# Personal Data Sharing Policy

**Version number:** 3.0

**Status:** Published

**Department/Team:** Data and Information Management

**Relevant policies:**

Data Protection Policy

Disclosure of information about ICO employees

**Distribution:** Internal and External

**Author/Owner:** Data and Information Management

**Application date:** 16/04/2024

**Review date:** 31/01/2027

**Security classification:** Official

## Key messages

The main objective of this policy is to provide:

- Outline how the ICO will ensure compliance with the UK GDPR and Data Protection Act 2018 (DPA 2018) when sharing personal data with other controllers.
- Explain the roles and responsibilities relevant to sharing personal data.

## Does this policy relate to me?

This policy applies to sharing personal data with other organisations or people and applies to all staff.

# Table of Contents



# 1.Introduction

1.1. This policy is based on the statutory data sharing code of practice (the Code), which applies to all organisations including the Information

Commissioner's Office (ICO). The policy is also informed by the government's data sharing governance framework.

1.2. The policy sets out ICO's data sharing rules and ensures we share personal data lawfully and fairly with other controllers.

Back to the top

# 2. Sharing personal information at the ICO

2.1. Data protection law facilitates data sharing when you approach it in a fair and proportionate way. The benefits of data sharing are mentioned in the Code. Some examples of benefits are: to help us to fulfil our public task efficiently and to produce official statistics.

2.2. We share personal data in a way that is fair, transparent, and proportionate.

2.3. We share personal data in different circumstances. For example:

- because we are required to do so by law eg employee tax information,
- via regular publishing, eg pay and pension data and register of interests for Management Board Members,
- in the course of our regulatory work, through a data sharing agreement,
- we also share personal data every day, as part of investigating complaints.

2.4. The personal data we share might be of our employees, contractors, complainants, people who are involved in our investigations and public and private stakeholders.

## Legal power to share

2.5. Article 5(1) of the UK GDPR requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals."

2.6. As a public sector body, we ensure we have a legal power to share personal data where necessary for our functions. This is generally conferred on the ICO by statute or other laws. Where it is not obvious that we have a legal power to share, we consult with relevant departments and seek advice from people managers as appropriate.

2.7. This usually covers us when we share personal data in a regulatory context. Compliance with data protection legislation when sharing personal information makes it likely that the sharing also complies with Article 8 of the Human Rights Act 1998.

## Lawful basis to share personal data

2.8. We identify a data protection lawful basis for sharing personal data from the UK GDPR before we start. The position is different for law enforcement processing by a competent authority under part 3 of the DPA 2018).

2.9. The ICO as a public authority will mostly share regulatory personal data under Article 6(1)(e) "Public Task" in the instances where sharing is necessary for the performance of a task carried out in the public interest, eg complaints and enquiries handling or in the exercise of official authority vested in the controller. More information is available on the ICO's guidance on Public Task

2.10. However, depending on the purpose of sharing, other lawful bases may be appropriate. Our departments document their lawful basis for sharing as part of updating our records of processing activities (ROPAs).

Back to the top

# 3. Sharing special category data

3.1. Where it is necessary to share special category data, we ensure we have a lawful basis for the processing and meet a condition from Article 9(2). Where required we refer to the ICO's policy on this: Safeguards policy- processing of special categories and criminal offence data.

Back to the top

# 4. Limitations on disclosures

## Section 132 of the DPA 2018 and the limits on disclosure of information

4.1 Section 132 prohibits any previous or current Commissioners, ICO staff or agents of the Commissioner from disclosing information without lawful authority and makes it a criminal offence to do so knowingly or recklessly. It is not limited to personal data, but covers all information which:

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

4.2. s132(2) lists five grounds where the disclosure may be made with lawful authority, for example with consent of the individual or the business to whom the information relate.

