GRA
GIBRALTAR REGULATORY AUTHORITY

ico.
Information Commissioner's Office

Date: 25 October 2022

Memorandum of Understanding

between

The Gibraltar Regulatory Authority

as

the Information Commissioner for Gibraltar

- and -

The Information Commissioner

for

the United Kingdom of Great Britain & Northern Ireland

for Co-operation in the Regulation of Laws Protecting Personal Data

GRA
GIBRALTAR REGULATORY AUTHORITY

ico.
Information Commissioner's Office

Introduction

1. This Memorandum of Understanding **("MoU")** establishes a framework for co-operation and information sharing between:

(a) The Gibraltar Regulatory Authority as the Information Commissioner for Gibraltar **(the "GRA")**; and

(b) The Information Commissioner for the United Kingdom of Great Britain & Northern Ireland **(the "ICO")**,

each referred to as a **"Party"** and together referred to as the **"Parties"**.

2. The Parties recognise the nature of the modern global economy, the increase in circulation and exchange of personal data across borders, the increasing complexity of information technologies, and the resulting need for increased cross-border enforcement co-operation.

3. The Parties acknowledge that they have similar functions and duties for the protection of personal information in their respective jurisdictions.

4. This MoU reaffirms the intent of the Parties to deepen their existing relations and to promote exchanges to assist each other in the enforcement of laws protecting personal information.

5. This MoU sets out the broad principles of collaboration between the Parties and the legal framework governing the sharing of relevant information and intelligence between them.

6. The Parties confirm that nothing in this MoU should be interpreted as imposing a requirement on the Parties to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would breach their legal responsibilities, including:

(a) In the case of the ICO, the Data Protection Act 2018 **(the "UK DPA")** and/or the United Kingdom General Data Protection Regulation **(the "UK GDPR")**;

(b) In the case of the GRA, the Data Protection Act 2004 **(the "Gibraltar DPA")** and/or the Gibraltar General Data Protection Regulation **(the "Gibraltar GDPR")**.

7. This MoU sets out the legal framework for the Parties' ongoing collaboration, but it is for each Party to determine for themselves that any proposed activity is compliant with the law applicable to them.

The role and function of the GRA

8. The GRA is established by statute as Gibraltar's Information Commissioner, functioning as an independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

9. The GRA is empowered to take a range of regulatory action for breaches of, inter alia, the following legislation (as amended from time to time):

(a) Gibraltar DPA;

(b) Gibraltar GDPR;

(c) Data Protection (Search and Seizure) Regulations 2006;

(d) Communications (Personal Data and Privacy) Regulations 2006 **(the "Privacy Regs")**;

(e) Freedom of Access to Information on the Environment Regulations 2005 **(the "Gibraltar EIR")**; and

(f) Freedom of Information Act 2018 **(the "Gibraltar FOI").**

10. Article 57 of the Gibraltar GDPR and Section 124 of the Gibraltar DPA place a broad range of statutory duties on the GRA, including monitoring and enforcement of the Gibraltar GDPR and Gibraltar DPA, promotion of good practice and adherence to the data protection obligations by those who process personal data in Gibraltar. These duties sit alongside those relating to the other enforcement regimes outlined in paragraph 9 above.

11. The GRA's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the Gibraltar DPA and Gibraltar GDPR;

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

(c) 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;

(d) administering fines by way of penalty notices in the circumstances set out in section 162 of the Gibraltar DPA;

(e) issuing decision notices detailing the outcome of an investigation under the Gibraltar FOI and Gibraltar EIR; and

(f) prosecuting criminal offences relating to the protection of personal data before the Courts.

12. Regulation 31 of the Privacy Regs, also provides the GRA with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach the Privacy Regs. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of the Privacy Regs, including automated telephone calls made without consent, telephone calls which have not been screened against the Opt-Out Register [1], and unsolicited electronic messages (Regulations 22, 23 and 24 of the Privacy Regs respectively.)

13. Article 50 of the Gibraltar GDPR requires the GRA to, in relation to third countries and organisations, take appropriate steps to, inter alia:

(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

The role and function of the ICO

[1] This service is provided by the GRA, as the Information Commissioner, for fixed line and mobile subscribers who do not want to receive unsolicited direct marketing calls and/or faxes. This service is based on the provisions found in the Privacy Regs.

14. The ICO is a corporation sole appointed under the UK DPA to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

15. The ICO is empowered to take a range of regulatory action for breaches of, inter alia, the following legislation (as amended from time to time):

(a) UK DPA;

(b) UK GDPR;

(c) The Privacy and Electronic Communications (EC Directive) Regulations 2003 **(the "PECR")**;

(d) The Environmental Information Regulations 2004 **(the "UK EIR")**;

(e) Freedom of Information Act 2000 **(the "UK FOIA")**;

(f) Environmental Protection Public Sector Information Regulations 2009 **(the "UK EPPSIR")**;

(g) Investigatory Powers Act 2016;

(h) Re-use of Public Sector Information Regulations 2015;

(i) Enterprise Act 2002;

(j) Security of Network and Information Systems Directive **(the "NIS Directive")**;

(k) Electronic Identification, Authentication and Trust Services Regulation **(the "eIDAS")**.

