Schedule 15 to the DPA 2004, that a judge may grant the GRA a search and seizure warrant. Schedule 15 provides the conditions under which these can be granted and what a warrant must contain.

For the purposes of this section, it should be noted that Schedule 15(15) to the DPA 2004 makes it an offence for a person to intentionally obstruct a person in the execution of a warrant issued under that Schedule; to fail without reasonable excuse to give a person executing such a warrant such assistance as the person may reasonably require for the execution of the warrant; or to make a statement, knowingly or recklessly, or a statement which is false in a material respect.

Annex B sets out procedural information in relation to assessment notices.

### 3. Enforcement Notices

The GRA has the power to issue enforcement notices under Section 155 of the DPA 2004. The purpose of an enforcement notice is to mandate action (or halt action, such as processing or transfers) to bring about compliance with information rights and/or remedy a breach. Although this is not an exhaustive list, an enforcement notice may be issued in such circumstances as:

- repeated failure to meet information rights obligations or timescales for them (e.g. repeatedly delayed subject access requests);
- where processing or transferring of information to a third country fails (or risks failing) to meet the requirements of the Data Protection Legislation;
- to ensure communication of a data security breach to those who have been affected by it;
- 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:

- who is required to take the action and why;
- the specifics of the action to be taken;

- how to report that the action has been taken;
- the timescales that apply for that action;
- any appeal/challenge process that applies.

When deciding whether to issue an enforcement notice, the GRA will have regard to the factors set out above, and 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, the GRA 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:

- 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;
- the scope of the enforcement notice;
- the additional burden or impact on the recipient in having to comply with an urgent enforcement notice within the period specified;
- the comparative effectiveness of other enforcement powers of the GRA.

If a controller or processor fails to comply with an enforcement notice, the GRA will also consider whether or not to issue a penalty notice.

## 4. Penalty Notices

The GRA has the power to issue penalty notices under Section 162 of the DPA 2004. Penalty notices are reserved 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.

The GRA may issue a penalty notice if they are satisfied that a person:

- has failed or is failing as described in section 155(2), (3), (4) or (5) of the DPA 2004 (these relates to various areas of the GDPR, including, amongst other things, the data protection principles and the rights of data subjects); or
- has failed to comply with an information notice, an assessment notice or an enforcement notice.

The GRA adopt a hierarchy and risk-based approach to penalty notices, which means that it is more likely that a penalty will be imposed where, for example:

- a number of individuals have been affected;
- there has been a degree of damage or harm (which may include distress and/or embarrassment);
- sensitive personal data has been involved;
- there has been a failure to comply with an information notice, an assessment notice or an enforcement notice;
- there has been a repeated breach of obligations or a failure to rectify a previously identified problem or follow previous recommendations;
- wilful action (including inaction) is a feature of the case;
- 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
- there has been a failure to implement the accountability provisions of the GDPR.

In considering the degree of harm or damage to individuals, the GRA 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.

The GRA's powers to impose penalty notices are more restricted where the data processing in question is for "special purposes" (namely, journalism, academic, artistic or literary purposes)( see sections 179-181 of the DPA 2004). Another restriction exists under section 163(3) of the DPA 2004 where the "Commissioner [the GRA] may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of Parliament".

*Enforcement of Penalty Notices*

Schedule 16(9) to the DPA 2004 provides the mechanism for the GRA to enforce the payment of a penalty notice. This sets out that the GRA must not take action to recover a penalty unless the period for payment of the penalty has ended (a period not less than 28 days from when the Penalty Notice was served), any appeals against the penalty notice have been decided or ended, any appeals against a penalty variation notice have been decided or ended (if relevant) and the period for appeal against the penalty, and any variation of it, has ended.

As provided in Schedule 16(9)(2) to the DPA 2004 above, the GRA is able to apply to the courts seeking an order for the payment of a Penalty Notice. Thus, in essence, a Penalty Notice is recoverable as a civil debt via the standard mechanisms of the court, and as governed by the Civil Procedure Rules of England and Wales ("CPR") which apply in Gibraltar by virtue of section 38A of the Supreme Court Act 1960 (with minor exceptions).

## Appeals

With regard to legal challenges to the GRA's use of powers, section 168 of the DPA 2004 provides avenues for appeals to the courts against information notices, assessment notices, enforcement notices and Penalty Notices.

An individual or an organisation can appeal any of the above-mentioned notices by lodging a written notice with the Magistrates' Court of Gibraltar (the "Magistrates' Court"). Individuals or organisations who wish to challenge the Magistrates' Court judgement, can appeal to the Supreme Court of Gibraltar.

## Example of Civil Enforcement Action

When a contravention is identified, the GRA's response is proportionate to the circumstances of each case. In most cases, data controllers cooperate and resolve to review their arrangements and take corrective action to ensure compliance.

