MY Schools Together - General Data Protection Regulation (GDPR)

1. Introduction

In the UK, GDPR will apply from May 25th 2018. It will replace the UK Data Protection Act 1998.

The General Data Protection Regulation (GDPR) will apply to all organisations worldwide that process personal data of European Union (EU) citizens, effectively making it the first global data protection law. Its introduction is based on the fact that many businesses and services operate across borders, making international consistency around data protection laws and rights crucial both to organisations and individual alike. The growing digital economy also makes it important for safeguards to be in place regarding data, and the individuals to whom it applies.

My Schools Together falls under the description above, we will be under a legal obligation to comply with GDPR. The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the key areas will require your organisation to review its approach to governance and how it manages data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Every country in Europe will have a regulatory body to oversee the use of, provide advice on, and enforce the GDPR. In the UK this body is the Information Commissioner's Office (ICO).

2. Who does the GDPR apply to?

The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the DPA i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

3. What information does the GDPR apply to?

3.1 Personal Data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier e.g. an IP address can constitute personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised e.g. key-coded can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.2 Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes.

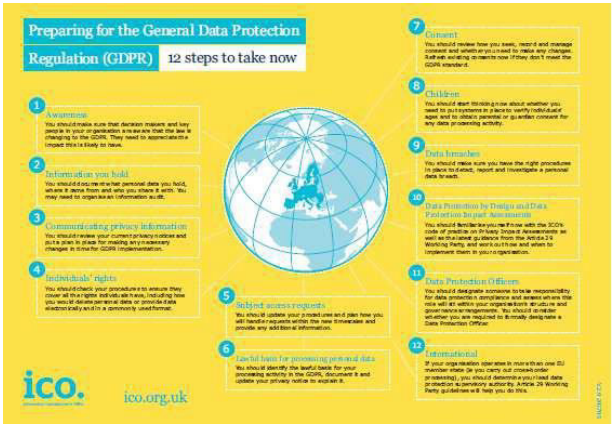
For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

4. Preparations for the GPDR - 12 steps for organisations

ICO have produced guidance for organisations to prepare for the GDPR. *Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.*

The document can be accessed at: [ICO preparing for the GDPR 12-steps.pdf]



5. Actions

My Schools Together conducted an internal assessment of the organisation to ensure the organisation is prepared for the GDPR using the 12 steps preparation method during February and March 2018. The actions that have been completed are outlined in the table below.

Step 1	**Awareness**	The decision makers and key people in My Schools Together are aware that the law is changing to the GDPR.

Step 2	**Information you hold**	My Schools Together have documented what personal data we hold, where it came from and who we share it with. We have produced an Information Audit which records our processing activities.

Step 3	**Communicating privacy information**	My Schools Together have updated the privacy notice to ensure the notice includes the requirements of the GDPR. My Schools Together have reviewed our current privacy notices and it has been updated, it provides concise, easy to understand and clear language and includes the following information: ▪ Who we are; ▪ What personal data we record ▪ The purpose for collecting and processing the data ▪ What we are going to do with the information ▪ Who it will be shared with ▪ What we do to ensure the security of personal information ▪ Information about their rights of access to their data ▪ Our data retention periods ▪ The right to complain to the ICO if they think there is a problem with the way we are handling their data We have added a privacy statement to the attendance registers that we use at the sessions we deliver. Staff and volunteers have been made aware of the updated notice and the statement added to the attendance registers and is able to discuss the privacy notice and the statement with the participants that attend the sessions we deliver.

Step 4	**Individuals' rights**	We have updated our Data Protection Policy and Procedures to ensure they cover all the rights individuals have, including how we would delete personal data and provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals: ▪ The right to be informed; ▪ The right of access; ▪ The right to rectification; ▪ The right to erasure; ▪ The right to restrict processing; ▪ The right to data portability; ▪ The right to object; and ▪ The right not to be subject to automated decision-making including profiling.

Step 5	**Subject access requests**	We have a Subject Access Procedure which states how we will handle requests based on the GDPR new rules: ▪ In most cases we will not be able to charge for complying with a request. ▪ We will comply within a month; ▪ We can refuse or charge for requests that are manifestly unfounded or excessive. ▪ If we refuse a request, we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We will do this without undue delay and at the latest, within one month.
Step 6	**Lawful basis for processing personal data**	We have identified the lawful basis for our processing activity in the GDPR, documented it and updated our privacy notice to explain it. We have trained our staff and they are able to discuss processing personal data and the privacy notice with service users.
Step 7	**Consent**	We have reviewed how we seek, record and manage consent to process their data. It ensures it meets the GDPR standards: ▪ Consent must be freely given, specific, informed and unambiguous. ▪ There is a positive opt-in; consent cannot be inferred from silence, pre-ticked boxes or inactivity. ▪ It is separate from other terms and conditions ▪ It has simple ways for people to withdraw consent.
Step 8	**Children**	We have systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. We do NOT offer online services ('information society services') to children.
Step 9	**Data breaches**	We have the right procedures in place to detect, report and investigate a personal data breach which includes the GDPR duty on all organisations to report certain types of data breach to the ICO*, and in some cases, to individuals. * *We will notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.*
Step 10	**Data Protection by Design and Data Protection Impact Assessment**	We have completed a DPIA (Data Protection Impact Assessment) to identify the situations where data processing is likely to result in high risk to individuals, for example: where a new technology is being deployed; where a profiling operation is likely to significantly affect individuals; or where there is processing on a large scale of the special categories of data.
Step 11	**Data Protection Officer**	Under the GDPR we are not required to formally designate a Data Protection Officer (DPO). However we have **informally** designated someone to take responsibility for data protection compliance and assess where this role will sit within our organisation's structure and governance arrangements.
Step 12	**International**	Our organisation does NOT operate in more than one EU member state. Therefore no actions have been completed for this step.