Explanatory Framework for Adequacy Discussions

Annex A-F to Section I3: Role of Gibraltar Regulatory Authority

Overview

These annexes are an extension to Section I3 (Gibraltar Regulatory Authority)which explains the way in which the Gibraltar Regulatory Authority meets the various adequacy requirements for an independent supervisory authority for Gibraltar. It provides further detail on:

- international engagement;
- assessment notice procedures;
- past enforcement cases, including criminal investigations;
- guidance activities and statistics.

ANNEX A - INTERNATIONAL ACTIVITIES OF THE GRA

The GRA is involved in international projects, such as the Global Privacy Enforcement Network's ("GPEN") Annual Sweeps. The GRA's work with GPEN also involves monthly teleconferences where GPEN members from across the world share their experiences and expertise.

Furthermore, the GRA has made significant contributions to the International Working Group on Digital Education. As a working group participant, the GRA is a user of the European Commission's CIRCABC collaborative online platform, through which it has actively shared its expertise and resources with other data protection authorities ("DP Authorities").

The GRA's international work in this area has contributed to local developments; in particular, it produced educational resources for teachers, including lesson plans, which integrate the International Framework developed by the Digital Education Working Group into Gibraltar's 'privacy awareness regime'. The work carried out by the GRA on this matter locally, was commended and had a specific mention at the International Conference of Data Protection & Privacy Commissioners ("ICDPPC") held in Brussels, during October 2018.

Additionally, in April 2018 the GRA participated, on the invitation of the European Commission, in the Joint Research Centre initiative called Cyber Chronix (https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/cyber-chronix), aimed at informing young European citizens about data protection and the GDPR. The GRA, alongside other regulators and researchers, reviewed a prototype of the Cyber Chronix program and provided feedback for its improvement prior to its completion.

The GRA is also a member of the Common Thread Network (the "CTN"), attending quarterly teleconferences and face to face meetings. The CTN is a forum for data protection and privacy authorities of Commonwealth countries that aims to promote cross-border cooperation.

International Cooperation and Enforcement

The GRA contributed to an ICDPPC working group dedicated to international cooperation and enforcement. In particular, the GRA attended the International Enforcement Coordination Conference hosted in Manchester by the UK's Information Commissioner. At the event, regulators exchanged ideas and experience in investigation and enforcement techniques.

The GRA also participated in discussions about the coordination of cross border case handling and enforcement coordination, which contributed to the development of a Global Cross Border Enforcement Cooperation Arrangement that was subsequently accepted at the 36th ICDPPC in Mauritius[1].

The GRA was amongst the Data Protection Authorities included in the launch of the Global Cross Border Enforcement Cooperation Arrangement in 2015, alongside the DP Authorities of Australia, Canada, British Columbia, Hungary, Isle of Man, Netherlands and the UK.

The arrangement aims to facilitate enforcement cooperation, and since October 2015 further Data Protection Authorities have signed up to participate. Amongst other things, it addresses information sharing, promotes common understandings and approaches to cross-border enforcement cooperation, and encourages authorities to coordinate cross border cooperation and to assist other authorities.

The GRA is also a member of the ICDPPC's International Enforcement Cooperation Working Group. The working group has several tasks divided amongst its members. The GRA worked on "workstream 2.2" alongside the UK's ICO. This involved researching options for international cooperation between DP Authorities, such as model clauses or agreements for cooperation.

The GRA has also been involved in several investigations which required working with Data Protection Authorities from other countries. Also, in the past five years, the GRA has significantly increased its participation and involvement in international events and projects. These are listed in the GRA's Annual Reports, which are published on the GRA's website: https://www.gra.gi/report.

Below is a summary of some of the international events attended and contributions made by the GRA:

Annual events

1. ICDPPC – The GRA attends this yearly Conference as an accredited member;

2. European Conference of Data Protection Authorities 2004 (the "ECDPA") – The GRA attends this yearly Conference, otherwise known as the Spring Conference, as an accredited member;

3. GPEN Sweeps – The GRA has participated in this annual sweep since 2014;

[1] https://icdppc.org/wp-content/uploads/2015/02/ResolutionInternational-cooperation.pdf

4. British and Islands Data Protection Authorities (BIIDPA 2004) Annual Meeting – The GRA has attended this meeting for the past 10 years. In 2017, the meeting was hosted by the GRA in Gibraltar and Data Protection Authorities from the UK, Ireland, Channel Islands, Isle of Man and Malta participated in the event. Gibraltar's Chief Minister, the Hon. Fabian Picardo, opened the event and spoke about the importance of Gibraltar maintaining EU standards on data protection post EU exit.