In the more serious cases, the GRA may ask the data controller to sign an Undertaking. In circumstances where a data controller does not satisfactorily comply with the GRA's requests, the GRA will use its enforcement powers by issuing an enforcement or information notice and, if necessary, instigate court proceedings to enforce compliance.

An example of recent enforcement action is as follows:

- IV20/18: An enforcement notice was issued against the Civil Status & Registration Office ("CSRO") in relation to an investigation regarding an individual (the "Complainant") who had submitted a Subject Access Request ("SAR"), exercising their right of access under Article 15 of the GDPR.

  In light of the CSRO's failure to adequately respond to the GRA's requests for the CSRO to engage with the Complainant and resolve the matter, the GRA required the CSRO to provide the Complainant with a response to his SAR that was in compliance with the GDPR within one month of the enforcement notice. The CSRO provided the individual with a response to the SAR just outside the timeframe required by the notice. This was noted by the GRA, who informed the CSRO that they would consider this failure in any future regulatory developments involving the CSRO.

Annex C identifies a list of selected past cases where civil enforcement action was taken.

## Criminal Enforcement Actions

*Prosecution of Offences*

The DPA 2004 confers on the GRA the power to prosecute individuals suspected of having committed a criminal offence under the DPA 2004. Proceedings for an offence under this Act may also be instituted by or with the consent of the Attorney General.

In relation to limitation periods, summary proceedings for an offence under section 178 of the DPA 2004 (the alteration of personal data to prevent disclosure) may be brought within the period of 6 months beginning with the day on which the prosecutor first knew of evidence that, in the prosecutor's opinion, was sufficient to bring the proceedings. Such proceedings may not be brought after the end of the period of 3 years beginning with the day on which the offence was committed.

*Penalties for Offences*
Section 192 of the DPA 2004 provides the extent of liability of offenders under the DPA 2004. This sets out that some offences are liable on summary conviction to a fine not exceeding level 5 on the "standard Scale" (set out below.) These include an offence under section 128 ("Inspection of personal data in accordance with international obligations") section 161 ("authorised officers") section 178 ("Alteration etc of personal data to prevent disclosure") or paragraph 15 of Schedule 15 (Offences under "Powers of Entry and Inspection") of the DPA 2004.

Other offences are liable to a fine not exceeding the statutory maximum on summary conviction or a fine on conviction on indictment. These include offences under section 140 ("Confidentiality of information"), section 152 ("False Statements made in response to an information notice"), section 154A ("Destroying of falsifying information and documents etc" ), section 175 ("Unlawful obtaining of personal data"), section 176 ("Re-identification of de-identified personal data") or section 186 ("Prohibition of requirement to produce relevant records") of the DPA 2004.

Additionally, where a person is convicted of an offence under section 175 ("Unlawful obtaining of personal data") or section 186 of the DPA 2004 ("Prohibition of requirement to produce relevant records"), the court may order a document or other material to be forfeited, destroyed or erased if it has been used in connection with the processing of personal data, and it appears to the court to be connected with the commission of an offence. This is subject to the courts giving any other person who claims to be the owner of the material or interested in the material an opportunity to why the order should not be made.

Lastly, a person who commits an offence under section 18(6) ("Data subject access requests") of the DPA 2004 is liable on summary conviction, to a fine not exceeding level 3 on the standard scale.

For ease of reference, the Standard Scale[8] is as follows:

- Level 1 £200
- Level 2 £400
- Level 3 £1,000
- Level 4 £4,000
- Level 5 £10,000

Annex D identifies a list of cases relating to criminal enforcement action and criminal investigation.

Annex E sets out a selection of case studies detailing investigations undertaken by the GRA since 2013.

## Enforcement Statistics

The GRA have taken enforcement action at least once per year (i.e. issuing one of either an information notice, assessment notice, enforcement notice, penalty notice; instigating court proceedings; or requesting and receiving an Undertaking (where the data controller commits to carry out specific tasks to improve compliance)) between the financial years 2013/14 and 2017/18.

The most active year was financial year 2013/2014 with six enforcement actions: three information notices and three enforcement notices. This relates to 32% of all investigations that year.

The most common enforcement action taken by the GRA is the issuing of enforcement notices, 8 out of the 19 actions taken for investigations beginning between the financial years 2013/14 and 2017/18 were the issuing of enforcement notices. This relates to 42% of all enforcement actions.

## Guidance

The GRA assists organisations in complying with the requirements of the Data Protection Legislation in various ways. These include:

- providing advice, information and support to data controllers;
- self-assessment toolkits and advisory visits;
- issuing guidance notes on several areas of the Data Protection Legislation;
- dealing with ad hoc data protection related queries over the phone and by email;
- providing data protection workshops aimed at data protection officers, including delivering presentations on the Data Protection Legislation to several organisations.

