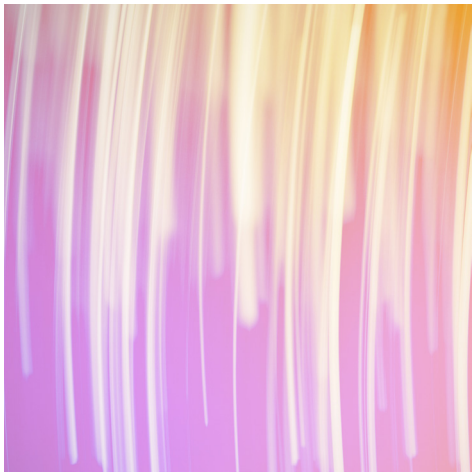
The data security issues facing membership organisations



Membership organisations hold personal data on their systems that must be protected. The General Data Protection Regulation (GDPR) coming into force on 25 May 2018 introduces additional compliance requirements for all organisations, including charities and membership bodies.

Though it may not necessarily be a requirement for all membership organisations to register with the Information Commissioner's Office (ICO) going forward, certain membership organisations employing more than 250 people, those processing "special categories of data" (for example health related information) or those where data processing activities are likely to result in high risk to individuals, will need to maintain detailed documentation about their data processing activities and make these available to the ICO on request.

This article considers the impact of GDPR on membership organisations and provides all you need to know on the upcoming changes.

What data is covered by GDPR?

GDPR relates to the protection of "personal data" by entities that control or process such data. Personal data is any information related to a natural person that can be used to identify them. Membership organisations will typically hold personal data in respect to each of their members including everything from simple contact information through to records of attendance at events, seminars and receipt of publications, etc. The new rules regarding the collection, use and retention of this personal data represents a major change, especially when you consider that the rules will be applied across the board, for example there will no distinction made between a not-for-profit entity and a direct marketing company.

Action required: Carry out an audit to understand what personal data is held, how it is held, for what purpose, how it is accessed and obtained and how it is kept up to date. It is good practice to maintain a list of those in the organisation who should have access to such data.

For some membership bodies it may be mandatory to appoint a Data Protection Officer (DPO). This is particularly relevant for those organisations where their main activities involve processing large volumes of personal data. Ascertain whether this will apply to you. Even if it does not, it is a good idea to designate someone within the charity to have responsibility for data protection.

What are the key requirements of GDPR?

Consent must be obtained to use or process personal data. 'Requests for Silence', pre-ticked boxes or inactivity do not constitute consent. All consent requests must be prominent, non-ambiguous and not form part of general terms and conditions. Crucially, the concept of 'implied consent' will no longer exist.

Action required: Obtain confirmation from members that the organisation can use their data, for example by asking them to tick a box on your website. This can be done when new members join or at the time of renewal for existing members. Ensure procedures are in place for retaining records that evidence consent as you may be required to prove that you have it. You must tell them what you will be using their data for.

The use of data will be more tightly controlled, with new principles introduced by GDPR such as:

- The right to be forgotten, meaning members can request their data to be deleted. This process should be an easy, one-step process; it will no longer be enough just to supress those records.
- Data portability, which gives members the right to transfer their data. Organisations will need to be able to provide the date in a structured and commonly used electronic format such as Microsoft Excel or Word;
- Right of access by the member to the personal data held about them.
- Data must only be used for the purposes for which the member has given consent.

Action required: Put processes in place to manage the personal data held on members to ensure it is only used for the purposes for which consent has been obtained. Data on members can no longer be used for activities such as marketing, unless the organisation has specific consent for this. There should be a system to record and evidence the consent of members. In the absence of consent, the organisation will need to stop the relevant processing activity and delete the data which is considered noncompliant.

Members are entitled to revoke their consent. So make sure you have robust withdrawal procedures in place. Consider privacy notices and ensure they are transparent, providing information about data retention periods and the right to complain to the Information Commissioner's Office.

Written compliance plans are needed to demonstrate that the organisation has appropriate controls and procedures in place to process and keep personal data in compliance with the GDPR. Action required: Review the personal data the organisation holds on members and the measures in place to ensure the data is processed and held securely.

Consider whether data should be encrypted and assess the systems and procedures in place for monitoring data and its usage. Such systems should be tested, reviewed and updated on a regular basis to ensure they are as failsafe as possible.Ensure all staff involved in data handling are aware of their responsibilities by establishing clear policies, encouraging a culture of accountability and introducing regular training and updates.

What are the risks facing membership organisations?

Personal data breaches (a breach of security leading to the accidental or unlawful access to, destruction or misuse of personal data), will have serious consequences for organisations under the GDPR.

If such a breach occurs with the personal membership data the organisation holds, it will need to inform the Information Commissioner's Office without delay (ideally within 72 hours). In addition, it will be required to inform the members affected of the nature of the data breach and recommend what actions they should take to mitigate the negative impact. Where applicable there may be a need to inform the Charity Commission.

This may lead to negative publicity, damage to reputation and loss of members, impacting on the income of your organisation and, in severe cases, its viability.

Data breaches may lead to compensation claims from members and serious non-compliance with the GDPR is punishable by fines of up to 4% of worldwide annual turnover or €20 million, whichever is higher.

Action required: Ensure there is a well thought out and tested data breach response plan. Such a plan should include a detailed policy to be followed in the event of a breach, staff training on what to do in such circumstances and template notifications to assist a speedy reaction.

Where aspects of data processing are outsourced, check that the contractual arrangements in place with the outsourcer are watertight and that there is the ability to audit their processes and procedures and that there are stringent obligations on them to report any data breaches back to the organisation.

It is important that membership organisations start planning for GDPR compliance now so that they can ensure key people and decision makers understand the requirements and the impact GDPR may have on the organisation, its policies and procedures and its training requirements.

How can we help?

Buzzacott's technology specialists can provide a wide range of data compliance and security advice, including data protection compliance reviews; assistance with preparation for the GDPR changes; review of information collection and retention policies; and review of relationship management procedures. For further guidance and advice on the new GDPR tailored to your situation, please speak to your usual Buzzacott contact in the first instance or:

David Fardell, Managing Director, Buzzacott Giving Solutions

T +44 (0)20 7556 1437
E fardelld@buzzacott.co.uk

Debbie Tilson, Senior Manager, Charity

T +44 (0)20 7556 1433
E tilsond@buzzacott.co.uk

Buzzacott LLP
130 Wood Street
London EC2V 6DL
www.buzzacott.co.uk