Other selected events

5. 2018 GDPR INFOEM/GRA Conference, Mexico – The CEO and Assistant Information Commissioner of the GRA were the main speakers at a conference organised by the INFOEM. The CEO delivered a presentation on the key points of the GDPR and the Assistant Information Commissioner delivered a presentation on the international aspects of the GDPR, focusing on the mechanisms that the GDPR provides for data to flow internationally in compliance with the law;

6. 2018 Commonwealth Data Forum, Gibraltar – The CEO and the Assistant Information Commissioner actively participated as expert speakers in the two-day forum organised by the Commonwealth Telecommunications Organisation;

7. 2018 GPEN Enforcement Practitioners Workshop, Israel – Two members of the GRA attended the second GPEN practitioner's workshop, which was held in Tel Aviv, Israel, for GPEN members. The workshop was organised by the Israeli Privacy Protection Authority and brought together speakers from different regulatory authorities and private agencies, to share and discuss practical solutions for enforcement in a Global Digital World;

8. 2018 Workshop on Delivering Accountability under the GDPR, Dublin – The Centre for Information Policy Leadership ("CIPL"), in collaboration with the Irish Data Protection Authority, hosted a practical workshop addressing how organisations can deliver accountability under the GDPR;

9. 2017 Unsolicited Communications Enforcement Network Sweep – The GRA participated in the global intelligence-gathering operation organised by the Unsolicited Communications Enforcement Network ("UCENet"). The UCENet Sweep involved 10 agencies from 6 countries visiting 902 websites and examining 6,536 consumer complaints related to affiliate marketing in their respective databases;

10. 2017 29th European Case Handling Workshop & GPEN Enforcement Practitioners Workshop, Manchester – Two members of the GRA attended the workshops hosted by the UK's ICO. They delivered a presentation and led a discussion in relation to privacy issues relating to the use of cookies in the online environment;

11. 2016 International Conference of Data Protection & Freedom of Information, Mexico – The Assistant Information Commissioner participated as a guest speaker at the International Conference of Data Protection and Freedom of Information in Mexico, organised by INFOEM[2]. The Conference brought together expert speakers from regulatory authorities from different regions, academics, and representatives of the private sector, to share and discuss experiences;

12. 2016 - 28th European Case Handling Workshop Podgorica, Montenegro – The GRA was invited to participate in the workshop, which brought together practitioners from European Data Protection Authorities, to discuss and share experiences in the investigation and handling of data protection cases. A member of the GRA delivered a presentation and led a discussion in relation to the use of cookies in the online environment and privacy notices;

13. 2014 International Enforcement Coordination Event, Manchester – The GRA attended the International Enforcement Coordination Conference hosted in Manchester by the UK's UK's ICO;

14. 2013 International Conference of Information Commissioners, Berlin – The GRA attended the 8th International Conference of Information Commissioners, which focused on Freedom of Information;

15. 2013 Visit to Facebook Headquarters, Dublin – The Irish Data Protection Commissioner, in cooperation with Facebook, arranged visits for DP Authorities to Facebook's headquarters in Dublin, with a view to better understand their product and the efforts being undertaken to ensure the protection of privacy. An officer of the GRA attended. It was a day-long event that allowed visitors to learn about Facebook and the extent to which Facebook goes to ensure compliance with relevant data protection laws. An insight into the workings of Facebook was provided by the managing director and members of his privacy team.

[2] See conference video at https://www.youtube.com/watch?v=7N1zInfN3y0&t=4939s – GRA's intervention from 1:60 onwards

ANNEX B - ASSESSMENT NOTICES - PROCEDURES

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

The GRA may require access to the specified documents and information, or classes of documents and information, which demonstrate how obligations have been met under the legislation, and the governance controls in place to monitor 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.

The GRA may also need access to specified personal data, or classes of personal data, and access to evidence that it is being processed in compliance with the legislation. The level of access sought by the GRA will be no more than the minimum required to assess compliance.

The GRA do not require access to information which:

- is subject to legal professional privilege;
- has a high level of commercial sensitivity;
- is exempt from the Gibraltar DPA 2004 by virtue of a security certificate under section 29.

The GRA 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, the GRA will ensure that properly vetted members of staff inspect such information. Where possible and appropriate, the GRA will seek to establish

memoranda of understanding with relevant bodies[3] to provide access and understanding of this type of material.

Individuals can contact the GRA to request that, if an assessment notice requires access to sensitive 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.

The GRA may need to view health and social care records. If they do, they will respect the confidentiality of this data, and will limit access to the minimum required to adequately assess compliance. Unless necessary, the GRA 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 the GRA 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.

The GRA use these reviews to evaluate how an organisation:

- obtains, stores, organises, adapts or alters information (e.g. policies and procedures) or personal data;
- ensures the confidentiality, integrity and availability of the data or service it provides;
- retrieves, consults, or uses the information or personal data;
- discloses personal data by transmitting or disseminating or otherwise making the data available;
- purges and destroys personal data.

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

[3] For example law enforcement authorities.

obligations under the legislation. It 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, the GRA 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:

- staff and contractors;
- any processor's staff;
- staff of relevant service providers as specified in the assessment notice.

The GRA 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, the GRA will schedule and agree interviews with the controller or processor before the on-site audit. It 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.

The GRA 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. The GRA will take notes during the interviews.

The GRA 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, they will arrange this with the consent of the controller. Similarly, the schedule will not prevent the GRA 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.

ANNEX C - LIST OF SELECTED CIVIL ENFORCEMENT ACTIONS

1. Information Notices

IV08/13

- On 8th November 2013, the GRA issued Dolphin Safari with an information notice under Section 27 of the DPA 2004 prior to its amendment following the GDPR, (the "Old DPA"), requesting information to ascertain whether they had breached the Old DPA;

- The matter involved a complaint received on 11th October 2013, regarding an alleged recording of a private conversation by Dolphin Safari;

- The GRA had made an initial attempt to engage with Dolphin Safari to establish the facts of the case and investigate the matter, however Dolphin Safari did not willingly collaborate and provide the GRA with the information requested. The information requested was provided and the investigation continued.