[8] Schedule 9, Part A Criminal Procedure and Evidence Act 2011.

In particular, as part of its duties and responsibilities, the Information Rights Division employs different tools such guidance notes, social media campaigns and TV/media engagement to reach out to as many members of the public as possible.

During the year 2018/19 financial year, the Information Rights Division focused its resources on the creation of GDPR-related guidance, in order to assist organisations and facilitate a smooth transition to the standards under the GDPR. This included the development of several guidance notes, GDPR-centric social media campaigns and participation in GDPR related awareness-raising and training events.

Following continuous increases in the number of data protection enquiries received by the Division in recent years (by email and telephone), the year 2018/19 has seen a further notable increase of 75% in comparison to the period 2017/18. These figures highlight the Division's ever-increasing importance as a point of reference for organisations and the general public.

Annex F set out more detailed information on guidance.

## PART IV: REMEDIES AND REDRESS

Data subjects with concerns with information rights practices can pursue various remedies to enforce their rights rapidly and effectively, and ensure compliance. This can take the form of complaints to the GRA.

Complaints may result in the enforcement actions outlined earlier in Part 3, including penalties. Alternatively, data subjects may seek a **judicial** remedy. This provides for a system of independent adjudications, which allows compensation to be paid and sanctions imposed where appropriate.

Data subjects may seek a judicial remedy from the start, or they may proceed to court after having already complained to the GRA. They may also in some instances seek a judicial remedy against the GRA or lodge a complaint in relation to its service.

This part sets out the various remedies there are. It covers:

- Data subjects' ability to go to court for redress against controllers or processors, including for compensation claims;
- Data subjects' remedies in case of dissatisfaction with GRA services.

### Data subjects' ability to seek judicial redress against controllers or processors

*Bringing controllers or processors into compliance:*
Under Article 79 of the Gibraltar GDPR (right to an effective remedy against a controller) and section 172 of the Gibraltar DPA 2004, where a data subject believes their data protection rights have been breached, they can apply to the Gibraltar Magistrates Court for a compliance order requiring the data controller or processor responsible for the breach to take or refrain from action in order to secure compliance with the relevant data protection legislation.

*Compensation*
Under Article 82 of the Gibraltar GDPR (right to compensation and liability) and section 173 of the Gibraltar DPA 2004, anyone who has suffered damage (including distress) as a result of breaches of the Gibraltar GDPR may apply to the courts for a compensation order against the responsible controller or processor. Similarly, orders for compensation are available for breaches of data protection legislation apart from the Gibraltar GDPR under Section 174 of the Gibraltar DPA 2004.

As Gibraltar court processes and procedures are governed by the CPR, the court will apply its discretion when awarding costs, in accordance with Part 44.2(4) of the CPR. In doing so, the court will take the following criteria into account:

- the conduct of the parties (both at pre-action stages and during the proceedings);

- whether a party has succeeded on points in its case, even if it was not wholly successful;
- whether an offer with costs consequences under Part 36 of the CPR was made.

## Data subjects' remedies in case of dissatisfaction with GRA service

*Judicial remedies against the GRA*
The right to an effective judicial remedy against a legally binding decision of the GRA is set out under Article 78(1) of the Gibraltar GDPR. A data subject can apply to the Supreme Court for **Judicial Review** where the complaints process has been exhausted.

Judicial review is a process which is used to challenge decisions made by public bodies, where the court reviews the lawfulness of a public body's decision. Grounds for judicial review include unreasonableness, illegality, procedural unfairness, legitimate expectation, and human rights breaches.

If the court decides that the GRA has acted unlawfully, it may provide a remedy such as:

- quashing the decision and requiring the body to retake the decision;
- requiring the body to take some other step or to not take certain action;
- making a declaration; and/or
- awarding damages (in limited circumstances).

As outlined above, data subjects may also proceed to take the controller or processor to court for the matter under Article 79 of the Gibraltar GDPR and section 172 of the DPA 2004, and the court may take a differing view from any GRA decision.

Article 78(2) of the Gibraltar GDPR also provides the data subject with a right to an effective judicial remedy if **the GRA does not handle the complaint or provide the data subject with a progress update within three months**.

Provisions for this are set out in Section 171 of the DPA 2004. Data subjects may apply to the Magistrate's Court to make an order against the Commissioner. The order can require the Commissioner to take appropriate steps to respond to the complaint, or inform the complainant of progress or the outcome of the complaint, within a specified period.

*Complaints about GRA service*
Where an individual or organisation is dissatisfied with the GRA's service (including a decision taken by the GRA as Data Protection Commissioner), the matter can be referred to the GRA Board for further consideration. Currently, only one case has been referred/appealed to the GRA Board.