16. Article 57 of the UK GDPR and Section 115 of the UK DPA place a broad range of statutory duties on the ICO, including monitoring and enforcement of the UK GDPR and UK DPA, promotion of good practice and adherence to the data protection obligations by those who process personal data in the UK. These duties sit alongside those relating to the other enforcement regimes outlined in paragraph 15 above.

17. The ICO's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the UK DPA, UK GDPR, PECR eIDAS, UK FOIA and UK EIR;

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

(c) 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;

(d) administering fines by way of penalty notices in the circumstances set out in section 155 of the UK DPA;

(e) administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the ICO);

(f) issuing decision notices detailing the outcome of an investigation under the UK FOIA and UK EIR;

(g) certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under the UK FOIA or UK EIR; and

(h) prosecuting criminal offences relating to certain information law matters before the Courts.

18. Regulation 31 of the PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the ICO with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach the PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of the PECR, including automated telephone calls made without consent, telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively.)

19. Further, Article 50 of the UK GDPR requires the ICO to, in relation to third countries and organisations, take appropriate steps to, inter alia:

(a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of legislation and practice for the protection of personal data, including legislation and practice relating to jurisdictional conflicts with third countries.

SHARING OF PERSONAL DATA

20. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the ICO or the GRA. The parties have determined that the personal data they exchange does not warrant entering into a separate data sharing agreement, but this will be kept under review.

21. If the Participants wish to share personal data, for example in relation to any cross border personal data incidents involving organisations in both jurisdictions, each Participant will consider compliance with its own applicable data protection laws, which may require the Participants to enter into a written agreement or further arrangements governing the sharing of such personal data.

Legal basis for sharing information

Information shared by the ICO with the GRA

22. The ICO, during the course of their activities, will receive information from a range of sources, including personal data. The ICO will process all personal data in accordance with the principles of the UK GDPR, the UK DPA and all other applicable legislation. The ICO may identify that information held, which may include personal data, ought to be shared with the GRA as it would assist in performing the functions and responsibilities of the GRA.

23. Section 132 of the UK DPA states that information obtained by the ICO in the course of, or for the purposes of, discharging their functions can only be shared with others if there is lawful authority to do so. Section 132 of the UK DPA sets out the circumstances in which the ICO will have the lawful authority to share that personal data with the GRA.

24. The ICO will be permitted to share information with the GRA in circumstances where they have determined that it is reasonably necessary to do so in furtherance of one of the grounds outlined at paragraph 23. In doing so, the UK will identify the function of the GRA with which that information may assist and assess whether that function could reasonably be achieved without access to the particular information in question. In

particular, where the information proposed for sharing with the GRA amounts to personal data, the ICO will consider whether it is necessary to provide it in an identifiable form in order for the GRA to perform their functions, or whether disclosing it in an anonymised form would suffice. The ICO will also be permitted to share information in matters where the ICO and GRA both have jurisdiction as a result of cross-border processing, where there has been a request for mutual assistance and where there is a joint investigation being conducted.

25. Where information is to be disclosed for law enforcement purposes[2] under section 35(4)(a) or (b) of the UK DPA, then the ICO will only disclose such information in accordance with an appropriate policy document as outlined by section 42 of the UK DPA.

26. Where a request for information is received by the ICO from a third-party under data protection laws, the ICO will seek the views of the GRA where the information being sought by the third-party includes information obtained from, or shared with the ICO by, the GRA. However, the decision to disclose or withhold information (and therefore any liability arising out of that decision) remains with the ICO as Data Controller in respect of that data.

Information shared by the GRA with the ICO

27. The GRA, during the course of their activities, will receive information from a range of sources, including personal data. The GRA will process all personal data in accordance with the principles of the Gibraltar GDPR, the Gibraltar DPA and all other applicable legislation. The GRA may identify that information held, which may include personal data, ought to be shared with the ICO as it would assist in performing the functions and responsibilities of the ICO.

28. Section 140 of the Gibraltar DPA states that information obtained by the GRA in the course of, or for the purposes of, discharging their functions can only be shared with others if there is lawful authority to do so. Section 140 of the Gibraltar DPA sets out the circumstances in which the GRA will have the lawful authority to share that personal data with the ICO.

29. The GRA will be permitted to share information with the ICO in circumstances where they have determined that it is reasonably necessary to do so in furtherance of one of the grounds outlined at paragraph 28. In doing so, the GRA will identify the function of the ICO with which that information may assist and assess whether that function could reasonably be achieved without access to the particular information in question. In particular, where the information proposed for sharing with the ICO amounts to

[2] As per section 31 of the UK DPA, the "law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguardng against and the prevention of threats to public security.

personal data, the GRA will consider whether it is necessary to provide it in an identifiable form in order for the ICO to perform its functions, or whether disclosing it in an anonymised form would suffice. The GRA will also be permitted to share information in matters where the GRA and ICO both have jurisdiction as a result of cross-border processing, where there has been a request for mutual assistance and where there is a joint investigation being conducted.

