GDPR, Schools and Contracts – Guidance Notes

Introduction

New data protection legislation, the General Data Protection Regulation ("GDPR") comes into effect on 25 May 2018. This will be supplemented by a new UK Data Protection Act. Among the changes made by GDPR is a requirement to have more detailed contracts where one organisation processes personal data on behalf of another.

As the date on which GDPR comes into full effect comes closer, organisations are trying to upgrade their contracts with the people they either share data with or who process data on their behalf. GDPR has stricter requirements for these contracts and almost all existing arrangements will need to be updated to some extent. Schools are starting to see requests from local authorities and other public sector bodies.

This guide focuses on the National Schools and Colleges Contract (version 2.5) but many of the principles will be applicable to other contractual arrangements.

Terminology

The key distinction to bear in mind is between the "data controller" and the "data processor". The data controller is the organisation which determines the reasons for which data will be processed and the manner in which this will be done. The data processor is a third party which processes data on behalf of a data controller, for example when providing outsourced services.

Personal data is information about a living individual. Schools will hold significant amounts of personal data about a variety of data subjects. The data subject is the individual person about whom personal data is held. The key focus is likely to be on data about learners but it is important to remember that schools will also hold personal data about parents, employees and non-employed staff, and contacts at the local authority such as social workers.

Data Transfers in a School Context

Typically, when looking at the relationship between a school and a local authority, the data sharing relationship is more co-operative than in a standard controller-processor relationship. The care and needs of the learner are critical, and this involves sharing a wide range of information both about the learner themselves and those individuals, such as school personnel, who they come into contact with. It may also involve data sharing among a wider group of organisations than simply the local authority and the school, for example involving health services and the Education Funding Authority.

The ICO's guidance, in particular a report issued in 2012, is consistently clear that schools are data controllers, and that transfers to local authorities constitute data sharing between two data controllers rather than a processing relationship from a controller to a processor. Although the existing guidance reflects the DPA position and has not yet been updated for GDPR, the definitions of controller and processor have not changed and GDPR is unlikely to affect this position.

Some practical examples of controller to controller data sharing in this context which may be of use include:

- Information about pupils. Although the local authority clearly has a close interest in the pupils it places with a school, the school needs to use a significant amount of data for the purposes of the day to day running of the school and will do so as data controller. The National Schools and Colleges Contract confirms that a number of responsibilities lie with the school and the school will need to use personal data to perform these. In addition to day to day activities, the school is responsible for dealing with disciplinary issues, exclusions and complaints and although there will be some data sharing and co-

operation, this is a process which the school will run for its purposes rather than because it has been instructed to do so by the local authority.

- Information about the school's personnel. The school will be the data controller in respect of this information when using it for HR related matters, such as recruitment, payroll, performance management and so on. However, the school will also have obligations to share this information with the local authority. For example under the National Schools and Colleges Contract, the school must notify the local authority if the head-teacher is absent for more than four weeks. This data is not collected solely because the local authority wants it – the school would hold it in any event e.g. for sick pay purposes.

- Another example relating to employees is in relation to employee vetting. A school has direct obligations under law to ensure that its staff are suitable. These are not simply contractual requirements carried out on behalf of the local authority. This means that data held or collected for the purpose of complying with these obligations will be data in respect of which the school is the data controller. Even where the local authority has a contractual right to review the school's record keeping in order to monitor compliance, this does not mean that the data is processed on the local authority's behalf.

- The school also has other directly enforceable legal obligations, and again data held in order to comply with these obligations will be data in respect of which the school is the data controller. These include requirements relating specifically to education such as those obligations listed in clause 4.2 of the National Schools and Colleges Contract, but also broader legal requirements such as health and safety. For example an accident book or health and safety report would be held or created for the school's own purposes to comply with these obligations.

- Data will also need to be shared in relation to safeguarding. This is likely to include information about school employees, non-employed staff or volunteer personnel as well as the learner or learners involved. Each party will have its own obligations in relation to safeguarding.

