Ending domestic abuse

Information Sharing
GDPR & Data Protection Act 2018

Since 25th May 2018 all agencies must be able to demonstrate that they are compliant with the General Data Protection Regulations (GDPR) and accompanying Data Protection Act 2018 (DPA). You must have appropriate policies in place. It is solely the responsibility of each agency to ensure compliance in terms of what and how information is shared and stored. SafeLives cannot provide legal advice on this subject but we can provide guidance. In this briefing we have aimed to offer guidance around the safe sharing of information. We have included links to relevant areas of the ICO Website which we hope will ease navigation around their comprehensive guidance online.

We recommend that all practitioners have a good working knowledge of Data Protection and that management facilitate the development of this knowledge amongst their staff. We also recommend a thorough understanding of the provisions of the Care Act 2014 as amended in 2016; The Statutory Guidance to the Care Act emphasises the need to share information about safeguarding concerns at an early stage; information-sharing agreements or protocols should be in place. Also the The Mental Capacity Act 2005 and Working Together to Safeguarding Children 2015.

We advise that decision-making should be done in consultation with others within your organisation or with the Information Commissioner's Office helpline: 08456 30 60 60. Alternatively, legal advice should be sought where appropriate. You need to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular sharing purpose.

This briefing can be used as a guide in situations where it may be necessary or desirable to share information with other agencies. Information about adults, children and young people at risk should only be shared between agencies:

- where relevant (has a rational link to the purpose) and limited to what is necessary, not simply all the information held;
- is adequate and sufficient to properly fulfil your stated purpose for sharing
- with the relevant people who need all or some of the information; and
- when there is a specific need for the information to be shared at that time.

Seven Principles of Data Protection

Article 5 of the GDPR sets out seven key principles which lie at the heart of general data protection. Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

The principles lie at the heart of the GDPR. Compliance with the spirit of these key principles is a fundamental building block for good data protection & information sharing practice. It is also key to your compliance with the detailed provisions of the GPDR.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines.

Lawful Basis

The first principle requires that you process all information lawfully, fairly and in a transparent manner. Sharing information is only lawful if you have a **lawful basis** under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.

The individual's right to be informed under Article 13 and 14 requires you to provide victims of abuse with information about your lawful basis for sharing. This means you need to include these details in your **privacy notice.**

You must use personal information in a way that is fair. This means you must not share information in a way that is "unduly detrimental, unexpected or misleading to the individuals concerned".

There are six options for lawful basis (see below) and which one is relevant will depend on the purpose for which you are sharing. There are also specific additional conditions for processing some especially sensitive types ("special category") of information. For more information, see the ICO website. You must be clear, open and honest with people from the start about how you will use and share their personal information. No single basis is 'better' or more important than the others.

You must determine your lawful basis before you begin sharing and processing information, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. You should have sight of your Local Information Sharing Policy and Marac Operating Policy which will detail the purpose for sharing information and the lawful basis. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

Consent

The GDPR sets a high standard for consent. But you often won't need consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your professional relationship. If you have assessed a victim of abuse to be at high risk of serious harm or homicide (i.e meeting the Marac threshold) then you will have grounds for sharing information in law. This therefore means that that individual does not have choice and is not in control of information sharing. **If you would still process the personal information without consent, asking for consent is misleading and inherently unfair.** Consent is one lawful basis for sharing information, and explicit consent can also legitimise use of special category data. Moreover, consent is important when sharing information where the risk to the victim of abuse has NOT been assessed to be high (so grounds in law do not exist). See the ICO's full guidance on Consent. For transparency we suggest you record your decision making process using this form

When is information sharing necessary?

Many of the lawful bases for sharing information depend on the processing being "necessary". This does not mean that sharing information always has to be essential. However, it must be a **targeted and proportionate** way of achieving the **purpose**. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

Purpose

At the heart of a Marac is the working assumption that no single agency or individual can see the complete picture of the life of a victim, but all may have insights that are crucial to their safety. A victim of abuse identified to be at high risk of serious harm or homicide needs a coordinated, multi-agency response with all agencies sharing relevant information to develop an action plan that is comprehensive, robust and addresses the risk
to all parties. The purpose of sharing information in the Marac process is to safeguard victims and any children that are affected by the domestic abuse.

To safeguard these victims of domestic abuse the Marac process must:

- Address the behaviour of the perpetrator
- Make links with other public protection arrangements in relation to children, perpetrators and vulnerable adults; and
- Safeguard agency staff

Special Category and criminal conviction information

If you are sharing special category data you need to identify both a lawful basis for general processing under Article 6 and an additional condition for sharing this type of information under Article 9. These do not have to be linked. There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards. The conditions are listed in Article 9(2) of the GDPR and you can find these listed on the ICO Website

If you are processing criminal conviction information or information about offences you need to identify both a lawful basis for general processing under Article 6 and an additional condition for processing this type of data under Article 10.

Children

The GDPR explicitly states that children's personal information merits specific protection. The GDPR contains provisions intended to enhance the protection of children's personal information and to ensure that children are addressed in plain clear language that they can understand. Transparency and accountability are important where children's information is concerned. In all circumstances you need to carefully consider the level of protection you are giving that information.

