# The General Data Protection Regulation (GDPR): an introduction for small charities and voluntary organisations

John R Hudson*

29th May 2018

This is an updated edition of an earlier paper about the GDPR incorporating the application of the GDPR to the UK through the Data Protection Act 2018; it does not purport to cover all aspects of the Regulation or the Act but just those matters which appear to be relevant to a small charity or voluntary organisation.

## 1 Introduction

1. This paper is intended to summarise the key implications of the General Data Protection Regulation (GDPR)[1] as enacted through the Data Protection Act 2018[2] for small charities and voluntary organisations which are not companies and have few or no paid staff.

2. The GDPR covers any data which can directly or indirectly identify a living person and which is being used for a purpose other than for a 'purely personal or household activity.' The Data Protection Act 2018 implements the GDPR for the UK, modifying some of its provisions as they apply to the UK and making some additional requirements which are not specified in the GDPR.

3. Even though UK legislation has historically not required organisations which only process the personal data of their members to register under data protection legislation, they have still been required to abide by the data protection principles enshrined in the law and the same is the case with the GDPR.[3]

4. Where Trustees, officers, staff or volunteers of small voluntary organisations know each other socially outside the organisation, it will be important for them to beware of sharing personal data related to their work for the voluntary organisation during, for example, a conversation in a café or other public place, or in the course of an unencrypted email covering other topics.

*With thanks to the members of the Bradford Linux Users Group for their helpful comments and suggestions.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[2] Data Protection Act 2018

[3] At the time of writing, there is no information on the Information Commissioner's website to indicate that this will change.

## 2 Background

1. The 1984 Data Protection Act enacted the 1981 Data Protection Convention of the Council of Europe in the UK.

2. In the 1990s the European Union made signing the 1981 Data Protection Convention a condition of membership of the EU.

3. However, with the rise of the Internet and social media, it became clear that the 1981 Convention was an inadequate tool for managing data protection. It also imposed limitations on data collection which undermined the ability of researchers to collect long term data on particular medical conditions and on some types of historical research.

4. So the European Union embarked on a long consultation on a new convention for the European Union whose more stringent regulations relating to privacy were criticised, particularly by US companies, until the Snowden revelations showed the extent to which individuals' privacy was being invaded anyway.

5. The Data Protection Act 2018 (DPA 2018) enshrines the GDPR in UK law because, as with the earlier Council of Europe Convention, other European countries, both inside and outside the EU, would refuse to trade with the UK if the UK did not treat personal data in the same way as other European countries.

## 3 Principles

Article 5 says that:

1. Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('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 ('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 ('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 ('storage limitation');
   (f) processed in a manner that ensures appropriate security of the personal data ('integrity and confidentiality').

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

## 4 Practical implications

1. Everyone whose personal data you use must have consented to the use of their personal data in the way you use it or entered into a contract with you which involves using personal data as part of the contract.[4] Otherwise, you must not use that personal data except to fulfil a legal obligation, to protect their vital interests or in the public interest (Article 6).

2. People must know who is collecting the data, by whom it will be used, for what it will be used and for how long and how to make queries/complaints about its use (Article 13). This also applies where the data is obtained from someone else (Article 14). Anyone can ask anyone whom they think may be holding personal data on them for the same information (Article 15).

   It is worth thinking about how you use people's personal data and then drawing up a privacy statement, which you share with everyone who contacts you or shares personal data with you, about

   - who is collecting the data,
   - by whom it will be used,
   - for what it will be used and for how long and
   - how to make queries/complaints about its use, and
   - how to complain to the Information Commissioner if they are dissatisfied with your response.[5]

   You need to appoint someone as 'data controller,' responsible for keeping track of what data the organisation holds and who in the organisation is using it and for what purposes. That person should normally be the point of contact for queries/complaints.

3. You must be able to demonstrate that everyone had given their consent and everyone must be able to withdraw their consent easily at any time and that withdrawal must be acknowledged. 'It shall be as easy to withdraw as to give consent' (Article 7).

