APRIL 2024 • VOL. 3

1 MINUTE GUIDE

Safeguarding Committee

GDPR, data protection and sharing of information

The UK **GDPR** is a set of guidelines for the collection and processing of personal information of individuals within the UK, and sits alongside the **Data Protection Act** (DPA) 2018, replacing the DPA 1998.

The GDPR is an acronym for the General Data Protection Regulation and is a piece of European legislation that **protects personal information** (This has been revised as the UK GDPR since Brexit). It outlines several requirements businesses must follow to process that data legally. Although passed in the EU, it affects businesses worldwide and introduced the concept of Privacy by Design (PbD). This privacy approach involves keeping data collection to a minimum and building security measures from the inception of the processing activity to prevent data leaks and breaches at all stages of the processing of personal information.

WHY DO WE NEED THE GDPR?

We need laws like the GDPR because people have the right to know about and have some control over what information gets collected about them and how it's further used, or who it gets shared with. That includes you, me, and anyone else using the Internet. Personal data is highly valuable — it supports a trillion-dollar industry.

Nowadays, numerous companies make a portion of their profits by selling personal information to advertisers. Regulations like the GDPR create a privacy framework for companies of all sizes by creating rules about what they can and can't do with your personal information. Knowing how this key piece of legislation works and what your potential rights are helps you maintain more control over your life both online and offline.

The GDPR follows seven principles of data protection:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (aka, security)
- Accountability

It went into effect on 25th May 2018, and set new standards for data privacy and security, kickstarting a wave of global privacy laws that forever changed how consumers and businesses alike use the Internet.

YOUR RIGHTS

The UK GDPR has created new rights for individuals and strengthens some that existed under the DPA. These are as follows:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights to automated decision-making and profiling

Data subject – the individual who is the subject of the personal data.
Data controller – a person or organisation who determines the purposes and ways that data is processed.
Data processor – any person who processes data on behalf of the data controller.
Data protection officer (DPO) – the person(s) responsible (where applicable) for ensuring the company is compliant with data protection legislation.
Personal data – information that can identify an individual, such as an address.
Sensitive data – information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.

PUPILS DATA AND SAFE STORAGE

The UK GDPR has provisions that are intended to enhance the protection of children's data. Schools should have child-friendly privacy notices which are written in an age/developmentally appropriate way, to explain the ways in which the school processes and uses their data.

The UK GDPR states that personal data must be subject to the appropriate technical and organisational measures required to protect it against unlawful processing, and against accidental loss, destruction or damage. This could include a locked filing cabinet for paper files and encrypted, password protected files for digital data.

Under the UK GDPR, schools are expected to have comprehensive and proportionate governance measures in place to minimise the risk of data breaches. Schools should:

- Implement internal data protection policies, e.g. staff training or reviews of internal HR policies.
- Maintain relevant documentation and processing activities.
- Appoint an appropriate DPO (where needed).
- Implement measures that meet the principles of data protection by de-fault, including data minimisation and transparency.
- Use data protection impact assessments where appropriate.

7 GOLDEN RULES TO SHARING INFORMATION

According to the government's report, these are the seven golden rules:

- GDPR is not a barrier to justified information sharing, but provides a framework to ensure that personal information about living individuals is shared appropriately.
- Be open and honest with individuals about why, what and how information will be shared - unless it is unsafe or inappropriate to do so.
- Remember to seek advice from other practitioners if you have any doubt about sharing the information concerned (without disclosing identities if possible).
- Information should be shared with consent and respect should be shown to those who do not wish for their data to be shared. However, under GDPR information can be shared without consent in incidents where safety may be at risk.
- Always consider safety of the individuals and other people affected by sharing information.
- Ensure the information being shared is necessary for the reason it is provided and only shared with the individuals that need to have it.
- Remember to keep a record of sharing decisions, including to who and for what purpose.

HEALTH AND WELLBEING SUPPORT

"Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps young people safe." UK Government.

Schools and colleges have developed robust policies around sharing attainment information relating to a child or young person with their new setting, however due to concerns regarding GDPR, there is often confusion or uncertainty around sharing safeguarding, SEN and behaviour records.

When a child or young person moves from one educational or care setting to another, it is essential that the safeguarding file, behaviour records, SEN information (including plans), attainment information, attendance information, medical records (including plans) and any additional information or records of support are shared with the new setting prior to the child/young person joining them. It is important to ensure that no information is lost and to ensure that the new setting has a complete picture of the child/young person, including any risks associated. These risks must include any vulnerabilities, for example risk of exploitation and/or radicalisation.

Safeguarding should always take priority over GDPR. If there is a concern about sharing information on a safeguarding matter, you don't need the individual's consent to share the information in most circumstances.

These circumstances are detailed in the Data Protection Act 2018, which was updated in the UK to meet the GDPR Directive. It states:

"Fears about sharing information cannot be allowed to stand in the way of the need to promote welfare and protect the safety of children.

GDPR does not require you to delete safeguarding information from your records".

GDPR: WHAT IS IT AND HOW MIGHT IT AFFECT YOU? YOUTUBE

DATA PROTECTION ACT 2018

UK GENERAL DATA PROTECTION REGULATION

ADVICE FOR PRACTITIONERS PROVIDING SAFEGUARDING SERVICES TO CHILDREN, YOUNG PEOPLE, PARENTS AND CARERS