As with adults, you need to have a lawful basis for sharing a child's personal information and you need to decide what that basis is before you start sharing. You can use any of the lawful bases for processing set out in the GDPR when sharing children's information. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in sharing information against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks. For more detailed Guidance see the ICO Website

Accuracy

You should take all reasonable steps to ensure the information you share and hold is not incorrect or misleading as to any matter of fact.
A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

Caldicott Guardian Principles

A guidance has been published jointly by the Department and the UK Council of Caldicott Guardians to assist those who need to share information about individuals involved in domestic abuse. Specifically, designed for Marac but equally applies to other multi agency meetings. It sets out the underlying ethical considerations between confidentiality and information sharing and identifies the role of the Caldicott Guardian to 'strike the balance' between maintaining the individuals' confidentiality and privacy and wider considerations such as protection from harm.

We recommend that you read the fill report: 'Striking the Balance': Practical Guidance on the application of Caldicott Guardian Principles to Domestic Violence and MARACs (Multi Agency Risk Assessment Conferences)

Subject Access Requests

Individuals have the right to access their personal data that you hold. A subject access request verbally or in writing. You have one month to respond to a request. The right of access, referred to as subject access SAR), gives individuals the right to obtain a copy of their personal information as well as other supplementary information. It helps individuals to understand how and why you are using their information, and check you are doing it lawfully.

An individual is only entitled to *their own* personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see the ICO guidance on what is personal data.

The GDPR does not prevent an individual making a subject access request via a third party such as a solicitor. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

A child can also request access to information held and shared. Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual (perhaps the perpetrator). The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must consider all the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

This means that although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

For more information about Subject Access Requests please see the **ICO website**

Lawful basis & legal grounds for sharing information

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you share information (see also special category data above):

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, read the relevant page of the ICO guide

Main grounds in UK legislation which require the sharing of information

Requirement	Legal authority
Prevention and detection of crime	s.115 Crime and Disorder Act 1998
To protect vital interests of the data subject; serious harm or matter of life or death	Schedule 8, DPA 2018
For the administration of justice (usually bringing perpetrators to justice)	Part 3 & Schedule 8 DPA 2018
For the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	Part 3 s.31 & 35 DPA 2018
Child protection. Disclosure to Children's Social Care or the Police for the exercise of functions under:	Children Act 1989 & 2004
In accordance with a court order	(so requests to share information must show why it is relevant for the purpose for which they are requested, including a Court Order)
Overriding public interest	Common law
Right to life Right to be free from torture or inhuman or degrading treatment	Human Rights Act, Articles 2 & 3
Prevention of Abuse and Neglect	The Care Act 2014
Person lacks the mental capacity to make the decision regarding consent	Mental Capacity Act 2005

Balancing principles: Rights of the individual

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

See the ICO Guide for more information

Record all decisions & reasoning for decision making whether that decision is to share information or not to share information.

Balancing considerations:

Proportionate response • Respective risks to and safety of those affected • Relevancy & proportionality • Pressing need • Need to know of other agencies • Sharing is necessary for the purpose • Sharing information is justifiable • The rights of the individual	Article 5(1)(c) says: 1. Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"

Sharing information – a checklist

Decisions on sharing information must be justifiable and proportionate, based on the potential or actual harm to adults or children at risk and the rationale for decision-making should always be recorded. To assist with your decisions use the Information Commissioner's Office data sharing checklist.

Decisions should be **defensible** and not **defensive** decisions; confidentiality must not be confused with secrecy.

- ✓ Record that a decision has been made to share/disclose information
- ✓ What are the protocols/guidance referred to and which agencies or colleagues have been consulted about this decision? Set these out clearly in recording – for example, Home Office guidance, the Information Commissioner's Office helpline, own protocols?
- ✓ What is the lawful basis for sharing? Record it clearly.
- ✓ Be clear exactly what details of the information is to be shared and with whom. Set this out in your records.
- ✓ Think through the balancing exercise undertaken; that consideration of the interest of the other agency/person in receiving the information has been given and the degree of risk posed to any person by disclosure/nondisclosure. Consider the duty of confidentiality, human rights and the public interest. Record this. Record whether the sharing is proportionate, that there is a pressing need and summarise why.
- ✓ What is the amount of information to be disclosed and the number of people/agencies disclosed to? Is this no more than strictly necessary to meet the need for disclosure? Record why this is the case.
- ✓ Set out whether and when the survivor/person affected has been informed that the information will be disclosed and to whom, whether reasons have been given and whether details of next steps explained. Has this been done in advance of the information been disclosed? If the survivor/person affected has not been informed set out reasons why.
- ✓ The Care Act 2014 puts a legal responsibility on Local authorities to make enquiries, or ensure others do so, if it reasonably suspects an adult who has care and support needs and is, or is at risk of, being abused or neglected and unable to protect themselves against the abuse or neglect or risk of it because of those needs. An enquiry is the action taken or instigated by the local authority in response to a concern that abuse or neglect may be taking place.
- ✓ If in doubt, **always** seek specialist advice and **always** consult with your supervisor or line manager.

Remember: Information shared must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Further advice on information sharing

Confidentiality and Information Sharing for Direct Care (Department of Health)

Making effective use of data and information to improve safety and quality in adult safeguarding (Association of Directors of Adult Social Services and the Local Government Association, 2013)

What if a person does not want you to share their information? - Adult safeguarding: sharing information (Social Care Institute for Excellence)

Information: To share or not to share? - The Information Governance Review (Department of Health, 2013)