Ending domestic abuse

The General Data Protection Regulation (GDPR) A briefing for Maracs

updated May 25th 2018

The General Data Protection Regulation (also known as the GDPR), replaces the existing Data Protection Act of 1998 on 25th May 2018. The UK Data Protection Act 2018 sits alongside but remains separate from the GDPR. The introduction of new legislation can cause concern and confusion, which can in turn limit information sharing. For a full list of the legislative changes, see the website of the **Information Commissioner's Office**.

We have created this briefing as a general guidance for those managing the Marac process to help understand what **changes** you can expect; the **impact** on the Marac process and what Marac Governance groups need to **consider** to ensure compliance; linking relevant and useful **resources** where appropriate.

How does GDPR change Data Protection?

The changes which the GDPR bring are predominately about tightening up data management practices including, for instance better recording of data, improving the content of privacy notices, and the way consent is obtained. It is not, therefore, a total overhaul of systems and processes. The GDPR places more emphasis on being accountable for and transparent about the lawful basis for processing data. (See Article 6)

How will GDPR impact on the Marac process?

Under the GDPR, the data protection principles set out the main responsibilities for organisations and it is each organisation's responsibility to ensure that they are GDPR compliant by 25th May 2018. A useful guide has been produced by the ICO for all agencies to plan for compliance: **'12 steps to prepare for GDPR'**.

Considerations for Marac Governance Groups

Awareness

All organisations that are currently signed up to the Marac operating & information sharing process need to be aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and ensure that they are compliant. We recommend that Marac Governance Groups as part of their review of operating protocols be satisfied that all agencies are GDPR compliant. This will ensure high level compliance with data protection legislation throughout the process and reduce the risks of data breaches, notifications of which will now be mandatory. It seems reasonable that Marac Governance Groups know the identity of designated Data Protection Officers in each agency.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(4) The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality**.**

Glossary of Terms & Resources

Controller: *controls the purposes and means of processing personal data*

GDPR checklist for data controllers

Processor: *responsible for processing personal data on behalf of a controller*

GDPR checklist for data processors

Personal Data: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (e.g. name, DOB, ID code etc)

DPIA (Data Protection Impact Assessment): *(See Article 35)* A DPIA is a process for building & demonstrating compliance. It is designed to describe the processing, assess the **necessity and proportionality** of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)4 (also referred to as Privacy Impact Assessment)

IMPORTANT

A Marac is neither an organisation, nor an agency. A Marac is not a legal entity in its own right.

This Briefing is not intended to be a detailed Guidance for those agencies or practitioners looking to check their own GDPR Compliance status. It is essential that the ICO is used as the source for that information and we have added links here where appropriate which will help you navigate the websites, the GDPR & The DP Bill

ICO: DPA 2018

Children & the GDPR Guidance
The consultation closed on 28 February & the ICO are yet to publish the Final Guidance. See Draft here

SafeLives are currently reviewing and updating all relevant Marac templates, Guidance and other documents to reflect GDPR & The UK DP Act 2018

They will be published on our website in due course

www.safelives.org.uk

knowledghub@safelives.org.uk

Data Protection by Design and Data Protection Impact Assessments

We recommend that Marac Governance groups familiarise themselves now with the **ICO's code of practice on Privacy Impact Assessments (PIA)** as well as the latest guidance from the Article 29 Working Party, and Part 3 Chapter 4 point s.64 DPA 2018. If the Marac has a website or has links to websites the PIA must be displayed.
"Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment." (Pt3 Ch 4 s,64(1) DPA 2018)

Data Protection Officers

Marac Governance groups should consider designating a task group to take responsibility for data protection compliance and assess where this role will sit within the Marac structure and governance arrangements. As Marac is not an entity it relies on each agency being data compliant.

Information held

The Marac as best practice evidences should document what personal data is held in the minutes, where it came from (the agency referring in) and who it is shared with – agencies in attendance when the case is heard. The ICO advise to organise an information audit. The agency that hosts Marac administration systems will need to include this within their process and enable Marac data in their audit to be GDPR compliant.

Communicating privacy information

Marac should review current information sharing, operating protocols and privacy notices, putting a plan in place for making any necessary changes in time for GDPR implementation.

