Information sharing

This page is from APP, the official source of professional practice for policing.

First published 3 August 2016 Updated 5 February 2020
Written by College of Policing
15 mins read

The General Data Protection Regulation (GDPR) entered into force on the 24 May 2016 and took effect on the 25 May 2018. Processing of personal data for 'law enforcement purposes' is not covered by the GDPR but by the Law Enforcement Directive, which replaced the European Council Framework Decision 2008/977/JHA. The directive entered into force on 5 May 2016 and European Union (EU) countries had to transpose it into their national law by 6 May 2018.

Some links on this page are only available to authorised users who are logged on to College Learn.

Authorised professional practice (APP) on information sharing has been produced to assist forces with the statutory duty to comply with the **GDPR 2016/679**, **Data Protection Act 2018** (DPA) and the **Human Rights Act 1998** (HRA) when sharing personal information. This APP:

- relates to sharing **personal data**, which is defined by the DPA as data relating to a living individual who can be identified from that data – consequently, throughout this APP the terms ‘data’ and ‘information’ are interchangeable
- only applies to sharing personal information – sharing non-personal information will be governed by national and local force policy
- aims to achieve a consistent approach across the police service to sharing personal information with external partners or agencies and provides professional guidance

Information sharing includes **personal data** and **special categories of personal data**.

Information sharing enables early intervention and preventative work to safeguard and promote welfare, as well as for wider public protection. The public needs to be confident that their personal information is kept safe and secure. All members of the police service are responsible for ensuring that we share information appropriately as part of our day-to-day practice and do so confidently, proportionately and lawfully.

For Welsh forces: Where reference is made to national templates in this APP, Welsh forces should adhere to the **Wales Accord on the Sharing of Personal Information (WASPI)**, which provides a framework for service-providing organisations directly concerned with the health, education, safety, and social wellbeing of the people in Wales.

Information sharing

Information sharing can mean disclosing information from one or more organisations to a third-party organisation(s) or sharing information between different parts of an organisation. It may include processing information either on a one-off or an ongoing basis between partners for the purpose of achieving a common aim.

Data sharing can take the form of:

- a mutual exchange of data
- one or more organisations providing data to a third party or parties
- several organisations making information available to each other on a shared platform
- several organisations combining information and making it available to a third party or parties

Sharing police information must be linked to a policing purpose. APP on information management – **management of police information** – defines such purposes as:

- protecting life and property
- preserving order
- preventing and detecting offences
- bringing offenders to justice
- any duty or responsibility arising from common or statute law

Some data sharing does not involve personal data, eg, sharing statistical data that does not identify a person. When this occurs, neither the DPA nor this APP applies.

Shared situational awareness and sharing of information is one of the key joint emergency service interoperability principles – more information can be found at **Joint Emergency Services Interoperability Principles (JESIP)**.

Sharing agreements

Organisations exchange information in different ways. The following are definitions of the differing types of agreement that enable effective information exchange.

Data processing contract

Whenever a controller uses a processor, there must be a legally-binding written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the **contract**. If a processor uses another organisation (namely, a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

Memorandum of understanding

A memorandum of understanding (MoU) describes a bilateral or multilateral agreement between two or more parties. An MoU expresses the parties' common objectives, indicating an intended common line of action leading to establishing a working relationship. It is a formal record of high-level commitment and agreement between organisations.

An MoU:

- describes the general principles of the agreements and the working relationships
- does not amount to a substantive contract
- is often used in cases where parties do not, for whatever reason, wish to create a legally binding commitment

Where there is a requirement to share personal information as a result of an MoU, there should be a separate information sharing agreement (ISA) which supports that MoU.

Service level agreement

A service level agreement (SLA) is an agreement between a service provider and its internal/external customers. It records the level to which the provider will perform the services. An SLA should be distinguished from (and should form a part of) the contract for the performance of the services themselves (services contract). The services contract will set out a full description of the services and include a number of terms and conditions such as price, payment, warranties and termination provisions.

SLAs measure the service provider's performance and quality. They can be structured in a number of ways, namely, with or without key performance indicators and/or service credits. The simpler they are (focusing on key issues only), the easier they will be to manage and are thus more likely to be effective.

For any SLA to be effective (particularly if it is to be used with a third-party provider) it should:

- form part of a services contract
- be periodically reported against by the service provider
- be actively managed (along with the contract itself)
- be periodically reviewed and updated to reflect relevant changes

This type of agreement is often used, especially in policing, to document how one unit/department provides a support service for a basic command unit/force.