IV16/15

- A complaint was received against the Gibraltar Taxi Association concerning the unlawful obtaining and disclosure of personal data, namely relating to the GPS data collected by Taximeters, on 15th December 2015. The GRA required information from the GTA to progress with the complaint

- An information notice was issued on 26th August 2016 under Section 27 of the Old DPA, which requested information in relation to the use of GPS data, as well as other information to assist in the matter;

- The information was provided and the GRA continued with the investigation.

IV06/16

- A complaint was received on 20th July 2016 regarding the use of cookies by WHG (International) ("WHG");

- An information notice was issued to WHG under Section 27 of the Old DPA. It was issued on 31st January 2017. This required the organisation to provide information regarding the use of a cookie by WHG, as well as how they complied with a Subject Access Request received from an individual;

- The information was provided, and the investigation continued.

2. Enforcement Notices/Court Proceedings

IV09/13

- A complaint was received from an individual on 11th October 2013, alleging that a private conversation between him and other individuals (the "Recording"), had been obtained and disseminated publicly by two other persons without his knowledge and consent;

- The GRA issued an enforcement notice on 3rd December 2013 requiring that individuals who were said to have recorded a private conversation remove the conversation from the internet or elsewhere and destroy the recording;

- After the individuals appealed the enforcement notice to the Magistrates Court, it was ruled that the individuals were not to disseminate otherwise process the recordings other than in the course of legal proceedings issued by them in the Supreme Court of Gibraltar.

IV20/14

- The GRA issued an enforcement notice on 28th August 2015, under section 26 of the Old DPA, requesting that an employee of an organisation cease processing personal data in documents that had been unlawfully obtained, destroy all copies held and provide written confirmation to the GRA once this was undertaken;

- The enforcement notice was appealed to the Magistrates Court of Gibraltar by the employee. However, prior to the hearing in the Magistrates Court, the GRA received written confirmation from the employee advising that the personal data had been shredded. In light of the confirmation, the GRA cancelled the notice and the employee withdrew the appeal.

IV21/15

- The GRA issued an enforcement notice on 27th July 2019, requesting that HM Customs produce and submit a policy, and provide written confirmation to the GRA once this was undertaken. The matter involved HM Customs not having appropriate security measures to protect the images captured and recorded by their CCTV System from being deliberately or accidentally compromised. The enforcement notice was issued under section 26 of the Old DPA;

- The GRA also requested for HM Customs to take all reasonable steps to ensure that all staff members and any other individuals who may have access to any personal data processed by HM Customs, are aware of the policy. The GRA received written confirmation from HM Customs advising that the enforcement notice had been complied with and a copy of the policy was provided to the GRA.

IV09/16

- The GRA issued an enforcement notice under section 26 of the Old DPA on 13th December 2016 requiring amongst other things, that Utopia cease the processing of CCTV footage via the cameras (other than the two cameras, which focused on the property of Utopia), and amend the CCTV signs used to provide data subjects with the information specified in section 10(2) of the Old DPA. The GRA received written confirmation from Utopia that the CCTV cameras (other than the two cameras which focused on the property of Utopia) had stopped being used. However, Utopia, had not, within the specified timeframe, amended the CCTV signs as per the terms of the notice;

- Consequently, in failing to comply with the terms of the notice, Utopia committed an offence under section 26(8) of the Old DPA. Notwithstanding the above, a site visit undertaken by the GRA's office confirmed that the CCTV signs had been amended to provide individuals with the information specified in section 10(2) of the Old DPA. This was later confirmed by Utopia in writing.

IV06/16

- On 24th November 2017, the GRA issued WHG (International) Limited ("WHG") with an enforcement notice under section 26 of the Old DPA, requiring the organisation to take corrective action to ensure compliance regarding its use of cookies;

- The GRA also instigated legal proceedings on 19th March 2018 for a failure to comply with the enforcement notice, requiring WHG to take corrective action in relation to informing individuals to their site about the use of cookies. This was issued as a result of WHG's failure to comply with the requirements of the enforcement notice without reasonable excuse, under section 26(8) of the Old DPA. The matter was withdrawn from the Magistrates Court when the requirements of the notice were satisfactorily actioned through an Undertaking.

IV01/17

- An enforcement notice was issued on 18th August 2017 to Oxford Learning College, requiring them to provide a complainant with his personal data in response to the Subject Access Request;

- After a complaint was received on 14th June 2017, the GRA investigated the matter and found that Oxford Learning College did not comply with a subject access request and were in breach of section 14 of the Old DPA. Following the issuing of the enforcement notice, it was found that Oxford Learning College deleted the personal data;

- Therefore, in October 2017, the GRA instigated court proceedings against Oxford Learning College for unlawfully deleting the complainant's personal data despite being bound to comply with the Subject Access Request, contrary to section 7(1) of the Old DPA, which required that for processing of personal data to be legitimate, section 6 of the Old DPA needed to be satisfied, which in turn required personal data to be processed lawfully;

- At the court hearing, Oxford Learning College pleaded guilty and were fined £1,000.

