Charities & Education

General Data Protection Regulation (GDPR)

A guide for charities

GUIDANCE FOR CHARITIES – GDPR

TABLE OF CONTENTS

GUIDANCE FOR CHARITIES - GDPR

General Data Protection Regulation (GDPR) comes into force on 25 May 2018. The GDPR is wide ranging and aims to put the rights of individuals at the centre of data protection law.

GDPR vs DPA

The GDPR is a continuation of the Data Protection Act. However, there are areas where enhancements have been introduced and therefore careful analysis of how data has been treated in your organisation in the past and how it will be treated in the future needs to be undertaken.

GDPR - WHAT STEPS YOU TAKE

1. YOU MUST REVIEW AND UNDERSTAND HOW YOUR ORGANISATION USES PERSONAL DATA

It is important to verify the data flows and existing systems and processes that utilise personal data. For example, you need to consider:

i. What data you hold and whether you have any sensitive or special category data as special rules apply to them;
ii. Where you receive data from and why;
iii. Who do you share data with and why; and
iv. How do you store data and for how long do you store it.

Once you have understood your organisation's approach to data you can then carry out a "gap analysis" to determine what areas need to be changed or updated to ensure compliance with the new regulation.

If you are a large organisation you may wish to instruct a company to determine your data flows and carry out a gap analysis for you.

2. YOU MUST DETERMINE ON WHAT BASIS YOUR ORGANISATION PROCESSES PERSONAL DATA

There are six lawful grounds on which your organisation may process data. You need to determine what ground you are relying on and publicise this in your Privacy Notice (discussed below).

It is likely that the most relevant ground will be one or a combination of the below:

- processing is necessary for the purposes of the legitimate interests pursued;
- the data subject has given consent;
- processing is necessary for the performance of a contract; or
- processing is necessary for compliance with a legal obligation.

You will need to consider what ground you use in relation to all of the different individuals you interact with (for example donors, service users, volunteers and employees) and in relation to the different data you collect from them.

Legitimate Interest Ground

The legitimate interest ground is satisfied if the individual data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place and that the interests and fundamental rights of the data subject do not override the interest of the data controller.

If you decide that you have a legitimate interest to process the data then you must be able to demonstrate that you satisfy the ground. You may do this by preparing a report to show that you have analysed your position and concluded that you believe the organisation satisfies the ground.

Consent Ground

Consent should be used as a ground for processing if you are giving a genuine choice to the individual over how their data is used. If you would still process the data without the consent of the individual, then this is an inappropriate ground to use.

When consent is used it must be freely given, specific, informed and unambiguous. For example, you may not infer consent from silence, pre-ticked boxes or inactivity.

If consent previously received does not comply with the new requirements then the existing consent will be invalid and new consent will need to be obtained.

Contractual Ground

If the individual is a party to a contract with the organisation or the organisation uses the data where there is the intention to entering into a contract, then this ground can be relied upon.

Special categories of personal data

There are particular grounds for holding sensitive or special category data and safeguards are required.

3. YOU MUST FORM A PLAN OF HOW YOUR ORGANISATION WILL ENSURE COMPLIANCE IS ACHIEVED PRIOR TO THE GDPR COMING INTO FORCE AND MOVING FORWARD TO MANAGE ONGOING COMPLIANCE

Senior management must get involved in relation to the implementation and moving forward.

In the plan allocate key tasks to each month from now until May 2018. Have monthly meetings to ensure that the plan is being implemented and to demonstrate that the organisation is actively seeking to change its regimes in order to ensure compliance by the time the GDPR comes into force.

4. YOU MUST ENSURE POLICIES AND PROCEDURES ARE UP TO DATE

You are expected to put into place comprehensive but proportionate governance measures. You will need to have in place the following policies and procedures to demonstrate compliance:

i. Privacy Notice

A Privacy Notice should be provided at the point data is collected from the individual. It must provide accessible information to individuals about how you will use their personal data and it must contain various required information. Many organisations may already have a Privacy Notice in place but the GDPR requires these to be much more detailed.

Information needs to be in a concise, transparent, intelligible and easily accessible form. Therefore, it may be necessary to have multiple Privacy Notices for different groups of people within your organisation to ensure clarity. In particular, if collecting children's data your privacy notice must be written in language that children can easily understand therefore it may be sensible to have a separate notice for children.

ii. Data Protection Policy

These are internal policies which explain to staff how data is used internally and may require staff to have training on data protection to ensure awareness. ICO has created a Toolkit specifically for charities regarding communicating the importance of data privacy to employees.

iii. Data Breach Response Policy and Procedure

A personal data breach which is likely to result in a risk to people's rights and freedoms must be reported to the ICO within 72 hours of your organisation

becoming aware of the breach. Furthermore, if there is the likelihood of a high risk to people's rights and freedoms, the organisation needs to report the breach to the individuals who have been affected as well.

