

Memorandum of Understanding between the Information Commissioner (IC) and the Scottish Biometrics Commissioner (SBC).

Introduction

1. This Memorandum of Understanding (MoU) establishes a framework for cooperation and information sharing between the Information Commissioner ("the IC") and the Scottish Biometrics Commissioner ("the SBC"), 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 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 functions. Any reference to the Information Commissioner shall include his statutory successors.
2. 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 SBC. The parties have determined that they do not anticipate exchanges of 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

3. The IC is a corporation sole appointed by His Majesty the King under the Data Protection Act 2018 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.
4. The IC is empowered to take a range of regulatory actions for breaches of a number of pieces of legislation and regulations. Further information on the IC's statutory responsibilities can be found on his website at: <https://ico.org.uk/about-the-ico/what-we-do>
5. In relation to this MOU the Commissioner's powers in relation to the following legislation are most relevant:
 - Data Protection Act 2018 (DPA);
 - General Data Protection Regulation (UK GDPR);
6. Article 57 of the UK GDPR and Section 115(2)(a) of the DPA 2018 place a broad range of statutory duties on the Commissioner, including monitoring and enforcement of the UK GDPR, promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes outlined in paragraph 4 above.
7. The Commissioner's regulatory and enforcement powers include:

- conducting assessments of compliance with the DPA 2018 and UK 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;

The role and function of the Scottish Biometrics Commissioner

8. The SBC is appointed by His Majesty the King on the nomination of the Scottish Parliament under the Scottish Biometrics Commissioner Act 2020. The general function of the SBC is to support and promote the adoption of lawful, effective and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes in Scotland.
9. The SBC is empowered to do anything which appears to the Commissioner to be necessary or expedient for the purposes of, or in connection with, the performance of the Commissioner's functions, or to be otherwise conducive to the performance of those functions. Further information on the SBC's statutory responsibilities can be found in the enabling legislation:
<https://www.legislation.gov.uk/asp/2020/8/contents>

Purpose of Information Sharing

10. The purpose of the MoU is to enable the parties to share relevant information and experience which enhances their ability to exercise their respective functions.
11. This MoU should not be interpreted as imposing any requirement on either party to disclose information. In particular, each party must ensure that any disclosure of personal data pursuant to these arrangements fully complies with both the UK GDPR and the DPA 2018. The MoU sets out the potential legal framework for information sharing, but it is for each party to determine for themselves that any proposed disclosure is compliant with the law.

Principles of cooperation and sharing

12. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, each Party will alert the other to any potential breaches of the legislation regulated by the respective organisation which is discovered whilst undertaking regulatory duties, and provide relevant and necessary supporting information.
13. Subject to any legal restrictions on the disclosure of information (whether imposed by statute or otherwise) and at their discretion, the Parties will:

- Maintain a working liaison through a nominated point of contact to regularly discuss matters of mutual interest (this may involve participating in multi-agency groups to address common issues and threats) - see Annex A for points of contact:
- Consult one another on any issues which might have significant implications for the other organisation, including sharing draft policy positions where appropriate; and
- Conduct joint audits where appropriate, providing expertise in relation to relevant areas of responsibility.

14. 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 as required by the relevant applicable law.

Lawful basis for joint working or sharing information

Information shared by the SBC with the IC

15. The IC's statutory function relates to the legislation set out at paragraph 5, and this MoU governs information shared by the SBC to assist the IC to meet those responsibilities. To the extent that any such shared information comprises personal data, as defined under the UK GDPR and DPA 2018, the SBC is a Data Controller in respect of such data and must ensure that it has legal basis to share it and that doing so would be compliant with the data protection principle.
16. Section 3 (h) of the Scottish Biometrics Commissioner Act 2020 provides that the SBC may, in the exercise of the Commissioner's functions, work jointly with, assist or consult the Information Commissioner. The SBC may share general information or findings from review activity with the IC. The SBC'S oversight functions extend to biometric data in a policing and criminal justice context in Scotland, but the SBC does not control or process personal biometric data.
17. Section 131 of the Data Protection Act 2018 may provide both the lawful basis, from a data protection perspective, and the legal power for the SBC to share information with the IC. Under this particular provision, the SBC 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 Commissioner's functions".

Information shared by the IC with the SBC

18. 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 UK GDPR, the DPA 2018 and all other applicable legislation. The IC may identify that information he holds ought to be shared with the SBC where it

would assist them in performing their functions and responsibilities. This may include personal data. If it is determined that it is necessary to share personal data

19. Section 132 (1) of the DPA 2018 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 it 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 132 (2) of the DPA 2018 sets out the circumstances in which the IC will have the lawful authority to share that information with the SBC. In particular, it will be lawful where:

- The sharing was necessary for the purposes of the IC discharging his functions (Section 132 [2] [c]);
- The sharing was made for the purposes of criminal or civil proceedings, however arising (Section 132 [2] [e]);
- The sharing was necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (Section 132 [2] [f]).

20. The IC will therefore be permitted to share information with the SBC 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 SBC with which that 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 SBC amounts to personal data the IC will consider whether it is necessary to provide it in an identifiable form in order for the SBC to perform its functions, or whether disclosing it in an anonymised form would suffice.

21. If information disclosed by the IC was received by him in the course of discharging his functions as a designated enforcer under the Enterprise Act 2002, any disclosure shall be made in accordance with the restrictions set out in Part 9 of the Act.

22. Where information is to be disclosed by either party for law enforcement purposes under section 35 (4) or (5) of the DPA 2018 then they will only do so in accordance with an appropriate policy document as outlined by section 42 of the DPA 2018.

23. The SBC is subject to the Freedom of Information (Scotland) Act 2002 and the provisions of public authorities legislation in Scotland extends to the SBC. Where a request for the disclosure of information is received by either Party under data protection laws or FOIA, 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 from that decision) remains with the party in receipt of the request as Data Controller in respect of that data.

Method of exchange

24. 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

25. Where confidential material is shared between the Parties it will be marked with the appropriate security classification and, where appropriate, handling conditions.
26. Unless it would be inconsistent with its legal obligations, where one Party has received information from the other, it shall consult with the other Party as far as possible and in accordance with its' own internal policies and procedures before passing the information to a third party or using the information in an enforcement proceeding or court case.
27. Where confidential material obtained from, or shared by, the originating Party is wrongfully disclosed by the receiving Party, 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 UK GDPR and/or DPA 2018 where personal data is contained in the information disclosed.

Duration and review of the MoU

28. The Parties will monitor the operation of this MoU and will review it biennially.
29. Any minor changes to this memorandum identified between reviews may be agreed in writing between the Parties.
30. Any issues arising in relation to this memorandum will be notified to the point of contact for each Party.

Annex A

Key Contacts

1. The Parties have identified a single point of contact for this MoU
2. The single points of contact are:

Information Commissioner's office	Scottish Biometrics Commissioner's office
Jenny Brotchie, Regional Manager Scotland	Diego Quiroz, SBC Operations Manager

3. The nominated points of contact for each party 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 ways to continuously strengthen the Parties' working relationship.

Signatories

Information Commissioner	Scottish Biometrics Commissioner
	

v1 11.12.2023



Note: This document has been signed and signatures redacted for publication.