30. Where information is to be disclosed for law enforcement purposes[3] under section 44(3)(a) or (b) of the Gibraltar DPA, then the GRA will only disclose such information in accordance with an appropriate policy document as outlined by section 51 of the Gibraltar DPA.

31. Where a request for information is received by the GRA from a third-party under data protection laws, the GRA will seek the views of the ICO where the information being sought under the request includes information obtained from, or shared with the GRA by, the ICO. However, the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the GRA as Data Controller in respect of that data.

Scope of Co-operation

32. The Parties acknowledge that it is their common interest to collaborate in accordance with this MoU in order to:

(a) ensure the Parties are able to deliver the regulatory co-operation necessary to underpin their data-based economies and protect the fundamental rights of citizens of the United Kingdom and Gibraltar respectively, in accordance with applicable laws of the Parties' respective jurisdictions;

(b) co-operate with respect to the enforcement of their respective applicable data protection and privacy laws;

(c) keep each other informed of developments in their respective jurisdictions having a bearing on this MoU;

(d) recognise parallel or joint investigations or enforcement actions by the Parties as priority issues for co-operation.

33. The Parties may jointly identify one or more areas or initiatives for co-operation. Such co-operation may include:

[3] As per section 40 of the Gibraltar DPA the "law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguardng against and the prevention of threats to public security.

(a) sharing of experiences and exchange of best practices on data protection policies, education and training programmes;

(b) implementation of joint research projects;

(c) co-operation in relation to specific projects of interest, including regulation of children's privacy, regulatory sandboxes and artificial intelligence;

(d) exchange of information involving potential or on-going investigations of organisations in the respective jurisdictions in relation to a contravention of personal data protection legislation;

(e) joint investigations into cross-border personal data incidents involving organisations in both jurisdictions;

(f) convening bilateral meetings annually or as mutually decided by the Parties;

(g) any other areas of co-operation as mutually decided by the Parties;

34. This MoU does not impose on either the ICO or the GRA any obligation to co-operate with each other or to share any information. Where a Party chooses to exercise its discretion to co-operate or to share information, it may limit or impose conditions on that request. This includes where (i) it is outside the scope of the MoU, or (ii) compliance with the request would breach the Parties' legal responsibilities.

Method of exchange

35. Appropriate security measures shall be agreed to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

Confidentiality and data breach reporting

36. Where confidential material is shared between the Parties, it will be marked with the appropriate security classification.

37. Where one Party has received information from the other Party, they may use the information solely for the purposes set out in the relevant request for information or as otherwise agreed in writing between the Parties.

38. Where one Party has received information from the other Party, they will obtain the written permission of the other Party before passing the information on to a third party or using the information in an enforcement proceeding or court case.

39. Where confidential material obtained from, or shared by, the originating Party is wrongfully disclosed by the Party holding the information, that Party will bring this to the attention of the originating Party without delay.

40. In accordance with relevant legislation, the ICO and the GRA will protect the confidentiality and sensitivity of all unpublished regulatory and other confidential information received from the other Party, and maintain effective controls designed to minimise the risk of inappropriate disclosures.

41. The ICO and the GRA will liaise where relevant, to the extent permitted by law and having regard to their respective objectives, on responding to enquiries from the public, including Freedom of Information Act requests and will consult each other before releasing information originally belonging to the other.

Duration and review of the MoU

42. The Parties will monitor the operation of this MoU and will review it biennially. Should the Parties fail to review the same, subject to paragraph 45 below, the MoU shall nevertheless continue in force as if a review had been conducted and no changes made.

43. Any minor changes to this MoU identified between reviews may be agreed in writing between the Parties.

44. Any issues arising in relation to this MoU will be notified to the key contact for each Party.

45. Either Party may terminate this MoU by submitting prior notice to the other Party at any given time. Such termination shall become effective thirty calendar days from the date of submission of said notice.

Non-binding effect of this MoU and dispute settlement

46. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the ICO or the GRA.

47. The Parties will settle any disputes or disagreement relating to or arising from this MoU amicably through consultations and negotiations in good faith without reference to any international court or other forum.

Designated contact points

48. The following persons will be the designated contact points for the Participants for matters under this MoU:

GRA	ICO
Name: Designation: Information Rights Manager	Name: Designation: Head of International Regulatory Cooperation

(a) The above individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

(b) Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.

Entry into effect and termination

49. This MoU will come into effect upon its signature by the Participants and remain in effect unless terminated by either Participant upon three months' written notice to the other Participant.

Signatories

John Paul Rodriguez
Gibraltar Information Commissioner

John Edwards
Information Commissioner for the United Kingdom of Great Britain and Northern Ireland

Dated this 25th **Day of October 2022**