GDPR

Preparing for the EU General Data Protection Regulation

Introduction

Early in 2016, the new EU General Data Protection Regulation (GDPR) was finalised and approved. EU members have until May 2018 to ensure that they are fully compliant with the new regulation. Regardless of Brexit, organisations in the UK that collect and use personal data will need to comply with the new regulation since there will be an overlap in the timing of the UK leaving the EU and the implementation of the regulation. It is also widely thought that UK data protection requirements will, in any event, match the requirements of EU GDPR post-Brexit.

Much of the new regulation matches the good practice and requirements already set by the Data Protection Act (the Act). However, there are some changes as described below.

Reporting breaches of GDPR and fines

High risk data breaches will have to be reported within 72 hours of occurring. Fines will increase from a maximum of £500,000 under the Act to up to 4% of annual global turnover or €20 million (whichever is greater) with GDPR. Officers and key employees could face civil and criminal liability for breaches of GDPR.

Demonstrating accountability and governance

GDPR places a stronger emphasis on the need for accountability and governance. Organisations will be required to demonstrate accountability and how they comply with the regulation. Appropriate technical and organisational measures must be implemented to ensure and demonstrate compliance. For example, internal data protection policies such as staff training, internal audits of processing activities, and impact assessments.

More detailed records of processing activities must be kept, including the types of people whose personal information is processed, the categories of personal information processed, the processing purpose, who information is shared with, how it is collected, and how it is kept securely.

Consent for processing personal information

GDPR requires that organisations obtain valid and active ("unambiguous") consent of a person in order to process their personal information. This means that implied consent is no longer sufficient and a person has to actually do something actively to provide their consent. Therefore, pre-ticked opt in boxes will no longer be adequate and empty opt-out boxes (which have to be ticked by the person in order to opt out) will no longer be considered good practice (although, under specific circumstances,

will be acceptable). It will also be necessary to be able to demonstrate that "explicit consent" (i.e. an affirmative statement/opt-in given by the data subject) has been given in the case of processing sensitive personal data. Some questions to consider are:

- Did the data subject give their information freely?
- Were they presented with straightforward information so that they had a clear understanding of what marketing/fundraising communications they could expect to receive?
- Did they have a clear and easy ability to choose to accept this, or to object if they didn't want to receive future marketing?

Consent must be given freely. For example, the performance of a contract must not depend upon consent being given when the processing is not actually required to perform the contract.

Parental or guardian consent will be required to process the personal information of children under the age of 16 (or possibly 13).

Data Protection Officer

Article 35 of the GDPR requires organisations that are public bodies or that regularly and systematically monitor data subjects to appoint a data protection officer. The GDPR does not specify credentials necessary for data protection officers, but does require that they have "expert knowledge of data protection law and practices."

The right to be informed

GDPR requires that people have a right to be informed (free of charge) about how their personal information is used. The level of detail provided goes beyond the requirements of the Act. Information provided about processing must be concise, transparent, intelligible, easily accessible and written in clear and plain language.

Users' rights to access, erasure, portability and rectification

GDPR gives people rights in addition to the rights that the Act affords.

- Subject access requests will change slightly with GDPR. In most circumstances requested information must be provided within a month rather than within the 40 days specified by the Act.
- GDPR also gives people the right to request that their personal information is erased. This may mean deleting a person's personal information if asked and if it is no longer actually being processed.

- Organisations must also be able if asked to provide a person's personal information in an electronic format which it can easily be transferred to another system. This is so that they can reuse their information for other purposes with other organisations.

- When notified it must be possible to rectify a person's personal information within a month if it is inaccurate or incomplete. This will include informing other organisations if information has been shared.

Data processors

GDPR puts direct and increased responsibility on data processors. These are the organisations that data controllers share personal information with in order to process it on their behalf. Under GDPR data processors can be held responsible for data breaches. The contracts currently in place with data processors will need to be revised to reflect this and comply with GDPR. Data controllers will still be responsible for ensuring that they have appropriate contracts in place, choose appropriate data processors and that they comply with GDPR.

Privacy by design

Compliance with GDPR must be considered in the design and implementation of all data handling processes, from start to finish. Protecting personal data can no longer be an afterthought.

Risk assessments (Data Protection Impact Assessment) should be undertaken when introducing new technology to process personal information and the processing is likely to result in a high risk to the rights and freedoms of individuals.

Conclusion

Organisations, and the wider NFP sector, should not ignore or underestimate the risks and impacts to reputation, supporter trust and income non-compliance with GDPR can bring – which means planning now for the changes that will need to be in place by May 2018.

Organisations should carry out a compliance review to identify and resolve areas where they are not complying, or at risk of not complying with the Act. They should provide data protection training to staff and volunteers, and develop new data protection policies and procedures which should be rolled out over the coming months.

It is important to understand that the work required generally does not fall within the remit of any one team; this is not an IT, Digital, Fundraising, HR or Database Team project. This is a cross- organisational project which will affect all parts of the organisation. Support from senior management, and resource and input from all teams is needed to implement your GDPR action plan and bring about the necessary changes successfully.

Adapta can help

Adapta are already working with organisations to ensure they are compliant with the new regulations. Speak to one of our specialists to discuss how we can help identity, prepare and implement changes within your own organisation.

Tel: 020 7250 4788 Email: help@adaptaconsulting.co.uk

Our specialist consultants






t: 020 7250 4788 e: help@adaptaconsulting.co.uk @AdaptaforNFP

About Adapta Consulting

We specialise in providing charities, membership organisations and other not-for-profit organisations with tailored advice and practical guidance to develop the three areas key to achieving strategic and operational effectiveness:

processes – through developing business processes and effective ways of working,

people – by offering the support people need to manage change,

technology – to help select and implement new systems or technology.

We are independent and objective and set the highest professional standards to ensure we provide services which are tailored to our clients' needs

For more information about us visit our website www.adaptaconsulting.co.uk