3. Undertakings

IV02/15:

- A complaint was received on 8 May 2015 against the Ministry for Housing (the "Ministry"). The complainant stated that the parking permits (the "Permits") issued by the Ministry for the parking spaces at an estate disclosed excessive personal information;

- Following the GRA's decision on the matter, the Ministry signed an undertaking issued on 21st August 2015 in relation to the Permits to ensure that they were replaced with Permits that do not display the address of the Permit holders.

ANNEX D - LIST OF CASES RELATING TO CRIMINAL ENFORCEMENT ACTION AND CRIMINAL INVESTIGATIONS

1. Court Proceedings

IV 01/17

- As highlighted earlier, an enforcement notice was issued on 18th August 2017 to Oxford Learning College, requiring them to provide a complainant with his personal data in response to the Subject Access Request;

- After a complaint was received on 14th June 2017, the GRA investigated the matter and found that Oxford Learning College did not comply with a subject access request, in breach of section 14 of the Old DPA. Following the issuing of the enforcement notice, it was found that Oxford Learning College deleted the personal data. This was contrary to section 7(1) of the Old DPA, which required that for processing of personal data to be legitimate, section 6 of the Old DPA needed to be satisfied, which in turn required personal data to be processed lawfully;

- Therefore, as previously stated, in October 2017, the GRA instigated court proceedings against Oxford Learning College for unlawfully deleting the complainant's personal data despite being bound to comply with the Subject Access Request;

- At the court hearing, Oxford Learning College pleaded guilty and were fined £1,000.

2. Criminal Investigations

On certain occasions, the GRA have found that individuals have committed an offence under section 12 of the Old DPA. This used to state that it was an offence for individuals to knowingly, or recklessly, without the consent of the data controller, obtain or disclose personal data. Some of these are set out below:

IV20/14

- A complaint was received on 18th February 2015 from the Gibraltar Broadcasting Corporation (the "Complainant") against one of its employees (the "Employee"). It was alleged that whilst working for the Complainant, the Employee had obtained and processed personal information pertaining to the Complainant's employees and third parties from the Complainant's files (the "Documents") for personal matters that were outside of the Employee's role specification;

- The GRA undertook an investigation which established, on 1st June 2015, that amongst other things an employee had obtained and used personal data, and therefore become a data controller. However, the Employee obtained and used personal data without the consent of the Complainant and/or the data subjects. The Employee's obtaining and use of the personal data without the Complainant's consent was in contravention of section 12 of the Old DPA, and therefore an offence. Please refer to the above section for an enforcement notice that was issued on the matter.

IV10/15

- On 3rd August 2015, the GRA became aware of a data breach that occurred at a gambling company where the full names and corresponding telephone numbers of 68,687 customers (the "Personal Data") were illegitimately copied and obtained by an individual (the "Perpetrator") who was allegedly selling the Personal Data to other third parties. Amongst other things, on 22nd December 2015, the GRA concluded that the Perpetrator obtained and used the Personal Data without the gambling company's consent and in contravention of section 12 of the Old DPA, and therefore committed an offence.

IV21/16

- On 9th March 2017 the GRA received information regarding a Borders and Coastguard Agency ("BCA") employee who appeared to have obtained and disclosed CCTV images (the "Images") originating from a CCTV system (the "CCTV System") operated at the Gibraltar International Airport by Gibraltar Air Terminal Limited ("GATL"), in breach of the Old DPA. Amongst other things, on 22nd August 2017 the GRA issued a decision where it was found that the employee had committed an offence under section 12(1) of the Old DPA by obtaining and disclosing the Images without the consent of the data controller.

ANNEX E - CASE STUDIES ON INVESTIGATIONS

Below details a selection of investigations undertaken by the GRA since 2013 and provides the following information:

- A selection of six case studies from the investigations undertaken since 2013, one for each year.
- These are provided in addition to the investigations identified in Annex C and Annex D above where either enforcement action was taken, or the matter related to criminal enforcement action or criminal investigations.

2013/14 Reporting Period

- Case Study 1 – Ref: IV05/13 Individual A vs Individuals B:

An individual (the "Complainant") stated that another individual (the "Individual") on social media, claimed to possess correspondence with information relating to him.

The GRA initiated an investigation and made attempts to engage with the Individual to establish the facts of the case. However, the Individual did not reply and did not provide the GRA with the information requested. Therefore, the GRA served the Individual with an information notice, under section 27 of the Old DPA, requiring the Individual to provide the GRA with specific information within a prescribed timeframe.

The Individual responded to the GRA's information notice with the information requested above. The GRA examined the information obtained from various sources, including the Individual, and established the following:

- Documents were identified, which included personal data relating to several individuals;

- The Individual was in contravention of the Old DPA as there was no legitimate reason for them to possess the information identified, and/or process it in any other way;

- Whilst the documents contained personal data relating to several individuals, no personal data was being processed about the Complainant, and consequently there was no breach of the Old DPA with regards to the Complainant's personal data.

Said documentation was obtained from the Individual, and the Individual was notified that any further processing of the information relating to the case would be in breach of the DPA and appropriate action would be taken.

