NATIONAL Maternity Voices

Networking Maternity Voices Partnerships in England

General Data Protection Regulations guidelines for Maternity Voices Partnerships

## What is GDPR?

New General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and is a regulation in EU law on data protection and privacy for all individuals within the European Union. GDPR aims primarily to give more control to citizens and residents over their personal data[1] and who can handle it. It applies to all organisations that offer goods and services to or monitor the behaviour of EU citizens.[2]

From 25 May 2018 any EU citizen can submit a Subject Access Request (SAR) to any organisation, asking for details of the information that that organisation holds about that individual.

## The seven data protection principles

1. Lawfulness, fairness and transparency:
   Personal data should be processed in a lawful, fair and transparent manner.

2. Purpose limitation
   Personal data should be collected for specified, explicit and legitimate purposes and not further processed for additional purposes.

3. Data minimisation
   Personal data should be adequate, relevant and limited to the purposes for which it is processed.

4. Accuracy
   Personal data should be accurate, and where necessary, kept up to date.

[1] Personal data is any information which relates directly to an individual and can be linked directly to them. For example, this includes: name, phone number, email address, photographs, genetic and economic data. https://www.voluntaryarts.org/Handlers/Download.ashx?IDMF=dae6266a-1b81-4326-a5b1-ebe7ef9b0835

[2] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

5. Storage limitation
   Personal data should not be kept in a form which permits identification of someone for longer than is necessary.

6. Integrity and confidentiality
   Personal data should be processed securely.

7. Accountability
   Organisations must be able to demonstrate compliance with data protection regulation.

   (There is an eighth principle, around international transfer, which states that personal data shall not be transferred to a country or territory outside the European Economic Area[3])

**What does this mean for MVPs?**

Each individual MVP is a data controller, and a data processor under the new law, meaning each individual MVP will be responsible for the data they collect on any individual. The type of data we generally collect is classed as sensitive personal data. The new regulations mean that organisations need to be open, honest and transparent about the data they collect and be extremely clear with any individual about what they are going to do with their data and how long it will be stored.

Recommendations to ensure MVPs are GDRP compliant by 25 May.

1. Emails

- when sending out group emails, blind-copy contacts.
- Have a signature at the bottom of your email enabling people to remove themselves from the mailing list at any time e.g. "You are being sent this email as part of the xxxx distribution list. If you no longer wish to be on this distribution list, please let me know and you will be removed". Remember, consent must be freely given and can be withdrawn at any time.
- You may want to consider having a generic email address for your MVP e.g. greenwichmvp@gmail.com (gmail addresses often work well for this) rather than having a personal email address for MVP business. This also helps with succession planning. You may want to password protect your email address.
- Set up an auto-response on your email account, outlining who will read the email and what will happen to their personal information. For example: “Thank you for contacting Bromley MVP. This email account is monitored by the

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

chair, XXXX, and your message will be responded to as soon as possible. For information on what we do with your personal data, please see our privacy policy at nationalmaternityvoices.org.uk/privacy

If you have a MVP website you can add the NMV privacy policy to it and refer to that link instead.

2. For data collection (e.g. Walk the Patch, surveys, questionnaires and gathering anonymous feedback)

- Under principle 1, see above, there should be a written privacy notice (see below) available at every point where we collect personal information. This includes surveys and questionnaires. If you are gathering data face-to-face or over the phone, (e.g. Walk the Patch) you must read out the appropriate privacy notice. Verbal consent from any individual is sufficient.
- Under principle 3 (see above) if someone offers more information than is needed it should not be kept or recorded. For example, if someone gives their job title or description when filling out a survey about maternity experience, it could be that this information is not relevant and so it should not be recorded.
- Anonymous data: Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by organisations to conduct research. Fully anonymous data is not covered by GDPR as it contains no personal information to protect[4].

3. Images:
Photographs are also classed as personal data and therefore a release document (see below) will be needed, signed by all participants, to use any images. This includes photos at any MVP event or meeting.

[4] https://www.voluntaryarts.org/Handlers/Download.ashx?IDMF=dae6266a-1b81-4326-a5b1-ebe7ef9b0835

**Further practical guidance**

There are many relatively simple steps that we can take to reduce the risk of losing or allowing someone unauthorised access to personal information. These include:

1. Follow a ‘clear desk’ policy when working with personal data in the office and if at home.
2. Do not leave papers and files containing personal information unattended on printers, photocopiers or on your desk, whether you are in the office or working at home. Access to personal information should be limited to those on a strict need to know basis.
3. Lock your screen when you leave your desk - press the Ctrl+Alt+Delete keys or Windows + L shortcut and log off properly from any machine you use at the end of the day.
4. Do not share or write down your passwords.
5. Ensure that the desks and cupboards that you use to store sensitive personal information are locked and the keys are securely stored.
6. Do not leave papers or screens containing personal information visible to others – for example, in meetings, on trains, even in your own home.
7. Dispose of all paper documents (including hand written notes) that contain personal information when you have finished with them in line with the data retention policy using a confidential waste bin or shredder.
8. Use Royal Mail registered post or courier when sending large volumes of hard copy personal information or sensitive personal information.
9. Limit your use of mobile devices such as memory sticks, CDs, DVDs and removable hard drives as much as possible, and ensure that if you do use them they are encrypted and password protected.
10. Protect all electronic devices that you use to process and store personal information with encryption and strong passwords. This includes computers, laptops, tablets and smart phones. Special care should be taken when travelling with these devices.
11. Do not disclose someone’s personal contact details such as email address or telephone number without their prior consent.
12. Always use the bcc field (not the cc field) when sending an email to more than one person so that the recipients’ email addresses are not visible to each other (unless you have permission of the recipients to share their email addresses).
13. Check first who is in an email group to ensure that only the right people receive the email.
14. Do not include personal information in the subject line of an email.
15. Protect files or documents containing personal information with encryption and a strong password if it is necessary to email them.
16. Double-check that you have attached the correct file before you click ‘send’ when attaching files to an email.
17. If it is necessary to email an electronic file or document containing personal information, protect it with encryption and a strong password.

Encryption is the scrambling of text or data for security purposes. Zip can be used for encryption.[5]

**MVP specific scenarios:**

**A woman contacts the chair of an MVP via email with a detailed description of her birth experience and asks how she can feed this back to the Trust**

Put the woman in touch with the appropriate channels to feed back (e.g. PALS, HoM, listening service if there is one). Do not forward the email on to anyone else or share any details without first gaining explicit consent from the woman to do so.

Once the matter has been successfully actioned, delete the original email and all other correspondence relating to it (suggest by 6 months after the last planned contact).

**A woman contacts the chair of an MVP via Facebook with a detailed description of her birth experience. Chair feels it would be useful to feedback the theme of her experience for Better Births implementation.**

Facebook/social media in general have their own consent policies. By sharing something over Facebook, the user is consenting to FB holding that data. The chair is not responsible for deleting any data on social media. Chair would ask the woman if she consents to her feedback being communicated anonymously. If there is any way that the data may make the woman identifiable, that should be explained to the woman and consent sought. No personal data should be shared with anyone else without express consent. Any records of conversations or correspondence relating to this matter (notes, emails etc) should be deleted once the matter has been successfully actioned.

**Walk the Patch is carried out by an MVP volunteer in a maternity unit or in the community.**

The volunteer must explain what Walk the Patch is and what the purpose is and explain clearly how the information they gather will be used (e.g. who it will be shared with, whether it will be anonymised, where it will be displayed etc). They should gain verbal consent from the woman/family that they are happy to share this information. Any written notes must be destroyed.

**An MVP wants to carry out a survey in their local area about womens' experiences of induction**

[5] Adapted from NCT data protection guidelines for practitioners

The MVP would draft a survey. A clear and explicit privacy notice would be at the top of the survey (see below). If the survey was for long term reference, this would have to be made explicit. The survey questions need to ensure the data captured is adequate, relevant and not excessive (principle 3). Data must be fully anonymised before use. Any personal data needs explicit further consent to be shared.

**Privacy policy**

National Maternity Voices has written a privacy policy for NMV and local MVPs which can be found here: nationalmaternityvoices.org.uk/privacy Do refer any service users to this. At each contact point (survey, questionnaires, face-to-face meetings) a privacy notice should be available (see below for template). The privacy notice must also be read out to service users if gathering feedback over the phone. Verbal consent is sufficient from the service user.

**Privacy notice – template**

We will use the personal information that you provide in this form in accordance with applicable data protection laws and our Privacy Policy - available at nationalmaternityvoices.org.uk/privacy

This information is being collected by your local Maternity Voices Partnership to gain a better understanding of current local maternity services so that improvements can be made in the future. We will process your personal information in order to deliver this service safely and effectively, and where otherwise reasonably necessary for our purposes.

You can expect your personal information to be stored securely. It will be kept on our systems for as long as is necessary for the relevant activity We will not share your personal information (contact information) with anyone else without your explicit prior consent. Your responses will be anonymised and only used for the purpose of improving local maternity services.

If you would like to find out more about your local MVP and the work that we do, please contact us

You can also contact us at any time to ask for your personal information to be updated or deleted.

**Release document for photos - template**

Photos are classed as personal data and therefore need consent before using.

I _____give permission to _____ to use my photographs to advertise the work of the Maternity Voices Partnership, without payment or any other consideration.

I understand that these photographs may be used in printed material as well as online and on social media.

I understand that I can access photographs featuring me on request and that I will receive confirmation regarding how these are being used.

I understand that I have the right to request photos be removed from future printed materials, websites and social media at any time.

I am the parent/legal guardian of the child featured in the images and give consent for these images to be used. (if the photo features a child under 18)

Signed_____ Date_____

For further information on GDPR see the ICO website https://ico.org.uk/for-organisations/