4.3. If in doubt about whether you can share personal data with another controller, please read our page guidance on Section 132. If you still have questions please contact the information access team.(*internal link*)

## Confidentiality

4.4 The ICO may also have received information (including personal data) that has been shared in confidence (for example HR data). Even where s132 DPA 2018 does not apply to the information, the common law duty of confidentiality (*internal link*) could apply and the ICO may still not be able to disclose it without some form of legal authority or justification such as consent. Please read our Section 132 (*internal link*) guidance. If you still have questions , please seek advice from the information access team.(*internal link*)

Back to the top

# 5. Transparency and accountability

5.1. We demonstrate we share personal data fairly and transparently. We make sure that the sharing is reasonable and proportionate and is not done in a way that people would find unexpected or objectionable.

5.2. The ICO's global privacy notice will be kept up to date to reflect new types of routine sharing.

5.3. We follow the memorandum of understanding (MOU) production procedure (*internal link*) when we sign an MOU.

5.4. However, for data sharing agreements which are legally binding documents, we need to involve our legal team.

5.5. We ensure that we share personal data securely in accordance with our Information Classification Guidance (*internal link*).

5.6. We may also receive requests to share relevant personal data with bodies in other countries, for example from other national data protection regulators where there are incidents affecting another country. We ensure that all transfers of personal data outside the UK are made in compliance with the relevant data protection legislation and we document those transfers where necessary in line with the latest ICO guidance: A guide to international transfers.

# 6. Assessing the risk of sharing personal data

## Data Protection Impact Assessment (DPIA) in routine sharing

6.1. When deciding to share personal data we consider the risk to people. Not all sharing of personal data requires a DPIA.

6.2. We assess the risk to new or changed sharing of personal data. The department owning the information should consider carrying out a DPIA.

6.3. We follow the ICO's internal DPIA process (*internal link*) to ensure we take a data protection by design and default approach and implement any additional safeguards.

6.4. If we want to share children's data, we must carry out a DPIA and clearly record the necessity of sharing.

# 7. Assessing necessity and proportionality

7.1. When we share personal data with other controllers, we document what we share, including a clear reason for why it is necessary.

7.2. We share only the minimum amount of data to satisfy our purpose for sharing the personal data / information.

7.3. We consider the categories of data, the objectives we want to achieve, the duration of sharing, and the way we share personal data.

7.4. We make sure all the personal data shared is necessary and proportionate for the purpose of the processing and we assess this on case-by-case basis.

# 8. What else we consider when sharing personal data

8.1. A signed data sharing agreements is an information asset owned by the relevant Information Asset Owner, who is responsible for ensuring that the agreement has the right legal input and is reviewed periodically.

8.2. Where we share personal data relying on the lawful basis of consent, we keep, and review consent records of any consent given.

8.3. Where an instant decision is needed to share personal data (eg in a health and safety emergency) we only share necessary data, as is fair and proportionate. We make a record, at the time of sharing or as soon as possible afterwards of what was shared and why.

8.4. The ICO may share personal data with other regulators and request the sharing of information by those authorities, to aid cooperation and mutual assistance. This might be, for instance, where overlapping regulatory and/or enforcement responsibilities are identified. Some teams' core work involves this type of sharing e.g. DRCF, Intel team; and those teams do so in line with their local processes which follow this policy on sharing personal data.

# 9. Sharing personal data for Law enforcement processing

9.1. We process most personal data under the UK GDPR (including for civil investigations; for example, civil monetary penalties are covered by the general processing provisions under the UK GDPR and Part 2 of the DPA 2018). However, as part of the Commissioner's statutory functions, we also investigate and prosecute individuals for criminal offences under the legislation we regulate, for example, under s77 of the Freedom of Information Act 2000 or s170 of the DPA18.

9.2. Part 3 of the DPA 18 applies to the processing of personal data by relevant authorities for law enforcement purposes ie for criminal investigations and potential prosecutions. The Information Commissioner is named as a 'competent authority' for the purposes of Part 3 DPA 18 at paragraph 52 of Schedule 7 of the DPA 2018.

9.3. Where we are considering disclosing personal data from a criminal investigation, it must be necessary for our purposes or for the purposes of another competent authority, eg a police force. Requests for personal data made by competent authorities should be handled by our Information Access team so that we can ensure the necessity of sharing and keep a record of what we shared.