2014/15 Reporting Period

- Case Study 2: Ref IV17/14 Electoral Registration Office

The GRA became aware that in order to compile the 2015 Register of Electors (the "Register") the Electoral Registration Office ("ERO") was sending out an Electoral Registration Form (the "Form") to the address of citizens potentially able to vote in the forthcoming general elections ("Potential Electors"), asking them to check personal data contained on the Form. The GRA identified potential data protection issues arising out of the Form.

Consequently, the GRA undertook an investigation, which established the following:

- The Forms were sent out to Potential Electors including, where available, the particulars of the persons residing at the address. This included the name, address, identity card/passport/civilian registration number ("ID Number"), and date of birth of individuals (the "Information");

- Individuals were asked to check that the Information was accurate and correct, sign the Form and send it back to the ERO. The pre-populated Forms included a bar code, which could be scanned to add the Information into the Register;

- The Forms were considered to simplify and expedite Electoral Registration for Citizens, which would result in a higher response from Potential Electors that would reduce the risk of Potential Electors being disenfranchised, and also improve efficiency by minimising the manual input required by the ERO

- Given time and resource constraints, the ERO considered that using the pre-populated Forms was the only practicable way in which to compile the Register;

- The GRA became aware of Forms that had been sent to addresses with the details of previous tenants who no longer lived there. It was considered likely that this would have happened on numerous occasions given the significant number of Potential Electors likely to have moved residence between the compilation of each Register.

Section 7(1)(d)(iii) of the Old DPA stated that processing of personal data was legitimate if necessary for the performance of a function of the Government. To this extent, the GRA determined that the processing of the Information was legitimate. However, the GRA also determined that the ERO had not processed the Information with appropriate organisational and technical security measures to protect personal data against accidental or unlawful forms of processing, including unauthorised disclosure or access, as required by section 6(1)(d) of the Old DPA.

Following the GRA's decision, the ERO undertook to review its arrangements to ensure that appropriate organisational and technical security measures were taken in the future to

protect personal data against accidental or unlawful forms of processing, including unauthorised disclosure or access, as required by section 6(1)(d) of the Old DPA.

2015/16 Reporting Period

- Case Study 3 – Ref: IV015/14 The Anchorage Management Limited

A complaint was received by an individual against The Anchorage Management Limited ("TAML"). The Complainant alleged that the processing of personal data through the implementation of a biometric data system (the "System") at The Anchorage residential gymnasium (the "Gym") was excessive and disproportionate when other less intrusive alternatives could be pursued.

The GRA undertook an investigation, key points of which can be summarised as follows:

The Complainant was a resident at the Anchorage. The Gym was for the exclusive use of residents at the Anchorage, who pay for its upkeep.

Following engagement with the GRA, TAML confirmed that the purpose of the System was to control access and prevent non-residents from entering the Gym. A considerable risk of unauthorised use of the Gym by non-residents had been identified, which resulted in unfair costs to residents at the Anchorage. Various methods, which included installation of CCTV cameras, the use of a key code system and key cards were found to be ineffective to control access to the Gym by non-residents. The System collects limited points of a fingerprint which are recorded against the name of a resident, apartment number, telephone number and timestamps showing entry into the Gym. This is regarded as personal data, which was regulated by the Old DPA.

The GRA determined that TAML had a legitimate interest in the implementation of access controls for the Gym and the System was effective in meeting the need to access control. However, section 6(1)(c)(iii) of the Old DPA stated that processing of personal data needs to be adequate, relevant and not excessive in relation to the purpose for which it is collected. Although TAML had been unsuccessful at using alternative methods to control access to the Gym by non-residents, the GRA determined that these less intrusive methods could be effective and therefore, the System appeared to be excessive, in contravention of section 6(1)(c)(iii) of the Old DPA.

Consequently, the processing of personal data did not meet the criteria for the legitimate processing of personal data under section 7(1) of the Old DPA, and therefore the processing by the System was in contravention of the Old DPA. Following the GRA's determination, TAML modified and replaced the System as the only means of access to the Gym by introducing an alternative method of entry, namely a card reader, which users could use if

they would not give consent for the use of the biometric system. Further, they confirmed that letters were issued to all residents informing them of this alternative means of access.

2016/17 Reporting Period

- Case Study 4 Ref: IV02/16 Beachview Terraces Limited:

The GRA became aware of an incident concerning images of CCTV footage (the "Images") that originated from a CCTV system run by Beach View Terraces Management Limited ("BVT") which were posted on Facebook by a member (the "Individual") of the Beach View Terraces Residents Committee (the "Committee").

The GRA undertook an investigation which concluded that BVT granted the Individual authorised and unlimited access to the CCTV system without any guidance or rules regarding its use, and therefore, BVT did not have appropriate organisational and technical security measures in place to protect against the unlawful disclosure of the Images. Consequently, BVT's processing of personal data, through the CCTV System, was in contravention of section 6(1)(d) of the Old DPA.

Further, the GRA concluded that the disclosure of the Images on Facebook was incompatible with the purpose of the CCTV System and therefore, BVT processed personal data in contravention of section 6(1)(c)(ii) of the Old DPA.

In addition, the CCTV signs displayed within the residential estates of Beach View Terraces did not identify BVT as the data controller of the CCTV system, and therefore did not comply with the transparency requirements in section 10(2) of the Old DPA.

Following the GRA's decision and intervention, BVT reviewed their arrangements to improve compliance with the Old DPA.

