

## **MEMORANDUM OF UNDERSTANDING BETWEEN THE INFORMATION COMMISSIONER AND THE COMMISSIONER OF THE ROYAL GIBRALTAR POLICE**

- (A) This Memorandum of Understanding ("the MoU") between the Information Commissioner and the Commissioner of Police on behalf of the Royal Gibraltar Police establishes a framework for cooperation and information sharing between the Information Commissioner ("the IC") and the Commissioner of Police and Royal Gibraltar Police ("the CoP"), collectively referred to as "the parties" throughout this document. In particular, it sets out the broad principles of collaboration and the legal framework governing the sharing of relevant information and intelligence between the parties. The shared aims of this MoU are to enable closer working between the parties, including the exchange of appropriate information, so as to assist them in discharging their regulatory and statutory functions.
- (B) This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the IC or the CoP. The arrangements set out in this MoU are subject to what is permitted and required by law. The parties have determined that they do not exchange sufficient quantities of personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

### **The role and function of the Information Commissioner**

1. The IC is the Chief Executive Officer of the Gibraltar Regulatory Authority established by statute as Gibraltar's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.
2. The IC is empowered to take a range of regulatory action for breaches of, inter alia, the following legislation:
  - Data Protection Act 2004 ("the DPA");
  - General Data Protection Regulation ("the GDPR");
3. Article 57 of the GDPR and Section 124 of the DPA place a broad range of statutory duties on the IC, including monitoring and enforcement of the GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data.
4. The IC's regulatory and enforcement powers include:
  - conducting assessments of compliance with the DPA and GDPR;
  - issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;
  - 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;
- administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the IC);
- prosecuting criminal offences before the Courts.

#### **Functions and powers of the Commissioner of Police and the RGP**

5. The CoP is appointed under the Police Act 2006, subject to the provisions of that Act, to have command, superintendence, direction and control of the police force known as the Royal Gibraltar Police (the RGP), and shall be responsible for the efficient administration and government of the RGP and for the proper expenditure of all public moneys appropriated for the service thereof. The RGP are employed in and throughout Gibraltar for (a) the preservation of the peace; (b) the maintenance of law and order; (c) the prevention and detection of crime; (d) the apprehension and guarding of offenders; and (e) the protection of property.

#### **Purpose of information sharing**

6. The purpose of the MoU is to enable the parties to share relevant information which enhances their ability to exercise their respective functions.
7. This MoU should not be interpreted as imposing a requirement on either party to disclose information in circumstances where doing so would breach their statutory responsibilities. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with both the DPA and the GDPR. The MoU sets out the potential legal basis for information sharing, but it is for each party to determine for themselves that any proposed disclosure they make is compliant with the law.

#### **Principles of cooperation and sharing**

8. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the CoP agrees that he will alert the IC to any potential breaches of the legislation regulated by the IC, within the context of this relationship, discovered whilst undertaking statutory duties, and provide relevant and necessary supporting information.
9. Similarly, although again subject to any legal restrictions on the disclosure of information, the IC will, at his discretion, alert the CoP to any potential breaches of legislation which have criminal implications within the context of this relationship and provide relevant and necessary supporting information.
10. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the parties will:
  - Communicate as required to discuss matters of mutual interest; and
  - Consult one another on any issues which might have significant implications for the other organisation.

11. The parties will comply with the general laws they are subject to, including, but not limited to, local data protection laws; the maintenance of any prescribed documentation and policies; and comply with any governance requirements in particular relating to security and retention, and process personal data in accordance with the statutory rights of individuals.

#### **Legal basis for sharing information**

##### ***Information shared by the CoP with the IC***

12. The IC's statutory function relates to the legislation set out at paragraph 2, and this MoU governs information shared by the CoP to assist the IC to meet those responsibilities. To the extent that any such shared information is to comprise personal data, as defined under the DPA and GDPR, the RGP is a Data Controller so must ensure that it has legal basis to share it and that doing so would otherwise be compliant with the data protection principles.
13. Section 139 of the DPA may provide a legal basis for the RGP to share information with the IC. Under this particular provision, the CoP is not prohibited or restricted from disclosing information to the IC by any other enactment or rule of law provided it is "information necessary for the discharge of the IC's functions".

##### ***Information shared by the IC with the CoP***

14. The IC, during the course of his activities, will receive information from a range of sources, including personal data. He will process all personal data in accordance with the principles of the DPA, the GDPR and all other applicable legislation. The IC may identify that information he holds, which may include personal data, ought to be shared with the CoP as it would assist them in performing their functions and responsibilities.
15. Section 140 of the DPA states that the IC can only share confidential information with others if there is lawful authority to do so. In this context, the information will be considered confidential if has been obtained, or provided to, the IC in the course of, or the purposes of, discharging his functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources. This therefore includes, but is not limited to, personal data. Section 140 of the DPA sets out the circumstances in which the IC will have the lawful authority to share that confidential information with the CoP. In particular, it will be lawful in circumstances where:
  - The sharing was necessary for the purpose of the IC discharging his functions (section 140(2)(c));
  - The sharing was made for the purposes of criminal or civil proceedings, however arising (section 140(2)(e)); and
  - The sharing was necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 140(f)).
16. The IC will therefore be permitted to share information with the CoP in circumstances where it has determined that it is reasonably necessary to do so in furtherance of one of those grounds outlined at paragraph 15. In doing so, the IC will identify the function

of the CoP with which that information may assist, and assess whether that function could reasonably be achieved without access to the particular information in question.

17. In particular, where the information proposed for sharing with the CoP amounts to personal data the IC will consider whether it is necessary to provide it in an identifiable form in order for the CoP to perform its functions, or whether disclosing it in an anonymised form would suffice.
18. Where information is to be disclosed by either party for law enforcement purposes under section 44(3)(a) or (b) of the DPA then they will only do so in accordance with an appropriate policy document as outlined by section 51 of the DPA.
19. Where a request for information is received by either party under data protection laws the recipient of the request will seek the views of the other party where the information being sought under the request includes information obtained from, or shared by, the other party. However, the decision to disclose or withhold the information (and therefore any liability arising out of that decision) remains with the party in receipt of the request as Data Controller in respect of that data.

#### **Confidentiality and data breach reporting**

20. 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.
21. Where confidential material is shared between the parties it will be marked with the appropriate security classification.
22. Where one party has received information from the other, it will consult with the other party before passing the information to a third party or using the information in an enforcement proceeding or court case.
23. Where confidential material obtained from, or shared by, the originating party is wrongfully disclosed by the party holding the information, this party will bring this to the attention of the originating party without delay. This is in addition to obligations to report a personal data breach under the DPA and/or GDPR where personal data is contained in the information disclosed.

#### **Duration and review of the MoU**

25. The parties will monitor the operation of this MoU and will review it biennially.
26. Any minor changes to this memorandum identified between reviews may be agreed in writing between the parties.
27. Any issues arising in relation to this memorandum will be notified to the point of contact for each organisation.

#### **Key contacts**

33. The parties have both identified a key person who is responsible for managing this MoU. Those 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.

Signatories

Information Commissioner	Commissioner of Police

Dated this *7<sup>th</sup>* day of *September* 2019