   You must keep a record of everyone's general consent under Article 6.

   Consent must be active; you need to use opt-in rather than opt-out buttons and check-boxes linked to a statement of the uses to which you will put someone's personal data on a website or a form in order to demonstrate that the person has actively consented.

   Also, if you have used opt-in buttons or checkboxes to gain consent, you should use opt-out buttons or checkboxes to enable people to withdraw consent.

   However, you do not have to re-seek consent where a person had given consent prior to the implementation of the GDPR though a contract, including membership of an organisation, or through explicitly giving their consent to your contacting them provided that you have some record of that previous consent.

4. The processing of personal data relating to criminal convictions and offences is prohibited unless permitted by an official authority (Article 10).

[4] Article 8 lays down conditions for parental consent for children under 16 years of age to use social media. DPA 2018 (§9) defines children as under 13 years of age for this purpose.

[5] If you happen to use personal data extensively, refer to Articles 13 and 14 for more specific details.

5. Processing of sensitive personal data such as that related to beliefs and health is prohibited without the person's explicit consent except where it may be essential to the functioning of the organisation (Article 9).

   In other words, you must ask people for specific consent to hold any data about personal beliefs or personal health and not rely on any general consent unless, for example, you are an organisation all of whose members share a particular belief system or suffer from the same medical condition or you are a hospice which would need to know about their personal health. In the case of a membership organisation, the data can only be shared within the organisation.

   The GDPR makes provision for organisations to have internal[6] policies where proportionate to the amount of data processing they do (Article 24(2)).

6. The data controller must supply information about their responsibilities and activities in a form which is easily accessible to people, including children, and make it easy for people to exercise their various rights (Article 12).

   Strictly speaking, the information only needs to be accessible to children if the organisation holds personal data relating to children; but it is worth remembering that there may be adults with certain disabilities who might need an accessible statement. As the DPA 2018 (§52(1)) says in another context: the information is to be provided 'in a concise, intelligible and easily accessible form, using clear and plain language.'

7. People have a right to the rectification of inaccurate or incomplete data (Article 16), the deletion of data for which there is no reason for it to be retained (Article 17), the restriction of its use in such cases (Article 18) and the right to receive an acknowledgement when any of these have been done (Article 19).

   Again, it is probably helpful if this is managed by the 'data controller.'

   This and other requests must be dealt with 'without undue delay and in any event within one month of receipt of the request.' You cannot charge a fee except in the case of 'manifestly unfounded or excessive' requests (Article 12).

8. People may withdraw their consent to certain types of processing, e.g. for marketing purposes (Articles 21 and 22).

   Another job for the 'data controller.'

9. Data controllers shall implement proportionate measures to ensure compliance (Articles 25ff).

   This allows small organisations to comply with the regulations in ways which are manageable for them. However, the expectation is that data controllers are familiar with the technical and organisational measures which it would be reasonable to implement. So organisations without anyone with the technical skills would be advised to get advice from someone with recognised qualifications.[7]

[6] Nowhere does the GDPR or the Data Protection Act 2018 require the publication of these policies where they exist; but they must be made available in appropriate circumstances.

[7] DPA 2018 (§58(3)) requires joint controllers to designate one as the point of contact; however, this section is not part of the section on the general application of the GDPR.

10. The data controller may appoint a data protection officer to advise on the implementation of data protection measures appropriate to risks if personal data were lost or misused; the data protection officer need not be a member of the organisation and data controllers in small organisations may agree to use one person as the data protection officer for them all (Article 37).[8]

11. People who use data (processors) must abide by the directions of the data controller (Articles 28 and 29) and keep adequate records of their data processing (Article 30).

    The data controller must issues directions and anyone in the organisation who uses data must follow these directions. Note that, under Article 82, if a processor does something wrong about which the data controller should have issued a direction and did not, the data controller will be held responsible. Equally, if a data controller has issued a direction and a processor has ignored it, the processor will be held responsible.

