BRIEFING

Winckworth Sherwood

GDPR: An Introduction for Schools and Academy Trusts

Introduction

The law relating to data protection is going to change on 25 May 2018. Although this may seem like a long time away, schools and academy trusts will need to start preparing now to ensure that they are compliant with the new legislation. This briefing note provides a brief introduction to the key changes that you need to be aware of. For the purposes of this note, references to "trusts" means both single and multi-academy trusts. In the case of multi-academy trusts, it is important to remember that personal data will be processed by the academies within the trust and by your central team who will also need to ensure they comply with the requirements of the new legislation.

What is the change to the law?

At the moment, the Data Protection Act 1998 ("DPA 1998") applies to the way in which schools and trusts handle personal data. Most schools and trusts will be familiar with the general requirements of the DPA 1998, for example, the circumstances when they can disclose personal data and what to do if a person submits a subject access request.

From May 2018, the DPA 1998 will be replaced by the General Data Protection Regulation which is often referred to as the "GDPR". Although many of the principles will remain the same as the DPA 1998, there will be some important changes which will affect schools and trusts.

Why is the law being changed?

Since the DPA 1998 became law, there have been a lot of changes to information technology and the way in which individuals and organisations share information. In addition, different member states of the European Union took different approaches to implementing the law relating to data protection which has made it difficult for many businesses to ensure that they are compliant with these different requirements. The GDPR is intended to harmonise the law and make it easier to comply with across Europe.

Will Brexit mean that we don't have to comply with the GDPR?

To ensure that there is sufficient protection for businesses to continue to share data across Europe, it is likely that the GDPR will still be implemented in the UK.

Why do we need to know about this?

Schools/trusts have to comply with the DPA 1998 at the moment and the GDPR will also apply to the education sector when it comes into force. Schools/trusts process a lot of personal data relating to pupils and staff in order to carry out their functions. They also acquire personal data relating to other people including, for example, parents / carers, governors, trustees, members of the local community, suppliers, contractors and consultants.

It is important that schools/trusts ensure that they handle personal data correctly as the Information Commissioner's Office ("ICO"), can issue fines to

organisations who breach the DPA 1998 (and, in fact, the maximum fine will increase when the GDPR comes into force to €20 million or 4% of the business's total worldwide annual turnover, whichever is higher).

There are also reputational risks to your organisation if you fail to handle and process personal data correctly.

What are the key changes that we need to know about?

In general terms, the GDPR places more emphasis on transparency, accountability and record keeping. Therefore, schools/trusts will need to review their current procedures to ensure that they meet the higher standards set out in the GDPR.

Given that some of the guidance on the GDPR is still being drafted, there may be some further information and detail which is published by the ICO in the coming months which could have a bearing on schools/trusts and the steps they need to take to comply with the law. However, we have highlighted below the key points that are likely to be relevant to our clients:

- You will no longer able to charge £10 before you respond to a subject access request (in practice, we know that many schools/trusts use their judgement before requesting the £10 fee in any event).

  You will be able to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive but this is likely to be a high threshold to meet. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

  The fee must be based on the administrative cost of providing the information.

- There will be less time to comply with a subject access request. At present, you must comply with a request without delay and, in any event, within 40 calendar days.

  When the GDPR comes into force, information must be provided without delay and at the latest within one month of receipt of the request. You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary. Again, this is likely to be a high threshold to satisfy.

- There will be a new accountability requirement which means that you will have to show how you comply with the GDPR principles – compliance alone is not enough. You will be expected to implement "…comprehensive but proportionate governance measures" to meet this accountability requirement.
- The principle of 'data protection by design and default' which is a feature of the GDPR means that you will have to implement technical and organisational measures to show that you have integrated data protection into your processing activities.
- As schools/trusts process sensitive personal data you must maintain additional internal records of your processing activities, namely:
  a. name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer);
  b. purposes of the processing;
  c. description of the categories of individuals and categories of personal data;
  d. categories of recipients of personal data;
  e. details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
  f. retention schedules;
  g. description of technical and organisational security measures.

- Under the GDPR, you will need to identify a legal basis which allows you to lawfully process personal data. For a number of functions carried out by schools/trusts, the processing of personal data is likely to be

covered by one of the following non-exhaustive grounds:

a. it's necessary for the performance of a contract;
b. it's necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and / or
c. it's necessary for compliance with a legal obligation.

However, the above grounds will not always be relevant, for example, if you wish to use personal data held about parents for marketing purposes.

Therefore, it is likely that there will be circumstances when you will need to rely on consent as the legal basis for processing personal data. Under the GDPR, the standard of consent will change. In summary, it must be:

a. clear and affirmative which means that you will not be able to rely on implied consent;
b. verifiable (i.e. you must have a record of how and when consent was given);
c. freely given, specific, informed and unambiguous.

As part of the review of your systems which you should undertake before the GDPR comes into force, you should check if any consent you currently rely on meets these higher standards[1].

There are additional requirements in order to process sensitive personal data[2] which we will not cover for the purposes of this briefing note.

- Many schools/trusts already have a privacy notice in place as a matter of good practice. However, the privacy notice will become an even more important tool to demonstrate transparency over how you use personal data and it will need to contain more information to let data subjects know how you use their personal data. The ICO have produced a checklist for privacy notices which is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/your-privacy-notice-checklist/

- It is likely that schools/trusts will have to appoint a Data Protection Officer who must have the ability to report to the governing body / board of trustees.
- There will be an obligation to notify the relevant supervisory body of 'notifiable breaches' within 72 hours otherwise you could incur a significant fine. A breach must be notified where it is likely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.
- A data subject will have the right to be forgotten in certain circumstances (the 'right of erasure'), amongst other rights.
- Schools / trusts will need to review their contracts with data processors (e.g. HR and payroll providers and other third parties who process personal data on your behalf) to ensure that they contain certain clauses that are mandatory under the GDPR.

Will we need to review our Data Protection policy?

Yes. As part of your preparations for the GDPR, you should review your existing policies and procedures and ensure that they reflect your obligations under the GDPR. As mentioned above, your privacy notice will also need to be much more comprehensive. Please contact our School Support Team if you would like us to review your policy for you.

What steps does our school/trust need to take to ensure that we are compliant with the GRPR when it comes into force?

The ICO has produced a document which sets out 12 steps that an organisation can take in order to prepare for the GDPR. The document is available via this link: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

[1] At the time of writing, the ICO has undertaken a consultation on its draft guidance on consent but the final version has not been issued yet. You should therefore refer to the guidance when it is published to ensure that you follow the precise requirements relating to consent.

[2] Sensitive personal data consists of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The key messages behind the document are to review your current processes and procedures regarding data protection and identify any weaknesses so that you have time to iron them out before the GDPR comes into force. This process will also help you to identify what measures you need to put in place, bearing in mind the higher standards that will apply to record keeping under the GDPR and the need to demonstrate compliance under the new accountability requirement. A data audit is a good place to start.

We recommend that you implement an action plan so that you can take appropriate steps to ensure that you are compliant before the law changes in May 2018. Raising awareness within your organisation about the GDPR is an important place to start. You should consider giving someone within your organisation responsibility to take the lead in terms of implementing the GDPR in your school or trust (with support from others!). This person can then report to your governors / trustees so that they are aware of the measures being taken to prepare for the new legislation.

For further information and advice on how we can support you with the GDPR, please contact us:

T: 0345 070 7437

E: schoolsupport@wslaw.co.uk