Tudhoe Learning Trust

Data Protection Briefing Paper

General Data Protection Regulation - GDPR

The way organisations handle personal data is changing. On May 25th this year The Data Protection Act 1998 (DPA) will be superseded by The General Data Protection Regulations 2018 (GDPR). The requirements of the DPA will remain but there will be some significant changes introduced by the new regulation:

- **Data protection by design not default**. This means that we must consider data processing activity in all we do and demonstrate it.

- **Consent**. We are no longer able to rely on opt-out waiver clauses as a method of obtaining consent. Consent must be given freely, in clear plain English and must be specific. Data subjects must be clear about their right to withdraw.

- **Data breaches**. Robust systems, practice and whole organisational culture must exist to prevent this from happening but where it does happen this must be reported to the Data Protection Lead Officer and then subsequently to the Information Commissioners Office. Substantial fines may be imposed where a data breach occurs.

- **Data Protection Lead Officer**. Organisations must demonstrate that they take data security seriously. A Data Protection Lead Officer must be appointed with Board reporting capacity to oversee compliance within the organisation. Compliance / auditing can be shared with other organisations or even outsourced but there must to someone within the organisation with this accountability.

- **Impact Assessments**. This means that whenever we change something or introduce a new system or process we must complete and document a Data Impact Assessment to show that we have considered the impact the change will have on data security and given forethought to any anticipated issues.

- **Data Audit**. We must audit our data storage, systems and processes now and make a plan to address any identified issues and then follow an auditing process at least annually but more frequently if required and document it to show that we are safely and compliantly processing and handling data in line with our GDPR obligations. We need to map our data and work flow.

- **Policy**. We must review our policies to ensure that they are up to date and are aligned with our GDPR obligations. Obvious policies will be Data Protection, Freedom of Information, Subject Access Requests, Safeguarding & Child Protection, Admissions, Accessibility, Recruitment & Selection, Grievance & Disciplinary, Code of Conduct and Finance related codes and procedures.

- **Contractors / Suppliers & Third Party Providers**. We must review all of our contracts and service providers and ensure that our contracts with them are compliant and satisfy ourselves that while transacting on our behalf they will be doing so appropriately. Obvious contracts will be IT, Payroll, EP, SSP, any SLAs, Legal etc.

GDPR Key Principles

Controllers and processors

The GDPR applies to both controllers and processors of data, as defined under the Data Protection Act. Controllers say how and why personal data is processed, and the processor acts on the controller's behalf to process the data.

There are specific legal obligations on both controllers and processors:

- controllers must specifically ensure that contracts with processors comply with the GDPR; and
- processors are required to maintain records of personal data and processing activities;
- processors are also legally responsible and liable for any security breaches.

Scope of the GDPR - data protection principles

The GDPR has a number of principles relating to personal data. Whilst these are not dissimilar to those under the UK Data Protection Act, there are some differences, together with a new accountability requirement. Personal data shall be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose
- accurate and kept up to date. Inaccurate data should be erased or corrected
- kept in an identifiable format for no longer than is necessary
- processed securely and protected from unauthorised or unlawful processing, accidental loss, or destruction or damage.

Finally, the GDPR requires that the controller shall be responsible for, and be able to demonstrate, compliance with these principles.

GDPR rights for Individuals:

The right to be informed

Individuals have the right to know how their personal data is going to be processed. The GDPR promotes transparency over processing by way of a privacy notice encompassing (amongst other things) details of the controller, the source of the data, recipients of the data, data transfers made outside the EU, and the retention period of the data.

The right of access (subject access request)

Individuals have the right to obtain confirmation that their data is being processed, access to their personal data, and other information, such as that provided in a privacy notice.

The maximum amount of time allowed to deal with a subject access request has been reduced from 40 to 30 days under the GDPR, and the right to charge a subject access fee has been removed, unless the request is unfounded, excessive or repetitive.

The right to rectification

Individuals have the right to have inaccurate or incomplete personal data rectified. This must also include personal data which is shared or given to third parties.

The right to erasure

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Again, this must also include personal data which is shared or given to third parties.

Note that there are extra requirements when the request relates to a child.

There are some exceptions to the right to erasure, such as where data is held to comply with a legal obligation.

The right to restrict processing

Individuals have the right to restrict the processing of personal data. In these circumstances the personal data can be stored but not processed.

The right to data portability

Individuals have the right to obtain and reuse their personal data across different services. It allows them to move, copy or transfer personal data. Personal data must be provided in a structured machine-readable format (such as.csv).

The right to object

Individuals have the right to object to the processing of personal data. Processing must stop immediately unless there are 'compelling' legitimate grounds for the processing, or if processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

Individuals have the right to ensure that safeguards are in place to protect against the risk of damaging decisions being taken without human intervention. This also extends to the safeguarding of personal data used for profiling purposes.

Accountability and governance

The GDPR contains the principle of accountability, which requires that appropriate governance measures are in place. We therefore need to:

- implement measures that meet the principles of data protection
- document policies and procedures in relation to the storage and processing of personal data
- implement technical and organisational measures to ensure and demonstrate compliance
- appoint a Data Protection Lead Officer
- certain types of organisations, such as public authorities, must appoint a data protection officer
- organisations which perform particular types of processing (large scale monitoring of individuals, or large scale processing of special categories of data, or data relating to criminal convictions and offences) must also appoint a data protection officer.

Conditions for consent

The new law places particular emphasis on the issue of consent, stating that an indication of consent must be specific, unambiguous and freely given. Positive consent cannot be assumed from inaction, such as failing to click an online 'unsubscribe' box, or from the use of pre-ticked boxes. Schools also need to make sure that they capture the date, time, method and the actual wording used to gain consent, so it is important to ensure that your business has the means to record and document such information.

Notification of breaches

Breaches must be notified to the relevant supervisory authority where '*it is likely to result in a risk to the rights and freedoms of individuals*'.

A notifiable breach must be reported within 72 hours.

Transfer of data

The GDPR places restrictions on the transfer of data outside of the EU.

Sources and links

- ICO home page for organisations
- ICO GDPR micro site self assessment toolkit 12 preparatory steps
- EU GDPR portal - http://www.eugdpr.org/
- Education www.ico.org/for-organisations/education/