GDPR: A Quick Reference Guide

Contents

About Eastside Primetimers

Eastside Primetimers is a management consultancy with a difference. Working exclusively on behalf of not-for-profits, we provide professional support for CEOs and Boards who are seeking to transform their organisations to be fit for the future.

We are dedicated to supporting the growth of a strong social sector that has the capacity and resources to play an even greater role in delivering services in our communities. We promote a business-like approach because we believe not-for-profit organisations can achieve greater sustainability and impact by combining their knowledge of the needs of their beneficiaries with business thinking.

We have a unique talent pool of more than 100 consultants who are carefully selected for their commercial know-how and their passion to make a difference. We call them our members because they are committed to supporting the not-for-profit sector either as consultants, interim managers or Board members.

Eastside Primetimers has specialist GDPR consultants who can provide expert help and advice at all stages of the charity's compliance programme. Michael Griffin is the lead GDPR consultant at Eastside Primetimers. He has 15 years' experience in data protection and an in-depth understanding of the charity sector, and is available for a no obligation initial telephone discussion.

This is a summary of Eastside Primetimers' comprehensive Good Data Guide for achieving GDPR compliance. The Guide provides detailed but user-friendly advice on conducting a data audit, drafting a project plan, and how to implement the plan. The Guide contains practical tips and recommendations for each step of the compliance process and has been specifically produced for charities and not-for-profit organisations.

To obtain a copy of the full GDPR Guide or to arrange to speak to Michael Griffin, please contact Eastside Primetimers on 020 7250 8334 or at dawn@ep-uk.org.

What is the GDPR?

The General Data Protection Regulation is a standard for data protection to apply across all 28 (pre-Brexit) members of the EU, and will become legally enforceable on May 25th 2018.

The GDPR is more complex and more robust than the current Data Protection Act 1998, and consists of 11 Chapters with a total of 99 Articles, many with several sub-sections. **Due to its complexity, professional advice is strongly recommended for an understanding of how to interpret and apply it.**

Why is compliance important?

One of the most significant changes under the GDPR will be the potential level of fines the Information Commissioner's Office (ICO) can levy for a data breach. This will be up to €20 million or 4% of an organisation's global turnover, whichever is the greater. As an example, in April 2017 the ICO fined 11 charities a total of £138,000 for a range of data breaches. Under the GDPR penalty guidelines for that same range of data breaches, this could have been as much as £1.8 million. Compliance is as much about mitigation of risk to the organisation as it is about upholding the rights of Data Subjects.

What is a Data Subject?

A Data Subject is any living person whose personal and/or sensitive data is collected, processed, or stored.

Risks to the charity of non-compliance

Supporter (e.g. donor; investor; funder; fundraiser) trust in a charity is vital in maintaining revenues and goodwill. Adverse publicity resulting from a charity being fined and named-and-shamed for a data breach is proven to have a significant negative impact on fundraising. One charity suffered an immediate 20% drop in revenue as a direct result of the bad publicity surrounding their data breach.

It is now generally acknowledged that any funder or investor will review an organisation's data protection procedures and policies as a part of their due-diligence. With greater potential penalties for non-compliance, any funder or investor will need to satisfy themselves that their investment is secure. Any charity which cannot show adequate compliance may risk losing funding.

How to conduct a data audit

The organisation must understand in detail the way it collects, handles, and retains personal data. The following questions need to be addressed:

- Whose data is being collected and retained?
    - e.g. donors; members; employees; volunteers and casual workers
- What data is being collected and retained?
    - e.g. contact details (name, address, telephone, email etc); lifestyle details; health details etc
- How and where is the data being collected?
    - e.g. website; paper forms; verbal; database (e.g. donor lists); purchase
- What are the reasons for collecting and retaining the data ("grounds for processing")?
- How and where is data retained?
- Who has access to the data?
- Why do they need access?
- What 3rd-parties have direct or indirect access?
- Why do they need access?
- Is the data accurate?
- What provision has been made for a Data Subject to review their data (response to Subject Access Request), and to ask for data to be deleted (Right To Be Forgotten)?
- Who is responsible for data protection within the charity?

