SHEPHERD+ WEDDERBURN

Charity sector quick guide to GDPR
8 top tips



The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. We have prepared a quick guide with 8 top tips to help charity organisations comply with the new rules.

CARRY OUT A DATA AUDIT

You need to understand what personal data you currently hold, why you hold it, where you hold it, if (to whom and why) it is transferred, and how long it is retained for. This can be a significant exercise. It applies to employees, volunteers, donors, service users and anyone else whose personal data you hold.

CONSIDER LEGAL BASES FOR PROCESSING DATA UNDER GDPR

GDPR requires privacy by design and not as an afterthought. Organisations should identify the legal basis for processing personal data before they process that data.

In some cases, you will be able to rely on consent. However, consent can be problematic (and is not recommended in the employment context) as it must be genuinely freely given, and individuals must be able to withdraw consent as easily as they gave it. As such, in most cases you will be relying on another legal basis for processing personal data and the newly named special categories of personal data (which replace 'sensitive personal data').

The legal bases available depend on (i) whether it is personal or special categories of data being processed; and (ii) whether it is employee data or not (as special rules apply in the employment context).

FUNDRAISING COMMUNICATIONS SHOULD BE REVIEWED

Many charities carry out email marketing and are used to relying on 'opt-out' consent. Under GDPR this will no longer be permitted save in limited circumstances. As such, processes will need to be updated and valid 'opt-in' consent obtained. You should get in touch with existing donors to update their consent if necessary, and change future fundraising materials to be GDPR complaint. Start this process early to ensure that fundraising is not adversely affected by the new rules.

SHEPHERD+WEDDERBURN

REVIEW AND IF NECESSARY UPDATE CONTRACTS AND POLICIES

Contracts and policies that deal with gathering and processing personal data will need to be reviewed and potentially updated. This will cover commercial contracts with suppliers/payroll providers etc. These contracts will need to include special provisions to ensure data is adequately protected. This is particularly important if data is being transferred outside the EU (including being hosted on the Cloud).

It will also cover employment and volunteer contracts. In most cases these should be amended to remove reference to consent and instead be transparent about what you do with data (and refer to the privacy notice – see below).

You will also need to ensure that you have suitable internal policies in place for dealing with personal data. The policy should explain the data protection principles and also address individual employees' accountability to comply with the policy when handling employee data, and the fact that a failure to do so may result in disciplinary action. In addition, the policy should contain details of how any personal data breach would be handled.

PREPARE PRIVACY NOTICES

You will need a privacy notice to explain to individuals what you do with their data. The privacy notice must be tailored to the situation and be clear and concise. You may need a different notice/different section dealing with data for different categories of people (employees/job applicants/volunteers/donors/service users etc.). You may also need to issue separate bespoke notices for any new/unforeseen data usage.

Privacy notices should contain details of:

- the legal data protection principles;
- the types of data being collected;
- the purposes / legal bases of processing;
- individual rights in respect of access to the data; and
- how data will be stored and how long data will be held.

CONSIDER HOW LONG YOU NEED TO RETAIN PERSONAL DATA

Consider the appropriate retention period for data. Personal data should not be held for longer than is necessary. For example, certain data will need to be retained in order for you to provide a service, and to employ people. Protecting yourself from litigation risk may justify retaining data for any claim limitation period. Some data has minimum retention periods: for example, for tax and HMRC purposes, certain payroll, data should be retained for seven years. Conversely, information about criminal record checks and spent convictions should also be deleted promptly in most cases.

The benefit of retaining information should be weighed against the potential drawbacks: the more data you hold the more onerous responding to a Subject Access Request will be; there may also be a storage cost; and the more data you have, the higher the chance of a data breach.

You should also consider the logistical issues with retaining (and deleting) data in line with your policy.

BE AWARE OF INDIVIDUALS RIGHTS IN RESPECT OF THEIR DATA

Individuals can submit a data Subject Access Request (SAR) and the scheme will operate in a similar way to the current one. Minor changes are that the £10 fee will no longer apply. However, if the SAR is 'manifestly unfounded or excessive' a reasonable fee can be charged to cover administrative costs, or you could refuse the request altogether. The 40-day response period will be reduced to one month. If there are a number of requests, or if the request is complex, the period can be extended. If a request is made by email then the response should also be electronic, unless otherwise requested by the individual.

Individuals also have the right, in respect of their data, to ask you to 'delete it, freeze it or correct it' in certain circumstances.

SHEPHERD+WEDDERBURN

PREPARE A DATA BREACH REPORTING PLAN

Under GDPR any personal data breach must be reported to the Information Commissioner within 72 hours of the company becoming aware of it. Where individuals affected by the data breach are at high risk of their rights being infringed, for example through identify theft or fraud, those individuals must also be informed of the data breach. A personal data breach is a 'breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.' For example, you could be responsible for an email containing an individual's address being sent to the wrong recipient. 72 hours is a relatively short timeframe, so you should ensure there are response plans in place so that breaches are identified, reviewed and reported in time.

GDPR is introducing substantial fines of up to €20 million (or 4% of a company's global annual turnover, whichever is higher) for non-compliance so it is important to be prepared. To learn more about compliance with GDPR **read our guides**. If you have any queries surrounding GDPR then please get in touch.

Key contacts

Katie Russell
Partner - Employment
T +44 (0)131 473 5266
M +44 (0)787 269 9897
E katie.russell@shepwedd.com

Joanna Boag-Thomson
Partner - Media and Technology
T +44 (0)141 566 8570
M +44 (0)775 387 1607
E joanna.bt@shepwedd.com

Christopher McGill
Partner - Charities
T +44 (0)131 473 5262
M +44 (0)791 206 9063
E christopher.mcgill@shepwedd.com