Therefore, due to the short timeframe to respond to a breach it is necessary to ensure the roles, responsibilities and processes are in place ready for the eventuality of a breach taking place.

iv. Subject Access Request Form and Procedure

A Subject Access Request Form should be produced to make any requests easily recognisable and ensure the individual includes the details needed to locate the information requested.

You only have one month to comply with subject access requests and therefore there needs to be a procedure in place to deal with these swiftly upon receipt.

Information needs to be provided in a structured, commonly used and machine-readable format to comply with the individuals new right to data portability.

v. Records Management Policy

What record keeping you are obliged to carry out is determined on your organisation's size and the processing carried out. If you are required to keep records, see the conditions below, you need to have a policy in place recording how you hold the data.

It would also be good practice to have an IT Security Policy in place. An IT Security Policy will ensure that all those employed or who volunteer at the organisation have an understanding of what is required of them to ensure data is used and accessed securely online. In drafting this policy, particular account should be taken of the particular risks that are presented in your organisation in relation to the accidental or unlawful access to personal data.

5. DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

An assessment must be made when you are using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals. The relevant GDPR requirements must be complied with.

It would be sensible to assess the situations where it will be necessary for your organisation to conduct an assessment now and to consider who needs to be involved.

Where the assessment indicates high risk data processing then you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with GDPR.

6. ENSURE SYSTEMS ARE IN PLACE TO ALLOW NEW RIGHTS OF INDIVIDUALS TO BE SATISFIED

The new rights given to individuals include the following:

- the right to transparent information and communication
- the right to have fair processing notices when data is collected
- the right to be forgotten
- the right to have inaccuracies corrected
- the right to data portability.

You need to demonstrate that you have explored the possibility of putting systems in place and where necessary implement the systems to facilitate it.

7. ENSURE CONTRACTS BETWEEN DATA CONTROLLERS AND DATA PROCESSORS ARE UP TO DATE

A "data controller" is someone who says how and why data is processed and a "data processer" is someone who acts on your organisation's behalf.

A written contract must be in place between the controller and processor which allows both parties to understand their responsibilities and liabilities. The contract needs to be robust and the GDPR sets out minimum requirements in relation to what terms must be included. To name a few the contract must require the processor to assist with providing subject access request, ensure that people processing the data are subject to a duty of confidence and take appropriate measures to ensure security of processing.

Standard clauses may be provided by the European Commission or the ICO in the future, but no clauses are available yet.

8. REVIEW RECORD KEEPING

What record keeping you are obliged to carry out is determined on your organisation's size and the processing carried out.

If your organisation has 250 or more employees and is a controller of data it must record in writing the following:

- **a.** the name and contact details of the controller (where applicable, the joint controller, the controller's representative and the data protection officer;
- **b.** the purposes of the processing;
- **c.** a description of the categories of data subjects and of the categories of personal data;
- **d.** the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- **e.** where applicable, transfers of personal data to a third country or an international organisation;
- **f.** where possible, the envisaged time limits for erasure of the different categories of data; and
- **g.** where possible, a general description of the technical and organisational security.

If your organisation has fewer than 250 persons is does not need to carry out the detailed record keeping above unless the processing it carries out:

- **i.** is likely to result in a risk to the rights and freedoms of data subjects;
- **ii.** is not occasional;
- **iii.** includes special categories of data or personal data relating to criminal convictions and offences.

Careful consideration should also be given to determine whether your organisation could be a data processor as data processors also need to record certain information.

When relying on consent as your basis for processing data you must record this in a way that can be evidenced later.

9. YOU MUST DECIDE WHO WILL TAKE THE LEAD ON DATA PROTECTION WITHIN YOUR ORGANISATION

A Data Protection Officer (DPO) is a new requirement, however, this is only mandatory when:

- You are a public body
- Your core activity is large scale systematic monitoring
- Your core activity is large scale data which includes criminal convictions and sensitive data.

The role of the DPO is to take responsibility for data protection compliance. The DPO must:

- Have the knowledge, support (including adequate resources) and authority to ensure compliance
- Conduct regular and systematic monitoring of individuals on a large scale
- Be sufficiently independent to be able to perform duties properly
- Report to highest level of management within the organisation, for charities the highest level of management will be the trustees.

If you voluntarily give the title of DPO to someone in your organisation they will need to comply with the requirements set out in the GDPR.

Therefore, it is advisable to appoint someone in such a role to ensure that data protection is not overlooked in your organisation. However, to avoid the rigid requirements in the GDPR it is advisable to use a different title, for example "Data Manager".

GUIDANCE FOR CHARITIES – GDPR

Has been written by Mark Lewis of Charities & Education Group member firm Lodders Solicitors. Mark also sits on the Charities & Education committee.

UK200Group 3 Wesley Hall, Queens Road, Aldershot, Hants, GU11 3NP. Tel: 01252 350733
admin@uk200group.co.uk: www.uk200group.co.uk

Version 1 – February 2018