Information sharing agreement

An ISA, also known as a data sharing agreement/information sharing protocol, identifies the statutory or basis for sharing personal information, and the extent and nature of the personal information to be shared. An ISA identifies:

- common standards for processing and handling information, including quality, retention and security considerations
- the lawful basis for using personal data, to achieve more effective policies and deliver better services while ensuring privacy and confidentiality of personal information
- the lawful transition of data from and to the law enforcement purpose

This type of agreement is appropriate whenever the police either request or are requested to share information on a regular basis with others, whether for a statutory or policing purpose.

For further information, see **ISA template** – this link is available to authorised users who are logged on to College Learn.

Common law

Common law does not provide the police with an unconditional power to engage in any activity that is not otherwise provided for by statute. It cannot be used in a way that contravenes or conflicts

with any legislation. In other ways, parliament is the supreme legal authority in the UK, and thus the court cannot overrule its legislation. Any use of common law powers to share information must be compliant with, in particular, the **HRA**, the **GDPR** and the **DPA**.

Pressing social need

There must also be a pressing social need to share information. The justification for disclosing personal information to a third party under common law is considered to be equivalent to that required for disclosing non-conviction information in accordance with the provisions of Part V of the Police Act 1997. See **R (on application of L) (FC) (Appellant) v Commissioner of Police for the Metropolis (2009) UKSC 3**.

Common law police disclosures

The common law police disclosure (CLPD) provisions allow forces to proactively provide personal data or sensitive personal data to a third party using common law powers. Chief officers should locally determine the implementation of CLPD provisions.

For further information see **National Police Chiefs' Council (NPCC) (2017) Common Law Police Disclosures (CLPD) – Provisions to supersede the Notifiable Occupations Scheme (NOS)**.

Statutory obligation

Subject to certain exemptions, statutory obligation means forces must share information. This is where there is a specific legal obligation to disclose police information to another party. Examples of where the police service is obliged to disclose information include:

- disclosure under **the Police Act 1997 Part V**
- disclosure under the **Freedom of Information Act 2000**
- disclosure under the **Safeguarding Vulnerable Groups Act 2006**
- disclosure under the **Data Protection Act 2018**
- responding to court orders (**APP on information management – data protection**)

Sharing information under statutory obligation does not require an ISA. Where in doubt, refer to the force point of contact for information sharing.

Statutory power

Subject to certain exemptions, statutory power means forces may share information. Under statutory power there is a specific legal power, but not an obligation, to share police information with another party. When sharing information under a statutory power:

- forces may do so without using an ISA, MoU or SLA
- forces must maintain an audit trail of the information shared

Legislative powers – GDPR and the Data Protection Act 2018

Police officers and police staff are sometimes required to make decisions in circumstances where those involved deliberately mislead or try to mislead them. The **national decision model (NDM)** helps police officers and staff make, examine and challenge decisions (both at the time and afterwards). The NDM can be used as a basis for assessing the need to share information. It should also be used to assess the limited sharing opportunities identified in the **Crime and Disorder Act 1998**. The Crime and Disorder Act 1998 imposes a duty on chief officers to share information with Crime and Disorder Reduction Partnerships (CDRPs) where appropriate.

Sharing police information can take place in a pre-planned and routine way as part of business as usual. This is governed by established rules and procedures. Forces may decide, or be asked, to share information in situations which are not covered by a formal agreement. This may result in sharing decisions being made under urgent conditions. Disclosing information in situations not covered by a formal agreement is still subject to the relevant sections of the DPA. In specific cases under general processing, an exemption in DPA may allow sharing for an incompatible but lawful purpose. For example:

- **Schedule 2 Part 1 Paragraph 2** – Personal data is exempt from principles 1 and 2 (Article 5(1)(a-b)) to the extent that they would otherwise prevent disclosure necessary to prevent prejudice to the following purposes:
  - preventing or detecting crime
  - apprehending or prosecuting offenders
  - assessing or collecting any tax or duty or an imposition of a similar nature

- **Schedule 2 Part 1 Paragraph 5** – Personal data is exempt from principles 1 and 2 (Article 5(1)(a-b)) to the extent that they would otherwise prevent disclosure when necessary for the following purposes:
  - required by enactment, rule of law or an order of a court or tribunal
  - required for, or in connection with, legal proceedings (including prospective legal proceedings)
  - required for obtaining legal advice
  - required for establishing, exercising or defending legal rights

Where an agreement does not exist, or the decision to share is a one-off, there are important questions that can help ensure that any information sharing is lawful:

- Who is asking for the information?
- Has the name, position, organisation and contact details of the person asking for the information been recorded?
- Has the identity of the person requesting the information been verified?
- What information is being requested?
- For what purpose will it be used?
- Is personal information being requested?
- Does a statutory or common law provision exist, and has a policing purpose to share information been established?
- If yes, in what format does the requester want the information?
- When does the requester want the information?

