Ending domestic abuse

Sharing Information and Marac: GDPR and Data Protection Act 2018

Frequently Asked Questions (FAQs) - Scotland

Updated June 2019

Q: Does GDPR prevent us from sharing information about the perpetrator, including criminal offences when they will not have consented for that information to be shared?

A: No.
The purpose of the Marac process is for multiple agencies to work collaboratively to identify and assess the risks face by the victim(s), including the adult and any child(ren). Those risks need to be addressed, managed and reduced.

The perpetrator is the person identified to present the risk to victims and children, and sometimes to the wider public. It is therefore ***necessary*** to share with relevant agencies, those agencies who are party to your local Marac arrangement, **adequate relevant** and **proportionate** information about the perpetrator that will serve to, combined with other information and expertise shared, fully identify the risks they pose to enable effective safeguarding.

If the perpetrator has criminal convictions for offences that may indicate they pose a risk (e.g. violence; burglary; arson; harm to animals etc) and harm an adult or child then it will be necessary and proportionate to share that information with those who are working to manage and support the perpetrator AND with those who are working to support and protect adults and children at risk.

Q Do we need consent to share information?

A: No, not always.
GDPR gives us six lawful bases for sharing information and all six have equal status; no one basis is stronger or better than the other. The regulations set a high standard for consent and 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 reputation. If consent is difficult, look for a different lawful basis.

The basic concept of consent, and its main role as one potential lawful basis (or condition) for processing, is not new. The definition and role of consent remains similar to that under the Data Protection Act 1998. However, the GDPR builds on the 1998 Act standard of consent in several areas. It contains much more detail and codifies existing European guidance and good practice.
The GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms. You need clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw consent.

The changes reflect a more dynamic idea of consent: **consent as an organic, ongoing and actively managed choice, and not simply a one-off compliance box to tick and file**.

GDPR requires distinct ('granular') consent options for distinct processing operations. GDPR brings in the concept of consent being temporary and not enduring – i.e. consent is given by a data subject for a specific processing activity, and nothing else. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. Consent to share information is very different from consent to engage with a service. This is often misunderstood – for instance where an agency may choose not to share information about children where a child protection concern is raised because those with parental responsibility have not consented to do so.

As with all other lawful bases, information that is shared should be limited to what is necessary to achieve the purpose (e.g. to inform risk and needs assessments for effective intervention/offer of services); be proportionate and relevant. Those sharing information must be accountable for the information they hold and share, and record or log how decisions on information sharing without consent are made. Consent must always be specific and informed. If the purpose for sharing information changes through a process you need to either get fresh consent which specifically covers the new purpose or find a different basis for the new purpose.

The ICO have created a **Guidance for Consent** which provides more details for organisations and practitioners.

Q: What lawful basis do we use to share information in the Marac process?

A: There is more than one lawful basis that may apply when sharing information through the Marac process. The key things to remember are that you must decide upon your basis before you share information, and that you should chose the basis that is most appropriate for that circumstance. It is not GDPR compliant to adopt a one-size-fits-all approach.

No one basis is better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR. You need to record your purposes as part of your documentation obligations and specify them in your privacy information for clients. You can only share information for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

Refer to your local Marac Operating/Information Sharing Protocol which will detail the Lawful Basis for information sharing in the Marac process in your records to demonstrate compliance.

Note that consent is *unlikely* to be the lawful basis that can be relied upon for Marac because the requirements for consent include offering individuals real choice and control. If the threshold for Marac has been met, practitioners would refer to Marac irrespective of whether the person they've assessed to be at high risk consents, and so they do not have real choice and control.

We also recommend the **ICO website** for detailed guidance on the legal bases for sharing information.

Q: Can we share information without consent where the victim of domestic abuse is assessed to be at medium or standard risk? (Please note Marac is for High Risk victims only)

A: Yes, BUT the information shared may be limited in detail and content. You will need to consider the following:

- Is there another lawful basis such as legitimate interest, legal obligation (e.g. reporting a crime/child protection), or public task that would enable information to be shared?
- What is your relationship with the individual? Would sharing of limited information (however transparently) have a detrimental impact on your relationship and a loss of trust? If so, consider how that can be managed/minimised/avoided.
- Consider seeking consent at every step of data processing – when the individual has full understanding of what is being shared, with whom, how and why they may give consent.
- What is the purpose for sharing the information? To identify risk and assess needs? Often, once information is shared, creating a clearer picture and understanding of risks, consent may not be the most suitable lawful basis for further sharing.
- How much of the information you hold is necessary to share to achieve an accurate risk assessment and with whom? (It is not always necessary to share information with several agencies and will not always be justifiable to do so)
- Record and always log your decision-making process noting any change in purpose and or lawful basis
- At **ALL TIMES** the safety of the adults and children living with domestic abuse takes precedence. If you choose not to share information you should document that too.

Local information sharing protocols should allow for situations when information does not reach thresholds for sharing widely in a multi-agency arrangement (e.g. Marac (high risk) threshold; child protection; Mappa (levels 2 & 3) etc. Practitioners must feel confident and supported to share and seek information (with expert analysis) for the purpose of making an accurate assessment of risk and need which will inform any offer of early help and intervention to reduce risks and meet needs to prevent escalation.

Consider the analogy of a dimmer switch when thinking about sharing information. The more the switch is turned, the brighter the light that shines, thus illuminating the bigger picture. Consider how you can break down the information sharing process to achieve an improved understanding of risk and need. How can you minimise the information you share whilst still achieving your aim/purpose? What lawful basis other than consent can you rely upon? **Document and log your decision-making process**.