One exception to the general position that each party will act as a data controller and will simply share information with the other is information used by the local authority for the purposes of fulfilling its statutory obligations (for example the creation of the Educational Health and Care Plan). Even where the local authority is legally responsible for doing this, it will sometimes outsource the work to school staff. When using data for this purpose, the school may be the data processor of the local authority.

Current Position under the National Schools and Colleges Contract

The National Schools and Colleges Contract reflects the position outlined above. Clause 8.11 envisages that both parties will act as a data controller when performing the contract. It places an obligation on both parties to comply with their own data protection obligations as data controller. It also makes it clear at clause 8.9 that schools will have obligations in respect of data subject access requests, which is consistent with the school's position as data controller.

The contract does not currently contain any data processing provisions. Arguably there may be some situations in which data processing does take place as described above, and although these should be regarded as the exception to the rule, there is an argument for including a provision to cover what happens in this situation, unless this is to be picked up in a separate contract. However, even in this situation using a standard data processor clause without amendment is unlikely to be appropriate, not least because it will usually restrict the use of that data for the processor's own purposes.

Likely Requests

Approaches from third parties, including local authorities, are likely to take one of two forms – audit/assurance and requests for contract variation.

1. Audit/Assurance Questionnaires

   GDPR includes stronger obligations around governance and due diligence. There is a greater expectation that due diligence will be carried out before either appointing data processors or entering into data sharing relationships, and that audits will be carried out during the contract term to monitor compliance.

   It is therefore understandable that local authorities may ask for assurances around data use and the school's GDPR readiness at this stage. However, the questionnaires which are currently being used do not tend to be fit for purpose as they often assume that the recipient acts solely as a data processor and do not reflect the complexity of the data sharing arrangements which are in place.

   Audit questionnaires are particularly problematic when the school is asked to confirm whether it will "only act on written instructions from the local authority" or that it does not use personal data for its own purposes. Unless the scope of the questionnaire is clearly limited to specific processing in respect of which the local authority is the data controller, it can be hard to answer this type of question with a yes/no answer.

   It should also be borne in mind that an audit/assurance questionnaire alone will not satisfy GDPR requirements, which require a written contract to be put in place. Although some organisations may try to rely on a signature on the questionnaire it is not a formal contract and it is likely therefore to be the precursor to a request for a contract variation.

2. Contract Variation

   As noted above, large organisations typically try to create a "standard" contract variation which is sent to everyone they have contracts with, without consideration of the specific features of each relationship. These can take several forms, either a "Data Protection Addendum" which sits alongside the existing contract, a contract variation which expressly amends certain provisions, or a new contract which replaces the old contract in its entirety.

   Rather than signing this sort of document, where the agreement to be varied is the National Schools and Colleges Contract, we have generated a template version of Schedule 6 to incorporate appropriate terms into the contract. More detailed comments on this are set out below.

   For contracts which are <u>not</u> based on the National Schools and Colleges Contract it would be possible to adapt the wording in the template Schedule 6. However, advice should be taken in respect of the most appropriate way to build this in to the contract as each contract may require a slightly different approach.

   We believe this Schedule 6 wording is preferable to alternatives for the following reasons:

   - A blanket statement that the authority is a data controller and the school is a data processor is incorrect. The explanations set out above could be provided to the authority to make this point.

   - An obligation that personal data is only processed in accordance with the instructions of the authority is problematic unless this is very clearly limited to specific data processing activities and does not prevent use of the same data for other purposes by the school.

- An obligation to return or destroy all copies of the personal data on termination may be problematic if the school would need to retain the same data for its own purposes as data controller.

- Restrictions on the use of sub-processors or the transfer of data outside the EEA should be limited so that they only apply to specific processing activities. They should not restrict the operations of the school when it acts as a data controller.