The information has been shared, the decision to share, why it was made and what information was shared should be recorded.

Requirement for an information sharing agreement

Factors to consider

- What is the purpose of sharing the data? When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both), set and document a clear purpose. This will help ensure that sharing is proportionate and relevant.

- What are the benefits and risks? Identify the potential benefits and risks (either to individuals or society) of sharing the data and assess the likely risks of not sharing.
- What information needs to be shared? Do not share all personal data held about someone if only certain data items are needed to achieve objectives (eg, there may be a need to share a person's current name and address but no other information held about them).
- Who requires access to the shared personal data? Apply the 'need to know' principles. Organisations and relevant staff should only have access to data if needed. This addresses necessary restrictions on onward sharing of data with third parties.
- When should it be shared? Document whether sharing is an ongoing, routine process or whether it should take place only in response to particular events.
- How should it be shared? Address security for accessing transmission/data and establish common rules for security.
- How can we check the sharing is achieving its objectives? Assess whether it is still appropriate to share and confirm that the safeguards still match the risks.
- What risk does the data sharing pose? Is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
- Could the objective be achieved without sharing the data or by anonymising it? Do not use personal data to plan service provision, eg, where this could be done with information that does not amount to personal data.
- What type of agreement is required? Is the requirement for an ISA only relevant to the local force or is there a need for a national agreement?

In addition to the above considerations, officers and staff should seek advice from the force lead for information sharing before creating an ISA. Forces should consider the requirements for a **data protection impact assessment**.

National information sharing agreements

National ISAs enable information to be shared from a national police system (for example, PNC) to an external organisation. For example, forces are under obligation to share information from PNC to the Gangmasters Licensing Authority (GLA).

National ISAs are commissioned by an NPCC lead and the agreements relate to their national policing coordination committee or portfolio area.

Local information sharing agreements

Local ISAs are those that are commissioned by a force lead or force information asset owner and relate to local policing, including safeguarding and public protection.

There is no requirement for the police service to have local ISAs in place between forces. Chief officers may arrange information sharing with other forces either by a formal request process or by providing direct access to force systems.

Consent

Consent is one of the conditions the DPA provides to legitimise processing. A data subject's consent is obtained through a freely given, informed, affirmative statement that the subject agrees to the processing. This means that the data subject understands the scope and nature of processing and has confirmed they agree to it. 'Freely given' means that the data subject is in control of processing and under no actual or perceived pressure to agree. It is a requirement of consent that it can be withdrawn as easily as it is given. When relying on consent, the data subject has control over the sharing.

For these reasons, the police service must seek consent only where strictly necessary and only where it cannot establish a policing purpose for processing. If the intent is to ask a data subject to volunteer data into an existing lawful purpose, or share regardless of the data subject's wishes, do not use consent.

If in doubt, refer to the force point of contact for information sharing.

Data sharing code of practice

The Information Commissioner has published the **Information Commissioner's Office (ICO) (2011) Data sharing code of practice under the DPA 1998 s 52**. The Commissioner will be publishing a revised code (under consultation at the time of updating this APP) **under section 121 of the DPA 2018**. The current code is statutory.

The published code covers the two main types of data sharing (under routine data sharing) where the same information is shared regularly between organisations for an established purpose.

- Example 1: Sharing personal information with the Security Industry Authority.
- Example 2: Sharing personal information with the General Medical Council.
    - Exceptional, one-off decisions to share data for any range of purposes.
- Example 3: Child Sex Offender Police Disclosure Scheme (Sarah's Law).
- Example 4: The Domestic Abuse Disclosure Scheme (Claire's Law).

Where in doubt, refer to the force point of contact for information sharing.

Drafting an information sharing agreement

Drafting

Forces should draft an ISA using the relevant **ISA template**. For a local agreement, local force processes apply.

The national **ISA template** has been produced by the national information sharing portfolio to encourage consistency and make the process of producing or updating a national ISA informal and flexible.

The template discusses both general processing and law enforcement processing and will guide the author through these parallel rules and assist in the tests for lawful transfer of information between them.