Individuals' rights

Marac Governance and all agencies will need to check procedures to ensure all the rights individuals have are covered, including how personal data would be deleted.

Subject access requests

Agencies should update their procedures and plan how they will handle requests within the new timescales and provide any additional information. Information shared in the Marac process is owned by those sharing that information or processing that data. Marac Governance Groups and agencies should familiarise themselves with the information that is Exempt (S40(4) & Reg 13(3))

Lawful basis for processing personal data

The Marac and agencies that are signed up to Marac will need to identify the lawful basis for all data processing activity in the GDPR Article 6; this must be documented and the privacy notice updated to explain it.

See advice and guidance on the ICO website. Of relevance to the Marac, it is important to note that to process personal data about criminal convictions or offences, there must be both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. Much of the information shared in the Marac process will fall into the **Special Category Data**. To lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked. See links on left to fully understand the categories of information.

Links to Relevant Resources

Lawful Basis for processing Data
Consent
Contract
Legal Obligation
Vital Interest
Public task
Legitimate Interests
Special Category Data
Criminal Offence Data
Safeguarding Amendment to

Victoria Atkins MP announced the bill is intended to make it easier to carry out "legitimate safeguarding activities that are in the substantial public interest, and will "cover the safeguarding activities expected of organisations responsible" for individuals at risk.

The bill will provide a framework within which organisations can justify such reasonable preparatory and policy steps as they deem necessary. This may include bespoke policies on monitoring, reporting, retention and record-keeping: to ensure organisations capture all the information relevant to questions of early help or prevention.

On 23rd May 2018 the DP Bill became law:

The UK Data Protection Act 2018

SafeLives recommend that all agencies continue to source advice & guidance on all aspects of processing & storage of personal data from the ICO website.
We will endeavour to update this briefing as and when required.

The DPA 2018, and amendment 85, goes further in empowering organisations to process personal data for safeguarding purposes lawfully, without consent where appropriate. The new amendment provides a lawful ground for the processing of special category personal data – without consent if the circumstances justify it – where it is in the substantial public interest, and necessary for the purpose of: (i) protecting an individual from neglect or physical, mental or emotional harm; or (ii) protecting the physical, mental or emotional well-being of an individual. Where that individual is:

- a child or an adult at risk
- under 18 or,
- having needs for care and support,
- experiencing or at risk of neglect or any type of harm
- unable to protect themselves.

The amendment still expects the **possibility** of obtaining consent, unless it would prejudice the safeguarding purpose (i.e. the protection of the individual). The question must be whether the use of the personal data is **proportionate** to the lawful aim. The law intends any justifiable step to protect individuals at risk to be considered as being in the substantial public interest.

It is worth noting that the amendment concerns special category data (including physical and mental health or sexual life) but not criminal records information, which is now to be treated separately.

Consent

Organisations should review how they seek, record and manage consent and whether they need to make any changes. Everyone will need to refresh existing consents now if they don't meet the GDPR standard. We recommend that agencies follow the advice and guidance of the ICO. Consent is one way to comply with the GDPR, but it's not the only way. The GDPR sets a high standard for consent. For cases meeting the Marac threshold of high risk, it is possible that consent will not be the lawful basis under which information is shared. However good practice would dictate that consent still be sought. Recording the lawful basis & any legislation relied upon will be key in justifiable decision making for every agency throughout the Marac process.

Children

The GDPR does not represent a fundamental change to many of the rights that children have over their personal data. It explicitly states that children's personal data merits specific protection and so contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand. Transparency and accountability are important where children's data is concerned. In all circumstances you need to carefully consider the level of protection you are giving that data. See the detailed guidance.

Data breaches

The Marac Operating/Information Sharing Protocol should make sure Maracs have the right procedures in place to detect, report and investigate a personal data breach. It is important going forward that Marac Governance groups track legal and regulatory developments to ensure ongoing compliance.
The ICO's intention in the longer term is to develop their main suite of guidance to cover the Data Protection Act 2018 in more detail. They will publish this under the umbrella of a new Guide to Data Protection and it will cover the GDPR, the applied GDPR, Law Enforcement and any other relevant provisions.