2017/18 Reporting Period

- Case Study 5 – Ref: IV19/17 St Bernard's Hospital

In or around August 2017, in response to a verbal request for information by an individual ("Individual B"), St Bernard's Hospital ("SBH") released the records of the complainant (the "Complainant") to Individual B, who had a similar name. The records disclosed to Individual B contained the Complainant's records, as well as the records of Individual B.

SBH's disclosure of the Complainant's medical records to Individual B, which included sensitive data, did not meet the conditions in Articles 6 and 9 of the GDPR (section 7 and 8 of the Old DPA).

SBH had also incorrectly mixed and placed together the records of the two different patients due to not having reasonable measures in place to ensure the accuracy of the personal data and sensitive data that they processed. SBH therefore also breached Article 5(1)(d) of the GDPR (section 6(1)(b) of the Old DPA).

Further, SBH did not have appropriate organisational and technical security arrangements in place to protect personal data from being accidentally or deliberately compromised as per Articles 5(1)(f) and 32 of the GDPR (sections 6(1)(d) and 11 of the Old DPA). This was based on the lack of measures in place to verify and validate access requests or the information released in response, the lack of policies and procedures in place to detect and/or manage data breaches and the lack of data protection training and awareness amongst SBH staff.

Following the issuing of the decision, and on the request of the GRA, SBH took corrective and the GRA considered the matter closed and the case resolved. Notwithstanding that the GRA considered the matter resolved, the GRA notified SBH of their intention to conduct an inspection by the end of 2019, focusing on areas relating to the breach.

2018/19 Reporting Period

- Case Study 6 – Ref: IV32/18 Bet365

The GRA received a complaint from an individual (the “Complainant”) in relation to a Subject Access Request (“'SAR'') that was submitted to Hillside (Gibraltar) Limited (“Bet365”,) by letter requesting personal data on an account with Bet365. The Complainant stated that Bet365 refused to provide him with the information requested in the letter, which requested "any personal data" held about him by Bet365.

In response, Bet365 stated that they were unable to provide the Complainant with the information “due to data protection regulations.” It was Bet365’s position that the Complainant was not the data subject of the account and to disclose information on him would breach the GDPR, as the Complainant had declared that the account was not his.

The GRA found that the account had personal data pertaining to the Complainant and the SAR should have been processed in accordance with Articles 12 and 15 of the GDPR. The response to the SAR was also in contravention of Article 12(4) of the GDPR which requires data controllers to "inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.”

The GRA required Bet365 to respond to the SAR in accordance with Articles 12 and 15 of the GDPR, and further issued Bet365 with a reprimand under section 124 of the DPA 2004 and Article 58(2)(b) of the GDPR.

ANNEX F - GUIDANCE

As part of its duties and responsibilities, the Information Rights Division of the GRA provides advice and information to the public on data protection related matters. The Information Rights Division uses different tools to achieve this and reaches out to as many members of the public as possible. These are summarised below.

Guidance notes

Guidance Notes form a key part of the Division's duty to inform the public of data protection issues and has been fundamental since the Old DPA and subsequently when the DPA 2004 and the GDPR became law in Gibraltar. The GRA uses the same type of structure as other jurisdictions, such as the Information Commissioner's Office in the UK, when producing guidance notes and therefore each guidance note targets a particular topic of data protection. To date, the GRA has issued several guidance notes for organisations and individuals and, most recently, have focused on specific areas of GDPR as follows:

GDPR Guidance Notes

- GDPR (1) Getting started;
- GDPR (2) Lead supervisory authority;
- GDPR (3) Data protection officer;
- GDPR (4) Data protection impact assessment;
- GDPR (5) Data portability;
- GDPR (6) Identifying the lawful basis;
- GDPR (7) Guidance for SMEs;
- GDPR (8) Guidance on personal data breach notification;
- GDPR (9) Guidance on the Information Commissioner's Regulatory Action; and
- GDPR (10) Getting ready for Brexit;
- GDPR (11) International transfers;
- GDPR (12) Data protection and Brexit for Law Enforcement Processing;
- GDPR (13) Guidance on consent;
- GDPR (14) Guidance on the use of CCTV;
- GDPR (15) The right of access.

The GRA has also issued other guidance notes aimed at organisations and individuals alike, which pre-date the implementation of the GDPR, but nonetheless remain available. These are the following:

Guidance for individuals (pre-GDPR):

- Privacy and data protection overview;
- Guidance dealing with SAR;
- Identity theft;

- Finding out what information is held about me;
- Accessing information about you;
- What's it all about; and
- A guide for people.

Guidance Notes for Data Controllers (pre-GDPR):

- Guidance dealing with SAR;
- Data protection guidance for EU Referendum campaign groups;
- Requests to obtain Certificates of Good Conduct;
- Use of cookies in websites;
- Opinions given in confidence;
- Monitoring of staff;
- A guide for business, organisations & public bodies;
- CCTV systems;
- Transfer of personal data outside of Gibraltar;
- Dealing with Subject Access Requests;
- Standard model clause;
- Are you a data controller or data processor?
- Assess your own DP policy; and
- Pre-employment vetting.