Review and feedback

During the review and feedback stage, a force submits the ISA for local and national consultation.

Publication

Once the ISA has been approved, the forces should publish it as required. For national agreements, this includes adding it to the national register and publishing it on the **NPCC Data Protection Group on the Knowledge Hub**. (Note: to access this link you must be a member of the group and logged into the Knowledge Hub).

Review

Reviews are an essential part of any ISA. The aim is to ensure that the agreement is achieving its purpose and that the actual sharing process is operating smoothly. The force point of contact for information sharing should carry out reviews annually in conjunction with partner agencies.

A review should include the following questions:

- Does the agreement still have the correct contact list?
- Is the agreement still useful and fit for purpose?
- Has the review identified any emerging issues?
- Should the ISA be extended or terminated?

For further information, see **ISA template** on College Learn (you will need to log in).

Governance process for national agreements

National information sharing portfolio

The national policing lead for information sharing chairs the national information sharing portfolio and reports directly to the Information Management Operational Requirements Coordination Committee (IMORCC).

The national information sharing portfolio aims to promote, support and enable lawful information sharing in support of a policing purpose. It reports directly to the IMORCC.

The national information sharing portfolio:

- facilitates and promotes best practice on information sharing
- influences policy and legislative developments regarding sharing police information
- oversees the governance framework for managing national ISAs
- supports national policing leads in developing ISAs
- provides guidance relating to the content and format of the standard national policing **ISA template**
- builds and maintains internal and external stakeholder relationships
- maintains the national policing ISA register
- facilitates the communications network

Governance process

Step one

National policing lead (NPL) commissions ISA and enlists services of local subject matter expert (SME).

Step two

SME checks national ISA register:

- If an an ISA already exists with the proposed partner agency and doesn't need updating then the process ends.
- If an ISA doesn't not exist or exists but needs to be updated then go to step three.

Step three

SME draft ISA/agreed by NPL.

Step four

ISA sent to regional coordinator.

Step five

Regional coordinator circulates to all regional coordinators and others in the ISA governance structure for review:

Step six

Feedback provided to initiating regional coordinator who provides a summary to the NPL (information sharing):

- If the ISA is complex or contentious then go to step seven.
- If the ISA is not complex or contentious then go to step nine.

Step seven

NPL (information sharing) liaises with NPL (ISA owner):

- If both NPL reconciled then go to step nine.
- If both NPL not reconciled then go to step eight.

Step eight

Refer to Chief Constable's Council via the NPCC lead:

- If the ISA is approved then go to step ten.
- If the ISA is not approved then the process ends.

Step nine

NPL (information sharing) advises NPL (ISA owner) has been approved.

Step ten

NPL (owner) and other party sign.

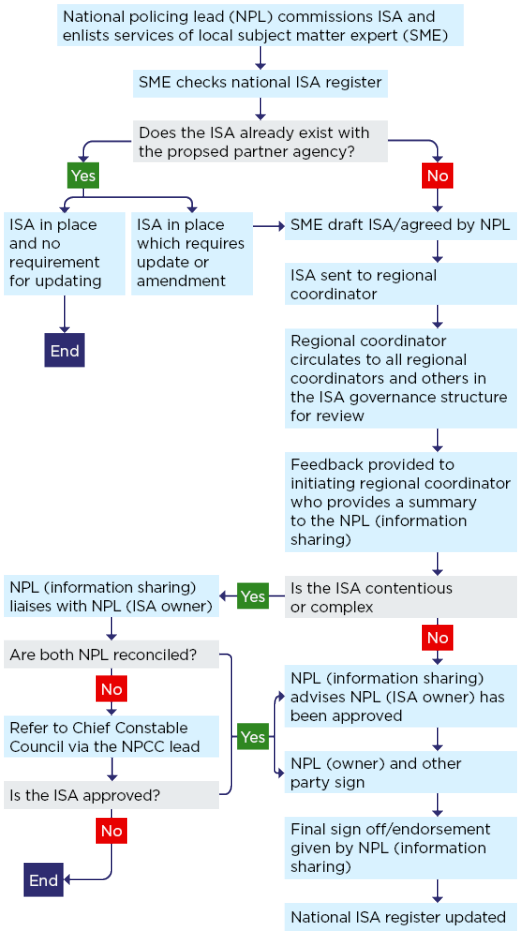
Step eleven

Final sign off/endorsement given by NPL (information sharing).

Step twelve

National ISA register updated.

Governance process diagram



Tags

Information management