12. Data controllers shall ensure that measures appropriate to the risk, including accidental risks, are taken to ensure the security, confidentiality and integrity of personal data (Article 32).

    This will primarily involve ensuring that data is held on password protected devices with all security updates installed, is only transmitted over the Internet in encrypted form and is backed up regularly. Note:

    (a) laptops and smartphones should be more highly protected because of the greater risk of loss or theft but desktop computers should also be sufficiently protected to prevent a thief or a casual visitor to an office from accessing the data;

    (b) everyone should have their own individual password for accessing a device and passwords to access a device should never be shared between two (or more) users;[9]

    (c) encryption can be provided by third parties, as when you use a secure website or secure messaging service, or can be provided by software you install on your devices; which you choose will depend on the sensitivity of the personal data which you hold, why you need to transmit it and the harm that might be caused by its loss;

    (d) encryption passwords and passphrases should be strong, that is, long rather than short, without any identifiable dictionary words and including upper and lower case letters, numerals and punctuation;

    (e) it will normally be prudent to ban the use of USB sticks for transferring data.

13. Data controllers shall report all data breaches to the appropriate authority within 72 hours (Article 33) and to the data subject (Article 34).

    This is mainly to stop banks and Internet providers from hiding the number of times people break into their systems and leaving customers vulnerable to harm which could have been mitigated if the customer had known about the break in. But some voluntary organisations will hold personal data about people whose disclosure could cause them serious harm if they cannot take steps to mitigate the harm.

[8] Note that, should a data controller decide to appoint a data protection officer, this is a data controller and not a Trustee appointment.

[9] One or more administrator users may have administrator passwords but these should not normally be used to access a device. Administrator users should access a device with their personal password and only use the administrator password once they have accessed the device.

14. Anyone who suffers as a result of an infringement of the GDPR has a right to compensation from the data controller or processor, unless they are in no way responsible for the event causing the harm (Article 82).

    For example, if there is a theft from a password protected device with all its security updates installed by a cybercriminal using a hitherto unknown bug in the software, a controller or processor would not be liable to pay compensation.

15. Processing for archiving, scientific or historical research or statistical purposes is permitted subject to particular provisions (Article 89). The DPA 2018 specifies that, in the case of archiving, research and statistical purposes:
    - processing cannot cause 'substantial damage or substantial distress to a data subject' (§19(2)), and
    - processing cannot be 'for the purposes of measures or decisions' in the present (§19(3)).

16. Religious associations which have their own rules for processing data must bring them into line with the GDPR (Article 91).

## 5 Conclusions

1. The key changes as far as most small voluntary organisations are concerned are:
    - the greater emphasis on obtaining consent to use someone's personal data,
    - the greater emphasis on the security and privacy of data and
    - the need to have someone responsible for how data is used and for people to abide by their instructions.

2. Don't rush into securing all data. Take time to identify what personal data you hold, how you use it and how it might need securing/encrypting. A lot of data held by voluntary organisations is not personal data and so is not affected by the GDPR even though organisations may need to be prudent about its care if it holds sensitive non-personal data.

3. Shred/delete personal data which you can no longer justify holding.

4. Seek advice if you are ensure how to secure/encrypt personal data but beware of expensive proprietary options; the best security software is available free though it may require some expert help to set up.

5. Finally, remember that most security breaches take place because of human error; make sure your Trustees, officers, staff and volunteers understand their responsibilities under the GDPR and know how to use any security software you put in place to meet your responsibilities under the GDPR.

## A Some software options

- Keybase: it works like Dropbox setting up shared folders which can be accessed only by certain people. No data is passed to Keybase, only the keys to the folders to allow sharing.
- VeraCrypt allows you to encrypt parts of hard drives; it is probably most suited to office based systems.
- WhatsApp, a secure messaging service, now owned by Facebook, might be suitable for some organisations but would need checking for its suitability.
- Thunderbird allows you to encrypt emails; however you need a program like GnuPG to provide the encryption keys.
- There is also a plugin for Outlook which enables you to use it with GnuPG encryption.