To view the GRA's Guidance Notes, please visit https://www.gra.gi/data-protection

Ad-hoc data protection enquiries

The GRA regularly responds to data protection related queries, which come in the form of enquiries either by telephone, email, letter or requests for a meeting. Each enquiry is assigned a unique reference number and can often be resolved by email or telephone.

In order to keep track of the number of inbound enquiries received, the GRA maintains an excel sheet broken down into categories of queries received from the public sector, the private sector and from individuals for each financial year.

The table showing the number of enquiries dealt by the GRA in the last twelve years:

Years	Public Sector	Private Sector	Individuals	Total
2007/2008	26	18	6	50
2008/2009	37	36	6	79
2009/2010	41	34	14	89
2010/2011	30	36	20	86
2011/2012	32	44	12	88

2012/2013	38	60	16	114
2013/2014	68	61	8	137
2014/2015	61	58	7	126
2015/2016	48	71	13	132
2016/2017	68	102	14	184
2017/2018	59	149	6	224
2018/2019	53	323	22	398
Total	561	992	144	1707

Social media campaign

To generate more awareness about the work that the GRA does and to reach a larger audience, the GRA embarked on a social media campaign which gives information on various social media platforms such as Facebook, Twitter and LinkedIn.

Since 2015, the GRA's social media posts have carried a range of information, including, but not limited to:

- conferences members of the GRA have attended;
- data protection presentations the GRA have provided;
- results of school surveys carried out on privacy and social media;
- relevant and current topics on data protection.

Recently, many of the social media posts have focused on a particular area of data protection, and these posts run over a number of weeks to give as much information on that topic as possible. A few examples of these are:

- Know Your Data Protection Rights;
- Know Your Responsibilities;
- GDPR Data Protection Rights;
- GDPR Data Protection Officer; and
- GDPR Data Protection Impact Assessment.

To view the social media posts released by the GRA, please visit the following social media platforms:

- https://www.facebook.com/GibraltarRegulatoryAuthority;
- https://twitter.com/Gibprivacy ;
- https://www.linkedin.com/company/gibraltar-regulatory-authority

Data protection workshops

In recent years, the GRA has engaged in various data protection workshops, where it delivers presentations on the Data Protection Legislation followed by a question and answer

session with the audience. The workshops aim to provide an overview of data protection laws and are normally arranged at the request of an organisation that wants to train or raise data protection awareness amongst its staff. The aim of these workshops is to promote and raise data protection awareness and to engage with as many different professionals and sectors as possible.

Examples of workshops that the GRA has held are:

- HMGoG departments – five workshops were held with a combined total of around 200 participants from Gibraltar's public sector. The workshops were arranged with the HMGoG's Human Resources Department;

- Royal Gibraltar Police – three workshops were held with a combined total of around sixty participants;

- The Teachers' Union – one workshop was arranged with the Gibraltar Teachers Association, predominantly involving head teachers, deputies and heads of department, with a combined total of around twenty participants;

- Land Property Services – one workshop was held with its staff members;

- The Bassadone Group, a company from the private sector – one workshop was held with senior staff members;

- The Bland Group, a company from the private sector – one workshop held with senior staff members;

- Gibraltar Association of Compliance Officers – one workshop held with around eighty members from different business sectors;

- Gibraltar Branch of the Chartered Institute of Personnel and Development – one workshop held with members from different business sectors;

- Gibraltar Branch of the Chartered Institute of Personnel and Development – the GRA attended a question and answer panel on the Gibraltar GDPR. There were around thirty members in attendance from both the public and private sector;

- Kusuma Trust GDPR Workshop for Charities where the GRA was invited, alongside a local law firm, to participate in a GDPR workshop designed to assist charities in their journey to become GDPR compliant.

The GRA also organises periodic data protection workshops for Data Protection Officers ("DPOs") in Gibraltar, as part of efforts to promote awareness and provide assistance to

data controllers and DPOs in relation to their data protection obligations. The workshops present DPOs with an opportunity to broaden their understanding of data protection law. The workshops are also an opportunity for the GRA to obtain a better insight into the issues/challenges faced by data controllers and DPOs. Further, the workshops provide a platform that promotes discussion and facilitates collaboration between DPOs (https://www.gra.gi/workshops-for-dpos).

The first round of workshops were held in March 2019, presenting DPOs with an opportunity to broaden their understanding of data protection law and provided an opportunity for the GRA to obtain a better insight into the issues/challenges faced by data controllers.

TV/media engagement

The GRA has on various occasions engaged with the media in Gibraltar, normally in response to a press release that has been issued by the GRA. This engagement has led to interviews in local television programmes, radio programmes and newspapers. Selected examples of media engagement involving members of the GRA in recent years include the following:

- 2019: GRA interview on awareness raising program with schools;
- 2018: The Assistant Information Commissioner took part in a discussion panel on a television program regarding topical data protection and privacy related matters;
- 2018: Interview on the commencement of the GDPR;
- 2017: Interview with a local newspaper in which the CEO discussed the GDPR;
- 2017: Interview with the Information Rights Manager on the participation and results of a UCENet Sweep that was aired on a local radio station;
- 2017: A live television interview in which the Assistant Information Commissioner discussed a GDPR Guidance note released;
- 2017: A television interview in which a member of the GRA spoke about an article in a UK newspaper about children's privacy rights and social media;
- Several television and radio news interviews conducted by the Information Rights Manager of the GRA regarding the GPEN Sweeps;
- An interview with a member of the GRA on a local radio station, regarding the results of the school surveys on privacy and social media;

- Several interviews with members of the GRA on both local television programmes and newspaper articles promoting the "Data Protection Days" held by the GRA.