9.4. We may carry out 'sensitive processing' on personal data when handling a criminal investigation. Sensitive data as defined in Part 3 section 35(8) is equivalent to UK GDPR special category data. We may need to share such 'sensitive' personal data and have published Sensitive processing for law enforcement purpose in line with the requirements of s42 of the DPA 2018. This policy explains that we may share personal data for law enforcement purposes if we have that person's consent or it is strictly necessary and the processing meets at least one of the conditions in Schedule 8. We are also obliged to comply with other safeguards, for example, keeping a record of processing activities and, where necessary, a log of certain automated processing actions including disclosure of personal data.

## Data sharing and reuse of data by competent authorities for non-law enforcement purposes

9.5. Data we have collated as a competent authority under Part 3 for law enforcement purposes may be shared for non-law enforcement purposes under the UK GDPR and Part 2 of the DPA 2018. Before sharing criminal offence data for a non-law enforcement purpose, as a competent authority we need to determine the purpose for the proposed sharing and whether this is 'authorised by law'. This might be provided, for example, by statute, common law, royal

prerogative or statutory codes. As the sharing is no longer for law enforcement purposes, we will need to have a lawful basis under Article 6 of the UK GDPR.

9.6. As the personal data is likely to include criminal offence data, we will also need to check we have met the requirements of Article 10 of the UK GDPR.

9.7. This means we either identify our official authority for the processing or identify a relevant condition in Schedule 1 of the DPA 2018.

9.8. If the data to be shared includes special category data, we will need to identify a condition for processing under Article 9 as well as a lawful basis under Article 6. For further information, please see the ICO 'Data sharing and reuse of data by competent authorities for non-law enforcement purposes.

# 10. Risk appetite

10.1. Our risk policy and appetite statement (*internal link*) clarifies that we are heavily reliant upon information and data including personal data in order to be able to operate as an effective risk-based regulator. The accidental or deliberate wrongful disclosure of personal data has the potential to erode trust, damage our reputation and ultimately prevent us from being able to function. As such we have minimal appetite for such risks.

10.2. Conversely, we are 'open' to taking some risks as we look to be transparent wherever possible. We also have a duty to comply with the re-use of public sector information regulations and the proactive disclosure of datasets. In doing so, we need to balance our risks by thinking about our risk appetites while encouraging responsible and compliant sharing of non-personal data.

# 11. Roles and responsibilities

11.1. The ICO Data Protection Officer is responsible for offering advice on data sharing, including whether it is necessary or appropriate to undertake a DPIA.

11.2. Information Asset Owners (Directors) are responsible for authorising any data sharing where we agree to systematic, routine or large-scale data sharing with a third-party controller organisation. They are also responsible for ensuring that those arrangements are reviewed on a regular basis.

11.3. The information access team is generally responsible for responding to ad hoc requests to share personal data made by third parties including regulators.

11.4. Senior staff at Director level may make exceptional, one-off decisions to share personal data internally or with a third-party organisation in accordance with this policy.

11.5. All staff are responsible for familiarising themselves with this policy and any associated policies or guidance.

# 12.Compliance

12.1. All staff (current and former) must comply with the duty not to disclose information without lawful authority under s132 DPA 2018 (see above) as well as any other restrictions on sharing information (including personal data) such as the common law duty of confidentiality and the Official Secrets Act 1989. Any non-compliance may result in sanctions up to and including suspension and dismissal. In addition, improper use of personal data may expose the member of staff to civil and criminal liability.

# Version history

| Version | Changes Made | Date | Made by |
|---|---|---|---|
| 1.0 | Document created and published | 16/04/2024 | Iman El Mehdawy |
| 1.1 | Title changed from 'Policy on sharing personal data' to 'Personal Data Sharing Policy' | 20/06/2024 | Simon Lochery |
| 2.0 | Links updated, minor addition to 11.4 | 16/01/2025 | Iman El Mehdawy |
| 3.0 | Content moved to new template, minor formatting changes | 01/04/2026 | Iman El Mehdawy |