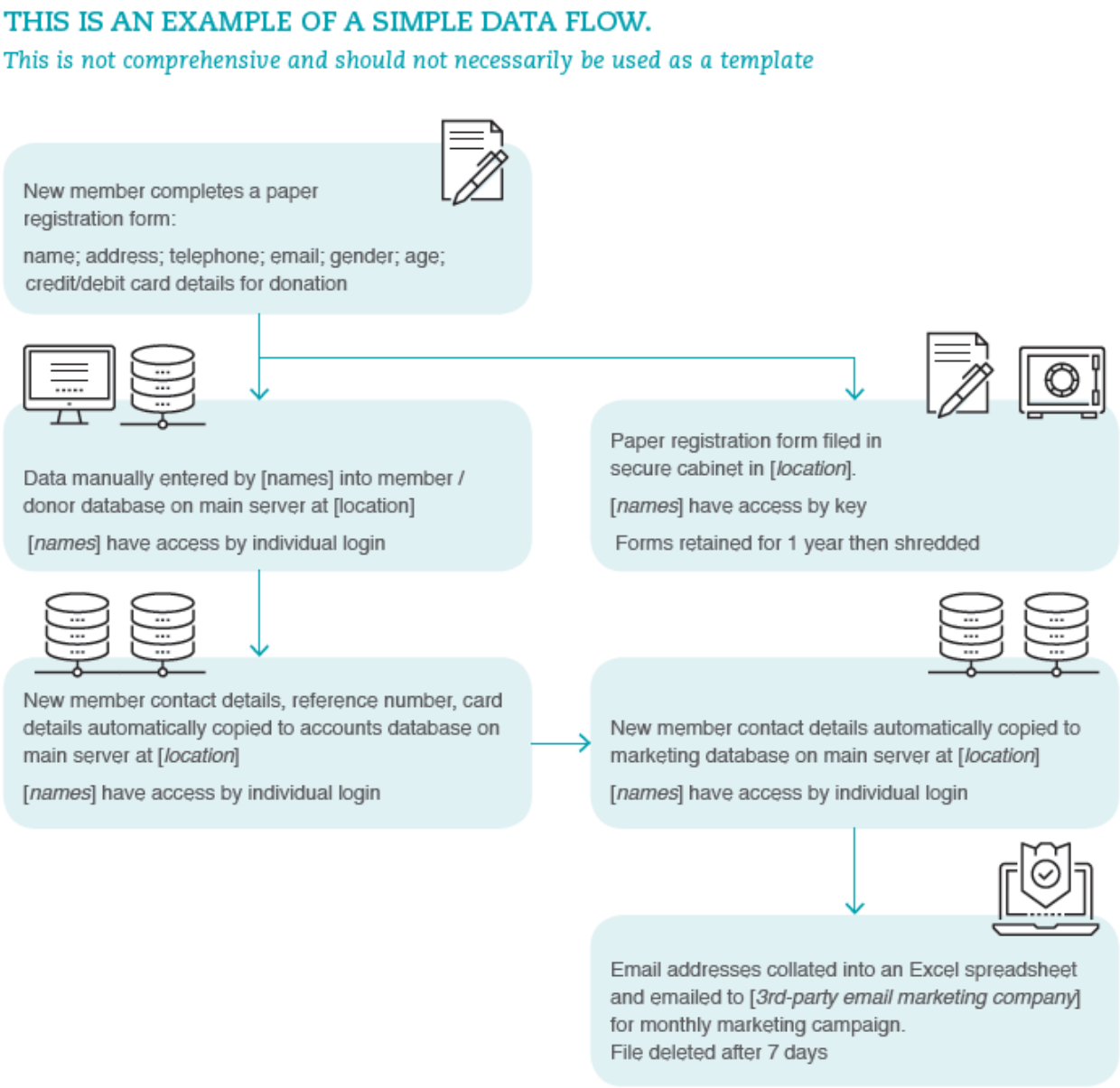
Data Mapping

The most effective method of understanding in detail how data is managed within a charity is to conduct a data mapping exercise (sometimes referred to as a data inventory).

The "flow" of data through the charity's systems and processes should be documented, stage by stage. The data map can take the form of a simple flowchart.

The data map must show the data flow "as is", not "as it should be". This will highlight any areas of weakness or non-compliance which can then be addressed.

Walking through the data lifecycle will identify unforeseen or unintended uses of data, superfluous or incomplete data, unnecessary duplication, and inefficient use of data management resources.



Next steps after the data audit

The data audit and mapping exercise should give the charity a clear understanding of how data is managed within the organisation. It will inevitably highlight areas of weakness which need addressing for compliance with the GDPR.

Addressing the issues arising should be carried out in a controlled and methodical way. It is recommended that the following be considered:

(i) Review the data audit with all key personnel, and obtain consensus on the changes which need to be made
(ii) Designate a priority to each change, ie: HIGH, MEDIUM, or LOW
(iii) Draft a GDPR change project plan showing the tasks, timescales, and task "owner" with the HIGH priority tasks first.

Consent

One of the key changes in the GDPR is the management of consent. The Data Subject "owns" their data and their consent is required for the use of that data.

The charity must now ensure that they explain clearly and simply how they will use personal data, and obtain explicit consent from the Data Subject for that use.

It has been common practice to allow a Data Subject to "opt out" of, for instance, receiving marketing material (e.g. emails and texts). The default being that if the Data Subject had not formally opted out by, say, unticking a box, they had consented to receiving marketing material. Under the GDPR the Data Subject must formally consent by ticking a box or signing that they "opt in". The default being that they have not opted in.

Any consent request in a contract, a written declaration, or similar, must be clearly distinguishable from other matters, and be presented in a clear and intelligible form. In effect, this means no "small-print".

In addition to being explicit, consent must also be informed. The Data Subject must be able to understand clearly what it is they are agreeing to.

Privacy Policy and Data Protection statements

The charity should have a formal privacy policy statement which is clearly presented wherever a Data Subject may be asked to provide any personal data (e.g. website; paper form).

It is recommended that the charity clearly displays a data protection statement on its website.

If you require assistance with your data audit, data mapping exercise, GDPR project plan, Privacy Policy, Data Protection Statements or any other GDPR issue, please contact Eastside Primetimers on 020 7250 8334 for a consultation.