Data Protection Day

As part of the "Control Your Privacy Campaign", the GRA has been promoting and conducting a yearly "Data Protection Day" since 2014, which sees staff members from the GRA, as well as the CEO and Deputy CEO, engage directly with members of the public to generate and promote awareness in data protection.

Data Protection Day is held in the town centre and sees the GRA set up a table with useful material. Further, staff members engage with members of the public by providing them with promotional material, including flyers and guidance notes, as well as having general discussions on matters relating to privacy.

In support of Data Protection Day, other regulatory bodies and organisations are invited to attend in support of the event. This includes the Office of the Ombudsman, the Royal Gibraltar Police and the Office of Fair Trading.

Education and Awareness

The Division's "Control Your Privacy" campaign with schools in Gibraltar entered its seventh year since its launch in the academic year 2013/2014. This campaign has progressively developed to establish a yearly awareness raising framework involving middle and comprehensive schools, which is undertaken in cooperation with Gibraltar's Department of Education. In this respect, members of the Information Rights Division of the GRA attend the schools to deliver presentations to students, followed by a question and answer session. Students are also asked to complete a privacy survey. The results of the survey are published in a report. The latest report also analyses the results alongside the survey results of the three previous academic years, in order to identify any key changes or behavioural trends in privacy practices amongst students in Gibraltar when they use digital technology.

Over the years, it has covered year 7 students from Gibraltar's middle schools, years 9 and 11 students from Bayside School (Gibraltar's comprehensive school for boys), and year 11 students from Westside School (Gibraltar's comprehensive school for girls). It has also covered students aged fifteen and over from the Gibraltar College, years 7 and 9 students from Loreto Convent, a local private school, as well as years 8 and 9 students from Prior Park School, a further local private school.

The purpose of the survey is to obtain information on the extent of the use of Social Network Sites ("SNS") and mobile devices amongst students between the ages of eleven

and eighteen. The surveys served to learn about the habits of these students in relation to SNS, in particular, which SNS are being used, the reasons and frequency of use, and the extent to which available privacy controls are being used.

Below is a summary of the number of students who participated in the surveys/report for each academic year. For further information on the findings of the reports please refer to the relevant section of the GRA's webpage, found here:
https://www.gra.gi/dataprotection/public-awareness

2013-2014	The survey was completed by 378 students, consisting of 192 boys and 186 girls. This survey focused on year 7 students only i.e. students aged eleven to twelve.
2014-2015	The survey covered 893 of Gibraltar's students, consisting of 558 boys and 335 girls. It encompassed all year 7 students, year 9 and year 11 students from Bayside School, year 11 students from Westside School and students aged fifteen and over from the Gibraltar College.
2015-2016	The survey comprised of 833 students, consisting of 541 boys and 292 girls, with most being between the ages of eleven and eighteen, and a minority being over 18. All year 7 students were surveyed, as were year 9 and year 11 students from Bayside School, year 9 students from Loreto Convent, year 11 students from Westside School and students aged 15 and over from the Gibraltar College.
2016-2017	The survey comprised of 818 students, consisting of 532 boys and 286 girls, with most being between the ages of 11 and 18, and a minority being over 18. Year 7 students were surveyed, as were year 9 and year 11 students from Bayside School, year 8 students from Prior Park (a new private school) and year 11 students from Westside School.
2017-2018	The survey comprised of 841 students, consisting of 481 boys and 360 girls, with most being between the ages of 11 and 18, and a minority being over 18. Year 7 students were surveyed, as were year 9 and year 11 students from Bayside School, year 8 and 9 students from Prior Park, year 11 students from Westside School and students aged seventeen and over from the Gibraltar College.
2018-2019	The survey comprised of 1038 students, consisting of 538 boys and 500 girls, with most being between the ages of 11 and 16. Year 7 students were surveyed, as were year 9 and year 11 students from Bayside School and Westside School, year 8 and 9 students from Prior Park, and students aged 15 and 16 from the Gibraltar College.

Additionally, as previously mentioned, the GRA has this year developed educational resources, which teachers can use to teach students on privacy and data protection. Two packs have been developed – one for middle schools and one for secondary schools. The lesson plans integrate into Gibraltar's 'privacy awareness regime' an International Framework, which was developed by an international working group on digital education that the GRA forms part of. The framework was adopted globally by the ICDPPC.

Codes of Practice

Recognising that under the right circumstances and for the right reasons, data sharing between organisations can be beneficial to society and individuals, the GRA released a Data Sharing Code of Practice (the "Code").

This Code provides good practice for the sharing of personal data and delivers a general framework, which organisations can use to develop their own data sharing agreements. Each organisation must adapt it in accordance with their circumstances, taking into account the nature of the data involved and type of data sharing e.g. frequency (ad hoc or routine), electronic/hard copies, etc.

For more information, please refer to the GRA's website at https://www.gra.gi/data-protection/documents/codes-of-practice/data-sharing-code-of-practice