Template Schedule 6

The template Schedule 6 is based on the standard format variation to the National Schools and Colleges Contract. The GDPR specific wording has been included in box 1 as follows:

- Paragraph 1 incorporates a new definition of data protection legislation. Because there are a number of matters which need domestic implementation, and because GDPR will not be directly applicable in the UK after Brexit, it will be supplemented by additional domestic legislation which is currently being considered by Parliament. This definition incorporates that legislation and deals with Brexit.

- Paragraphs 2 and 4 replace the reference to the Data Protection Act 1998 with the new definition of Data Protection Legislation, with the intention of keeping the change as simple as possible.

- Paragraph 3 again replaces the Data Protection Act 1998 definition with the new defined term. It also removes the reference to "respective registrations". The need to register details of an organisation's processing with the Information Commissioner has been removed by GDPR so this reference has been replaced with a reference to ensuring that any disclosures are permitted by law (which is particularly important for public sector data sharing), and that appropriate transparency information has been given.

These four paragraphs constitute the minimum variation required to replace obsolete wording in the original contract so that it actually reads correctly in light of the legislation changes. These paragraphs do not significantly alter the responsibilities or liabilities of either party. For that we've suggested different ways that a school might use the optional clause described below.

Optional Clause

Having included paragraphs 1-4, an additional optional clause (paragraph 5) can then be added to Schedule 6. This adds more detail around the respective responsibilities of each party than is in the current version. The existing wording simply states that each party will fully comply while the optional wording sets out much more detail about specific compliance requirements.

This approach is a more significant variation, rather than simply updating the contract. The majority of the changes apply equally to both parties, rather than favouring one party over the other.

These optional clauses should be used where the local authority has indicated that it wants to incorporate data processor clauses or to upgrade the level of protection above and beyond what is in the existing contract.

In order to use this clause there are two options:

- Use the full clause (whole of paragraph 5); or

- Include some or all of clauses 8.15 to 8.18 but not clause 8.19.

Clause 8.19 should not be used as a standalone clause because in isolation it does not cover off the GDPR data processor requirements in full. However, it does cover off everything if used in conjunction with the other clauses and the provisions which are already in the contract. This clause would not be required if the authority accepts that the school does not act as a data processor for it, but will give it the protection it is looking for if it insists that processing does take place.

Clauses 8.15 to 8.18 include wording which is not mandatory in data sharing agreements, but which could be included as a matter of good practice. They give greater clarity about the steps which both parties are expected to take to ensure compliance with GDPR and to assist the other's compliance efforts.

- Clause 8.15 covers security. There is a direct obligation on data controllers to meet these standards in any event so the main impact of including this rather than relying on clause 8.11 is simply to give local authorities comfort that schools are doing the right things. In return schools ask for the same commitments from LAs

- Clauses 8.16 and 8.17 cover confidentiality and assistance with compliance. These would be required in contracts between data controllers and data processors and although they are not strictly speaking required here, they make sense in a data sharing context and again they will give comfort to legal departments who are expecting to see this wording.

- Clause 8.18 is a data security breach notification provision. Again this is a reciprocal provision. The notifications required by Schedules 1 and 4 of the National Schools and Colleges Contract are one way only and do not include security breaches. However, it is advisable to improve that position with this reciprocal provision more suitable for a data sharing scenario as both parties will be affected by the tight timescales for notifying both the regulator and affected individuals if a personal data breach takes place.

Clause 8.19 sets out the position if one party processes data on behalf of the other. Whilst this is expected to be the exception to the rule for the all the reasons explained above, including some basic protection will give local authorities comfort that the issue is covered off. The clause only applies in respect of specific, agreed, processing activities and reflects the fact that the same data is likely to be used for each party's own purposes as well as the agreed data processing.

This clause does not cover the issues which have already been covered on a reciprocal basis in the other optional clauses. It also does not cover the audit rights required by GDPR because the authority's access rights are already picked up in clauses 8.3 and 8.5. If this clause is adapted for use in conjunction with other agreements, those agreements will need to be reviewed to see whether any additional wording is required.