What is the GDPR (General Data Protection Regulation) and why is it so important that associations understand it?

Terrance Barkan CAE, Chief Strategist at GLOBALSTRAT

The General Data Protection Regulation, referred to simply as the "**GDPR",** is Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016. It concerns the protection of natural persons regarding the processing of personal data and on the free movement of this data.

Because associations maintain extensive databases of personal data, this Regulation directly impacts how associations will collect, maintain and manage the data that is vital to their operations.

Note: "Personal Data" and "Personally Identifying Information" or "PII" are not the same thing and are often confused. Personal data is defined below.

What is equally important, this Regulation applies to any organization, regardless of where it may be located or headquartered, that maintains data of an EU resident. This casts a very wide net and touches essential any international organization.

What is the GDPR?

The GDPR came into force on 24 May 2016. However, due to its two-year implementation period, the GDPR will only be applicable from 25 May 2018. At this point, organizations have less than 10 months to ensure they are able to comply.

Because the GDPR is an EU wide regulation, it does not require Member States to pass additional legislation for implementation. Some EU Member States (such as Germany, Ireland and the UK) are however taking the opportunity to introduce new domestic law at the same time.

The GDPR covers the processing of 'personal data' that relates to 'data subjects' by or on behalf of a 'data controller'.

'Personal data' is defined as any information that relates to an identified or identifiable natural person (the 'data subject'). An identifiable natural person is anyone that can be identified, either directly or indirectly, by reference to anything that can ultimately identify them. This includes a name, an identification number,

location data, an online identifier or to data that relates to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Based on this broad description, it is clear that much of the types of data that associations hold on their members, prospects, former members, sponsors, donors, meeting participants etc. would be considered as 'personal data'.

The entity who determines the purposes and means of processing is the 'data controller'. This is contrasted with a 'data processor' which processes personal data on behalf of the data controller.

There are many changes for data processors under the GDPR, with many of the contractual obligations on them having been placed on a statutory footing. In practice the distinction between a data controller and a data processor is often not easy to ascertain.

What is the difference between a Data Controller and a Data Processor?

One way of looking at this is in the example of an Association that outsources its IT services to a third party (think of an online database management application). This is not an unusual situation, especially for many associations that outsource the hosting of their websites that may have an online membership directory as just one example.

The Association in this case would be considered the 'data controller' because the association maintains 'control' over the data (it is collected, maintained and manipulated at the direction of the association'). The third party service provider(s) would be considered a 'data processor' because they have access to the data through the provision of their IT services.

What are my responsibilities?

The 'data controller' bears the responsibility to prove to the relevant 'supervisory authority' that it is properly following the guidelines and regulations regarding the acquisition and management of personal data.

These Regulations include the following principles regarding the handling of personal data:

- **Lawfulness, fairness and transparency:** Personal data must be processed lawfully, fairly and in a transparent manner.

- **Purpose limitation:** Personal data must be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Data minimisation:** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date. Personal data that is known to be inaccurate is to be erased or rectified without delay.

- **Storage limitation:** Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary.

- **Integrity and confidentiality:** Personal data must be processed in an appropriately secure manner including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

  NOTE: This is where associations must have confidence that the third party services they use to manage data are properly secured. If your third party provider causes a breach, the association will remain liable.

- **Accountability:** The data controller is responsible for, and has to be able to demonstrate compliance with, the principles stated above.

Regulation and enforcement of the GDPR is performed by a country's 'supervisory authority' which in some countries may include data regulators at a national as well as a regional or local level.

In addition to the principles listed above, data controllers (associations) must also meet at least one the following criteria;

- **Obtain consent:** The data subject must give clear consent to the processing of his or her personal data for one or more specific purposes.

- **Performance of a contract:** Data processing is necessary for the performance of a contract with or on behalf of the data subject. For associations, membership and the delivery of services can be considered a contract. "Necessary" is a key element here however. Regulators and the courts are likely to interpret this narrowly and convenience is not the same as a necessity!

- **Compliance with a legal obligation:** Data processing is necessary for compliance with a legal obligation to which the data controller is subject. Again, this is a narrow criteria and a US legal obligation is unlikely to be sufficient.

- **Vital interests:** Data processing is necessary in order to protect the vital interests of the data subject or of another natural person.

- **Public interest:** Data processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. To meet this requirement it is likely to be in the interest of the public in the relevant Member State – US public interest will not be sufficient.

- **Legitimate interests:** processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The importance of 'Consent'

Obtaining proper consent from your data subjects is one of the most important aspects of compliance with this new Regulation. The definition of what constitutes proper consent has changed under the GDPR.

Consent in the GDPR is defined as: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes'.

Specifically, consent needs to be given by a clear affirmative act, 'such as by a written statement, including electronic means, or an oral statement' which demonstrates a data subject's agreement to the processing of personal data relating to him or her.

It is important to note that '**silence, pre-ticked boxes or inactivity**' do not establish consent.

Many associations may assume that they already have consent because of an existing relationship with their membership. While this may be true in some cases, it will depend on how the consent was originally obtained.

The data subject does not need to give his or her consent again if the original consent was obtained in line with the conditions detailed in the GDPR. This means

that many associations will have to consider obtaining consent that meets the GDPR requirements, even from existing members.

It should also be noted that associations will need to give members and other data subjects the ability to withdraw consent in a manner that is as easy to withdraw as it is to give consent.

What are the penalties for non-compliance?

Each supervisory authority has a range of investigative, corrective, authorisation and advisory powers in order to ensure compliance with the GDPR. A supervisory authority has the ability to:

- Issue warnings.
- Order the data controller or the data processor to comply with a data subject's requests to exercise his or her rights under the GDPR.
- Order the data controller to communicate a personal data breach to the data subject(s).
- Impose a temporary or definitive limitation including a ban on processing.
- Order the correction or erasure of personal data or restriction of processing pursuant to a data subject's rights.
- Impose an administrative fine.
- Order the suspension of data flows to a recipient in a third country or to an international organisation.

In addition, fines can be imposed, 'in addition to, or instead of' the corrective powers a supervisory authority has at its disposal. The potential levels of these fines is quite staggering.

- a fine of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- a fine of up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year for the most severe forms of a breach, including violations of;

- the basic principles for processing, including conditions for consent
- the data subjects' rights
- the transfers of personal data to a recipient in a third country or an international organisation, or
- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

What Next?

This article is meant to give a very brief overview of some of the most important elements of the GDPR. There are many more details to b considered regarding the rights of data subjects and how data controllers (associations) must act when acquiring, storing, managing and deleting personal data.

Associations will need to get proper legal compliance advice when it comes to the GDPR implementation. Because associations collect and manage data through multiple platforms (database management systems, websites, event registrations systems, members only networks, etc.) the range of exposure can be higher than imagined.

***

Acknowledgement: I want to thank Cordery , London, UK for the permission to reference some of their source material as an inspiration for this article.

***

For more information on the GDPR and Data Protection Information services, visit:

http://www.globalstrat.org/eu-data-protection-services/