Q: How long should we retain case files?

A: All methods of retaining personal information must be compliant with your Maracs Privacy Impact Assessment (see previous **GDPR Guidance for Marac Governance Groups** (under review)). This will provide your local guidance on information processing, storage and retention but each agency will also have their own internal policies which will need to be checked when planning if & how you intend to retain information from Marac.

Briefly, the Data Protection Act states: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

This requires organisations to do the following:

- Consider the **purpose or purposes** they hold the information for in deciding whether (and for how long) to retain it;
- **Review** the length of time they keep personal data;
- Securely **delete** information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

Recital 39 of the GDPR states that the period for which the personal data is stored should be limited to a strict minimum and that time limits should be established by the data controller for deletion of the records (referred to as erasure in the GDPR) or for a periodic review. This would be detailed in your retention schedule. Appropriate timescales for retention will depend on the purpose of processing and should have a regular review for accuracy and necessity built in.

Organisations must ensure personal data is securely disposed of when no longer needed. This will reduce the risk that it will become inaccurate, out of date or irrelevant.

The GDPR does not specify exact data retention timescales, and the reason for this is that the periods for which you can justifiably keep data are necessarily context-specific. For example, in relation to the guidance around flagging and tagging files in order to identify repeats; retaining personal data to enable practitioners to identify if someone has been referred to Marac would be justifiable for the 12 months we advise that someone remains high risk.

We support the ICO recommendation that organisations create a comprehensive data retention schedule/policy which will outline the relevant laws, regulations and risks that affect them and that may mandate specific retention periods. The retention schedule should also be very clear on what is the minimum data that can justifiably be retained.

Q: Do we have to have a privacy notice for every client (who comes into the Idaa Service)?

A: Yes, individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. You must provide individuals with information, including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.

We call this 'privacy information'. You must provide privacy information to individuals at the time you collect their personal data from them. The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

Q: Our local Information Sharing Protocol (ISP) has not been updated for a long time. What should I do?

A: It is essential that your ISP reflects the requirements laid down by GDPR and DPA 2018. It is the responsibility of your Marac governance group to ensure that these protocols are up to date and support the compliance of the Marac process with GDPR and DP. However, nothing removes the

accountability and responsibility for compliance held by each individual service who are holding and sharing information throughout the Marac process.

Q: Our local Idaa Service only accepts referrals when the victim has consented, can we challenge this?

A: Yes, this should be challenged because consent is not the appropriate lawful basis for sharing information when someone has been assessed to meet the Marac threshold (high risk).

By requiring consent before contacting a victim of domestic abuse, the service are potentially missing an opportunity to engage victims who would benefit greatly from their specialist support. SafeLives recommend that those who commission services are made aware of restrictions being placed on accessing the service in this way. Whilst we do understand that some Idaa services have made the decision to restrict access in this way to manage volume and capacity, it may raise the risk for some victims and children living with domestic abuse.

SafeLives can support organisations to seek additional funding from commissioners where their service is working over capacity and/or to consider how case management can be more efficient and effective and open to all those in need.

Q: Can victim services hold information about perpetrators on their case management systems?

A: Yes. Where information is held about victims of domestic abuse who are clients/former clients of that organisation it can be reasonably expected that within that information will be personal and sensitive information that identifies the perpetrator of abuse – the person who presents the risk to the victim and children. Retention of this information will be limited to what is considered to be a reasonable and justifiable length of time and should be subject to regular review.

Q: Is there guidance on where a domestic incident is recorded (i.e. child's file in children's social work or in mother's file). Does this have an impact on GDPR if the child was not involved in the incident and later requests to see their file?

A: The impact on children of living with domestic abuse is widely known and forms the basis for the current acknowledgment that children are victims of that domestic abuse regardless of whether they are directly physically harmed or not. It follows then that it can be justified and reasonable to record the incident on both the adult victim's (non-abusive parent) and the child(ren)'s file.

The level of detail and personal information recorded should be considered. What is the aim of recording and retaining this information – for the purpose of identifying adverse childhood experiences? Identifying potential risk? Would a reference to the victim's file or flag for domestic abuse be adequate and fulfil this purpose? Would it be of significant detriment to the individual if this information is retained (and later disclosed)? Does the reason for retaining that information override any detriment this may cause? Record and document all decisions.

Q: How long should the Marac Coordinator keep information with respect to a party to Marac?

A: Even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you need it. We recommend that the data held is reviewed **annually** from the date of the original referral, when the accuracy of the data is confirmed and consideration is given to deleting the information – bearing in mind the relevance and necessity to retain the data without anonymising it any longer. Anonymised data can be kept for as long as you want.

Ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention. From a more practical perspective, it is inefficient to hold more personal data than you need, and there may be unnecessary costs associated with storage and security.

Remember that you must also respond to subject access requests for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure. SafeLives cannot give legal advice around retention periods but would advise you to consider, on review of the data you hold, the following justifiable reasons for retaining the information (minimised to Marac minutes and action plans):

- To be available for scrutiny in the event of a homicide, suicide or unexplained death
- To be available for scrutiny where there is a child protection concern
- To be available for disclosure in court proceedings (civil, family or criminal)

Consideration should be given to the age of the children whose personal data is held and whether it is necessary or justifiable to hold information until any minors reach majority. Refer to your local Marac Operating Protocol, where applicable, internal data protection and retention policies and seek advice from your data officer; the ICO or your legal advisors when developing your policies and making decisions on retention periods.