**Data Protection Officers and independent schools: guidance on whether to appoint**

**One of the areas of the General Data Protection Regulation (GDPR) which has resulted in the most confusion in schools – and seen most mixed messaging from the many consultants and articles out there about GDPR – is the question of who will be caught by the new requirement for a mandatory Data Protection Officer (DPO), and what that title means.**

The short answer – which may surprise some – is that independent schools will not, in most cases, need to appoint one. The question of whether they ought to do so voluntarily is more complex. However, for reasons discussed below, adopting what might be seen as the most cautious or compliant approach (i.e. appointing a DPO in time for 25 May 2018) is not necessarily the safest route, let alone the most practical and commercial.

Appointing a DPO unnecessarily could be an expensive misstep, but many schools are confused about the role and what it entails. The Information Commissioner (ICO) has yet to put out guidance, while the existing EU working party guidance clearly does not consider the legal position of the UK independent schools sector. For this reason ISBA considers there is a clear need for a detailed note on the topic aimed at independent schools.

1. **What do we mean – and not mean – by a DPO?**

This is an important issue to get straight at the outset. Under GDPR, a DPO may not be what you think it is.

As a point of best practice – or, frequently enough, operational necessity – many schools already have a “Data Protection Officer”, or someone of similar title, who more often than not is the bursar. In times past this simply meant the person in charge of most data decisions and administration at the school, most notably dealing with subject access requests and other potential distractions.

Some schools, in common with other organisations, erroneously refer to this person referred to as a “data controller” – a misunderstanding of a term that refers, in data protection law, to the school itself. Prior to 25 May 2018, by contrast, "Data Protection Officer" or "DPO" would be a very sensible job title to give that person, in line with both ICO terminology and market practice. However, as we shall see, calling anyone by that title after 25 May 2018 will carry a risk if the role is not intended to have the precise legal effect intended of it by GDPR.

The more formalised, carefully prescribed role of the DPO set out in the GDPR pushes an already unwelcome series of operational responsibilities and requirements to a higher level – and brings with it HR and accountability headaches. This is why schools should think carefully before appointing a DPO, or even re-appointing the same person to the role, after 25 May 2018.

1. **Will your school legally require one?**

The ICO acknowledges (as it did at the ISBA Cyber Security conference in October 2017) that for independent schools this position is by no means certain. Neither the GDPR wording nor the current EU working party guidance discloses a clear basis to suppose that most independent schools would be intended to be caught by the strict requirement.

This is contrast to the much clearer position with maintained schools, because all public authorities do indeed require a DPO. It may be that a single individual DPO will affix to the local authority as a whole rather than to each school, according them a degree of independence (as well as being cheaper of course, allowing oversight of numerous maintained schools): but this will depend on levels of access and capacity to deal with issues. As set out below, there may be lessons to learn for independent schools in observing what works best.

1. The position with independent schools

For larger independent schools, it may be a relief that the draft GDPR requirement based on sheer numbers has not made it into the final regulation – for a time, it looked like any organisation of more than 250 people would require a DPO. Instead, the test is one of use and volume. Either

(a) do your “core activities” consist of either large-scale, systematic or regular monitoring of individuals?; or

(b) do your “core activities” relate to large-scale processing of special category personal data? (e.g. health, sexual life, ethnicity, religion – broadly the old “sensitive” categories).

The key terms here are “core activity” and “large scale”, and they are not further defined by GDPR. We are as yet lacking in clear and comprehensive guidance, but the EU working party guidance does draw some helpful conclusions. For example, it is the case that all employers are likely to process some special category data about their employees. However, while employing people is a necessary part of what they do, this does not make it their “core activity": it is ancillary to its main purpose.

A cautious analogy might be made to how schools process personal data of parents and, most obviously, pupils. Safeguarding, for example, is a core obligation on schools, and one which will properly involve both (a) the processing of sensitive personal data and (b) regular or systemic monitoring of staff and pupils. But the “core activity” of the school is education.

On balance, it might be safer to assume that a school's core activities *would* include processing special category data – but is it on a large scale? This is really where the DPO requirement looks less appropriate for most schools. "Large scale" is not defined but it would appear intended to cover bigger corporations who do market analysis, private health, tech companies and so on: it is unlikely to cover school communities of a few hundred people.

Considerations for what sort of larger independent school could be caught might, however, include:

* Do you hold a large amount of alumni data, and do you either monitor them or hold significant volumes of e.g. safeguarding files or incident reports?
* Do you have particularly intrusive monitoring systems?
* Is your school part of a large trust or multi-school business model where the "data controller" is likely to be the ultimate proprietor, i.e. the trustees or top company board?

If so, you might be looking at "large scale" processing activity of the sort that fits into either category, and consider the appointment of at least a single DPO for the entire group (where applicable). But until the ICO gives clear guidance on the topic, and lends some quantifiable measure to "large scale", there is something to be said for watching and waiting.

1. Comparison with other types of school

It will be of interest for the private schools sector to watch how the best practice position develops not simply with the ‘traditional’ state sector and academies, but also with more comparable models such as free schools and multi-academy trusts. These would qualify as public authorities, and require a DPO (albeit they are not always on all fours with maintained schools in how they are treated for certain other requirements of information law – e.g. a parent’s right to see the pupil file).

Structurally, and in terms of independence of decision making from local authorities (a key characteristic of a data controller being who actually determines what is done with personal data), such schools would seem to have more in common as data controllers with independents. Therefore independent schools should be vigilant as to developments elsewhere in education – even if they decide not to make the initial formal DPO appointment. It will be salutary to learn which DPO models work best in practice, especially for groups of schools, and which are less effective (or likely to have unintended consequences).

1. **What are the expectations of the new DPO role?**

**Notwithstanding the lack of certainty in the law – or perhaps because of it – some schools are considering appointing a DPO voluntarily. Whether or not you are required to appoint a DPO by law, if you do appoint one then the following applies:**

* **The DPO must possess “*expert knowledge of data protection law*”.**

This, notably, is not a requirement of IT expertise (although that might help!) but refers to a legal and practical understanding of how the law protects the privacy rights of individuals. GDPR values that over digital skills, and this seems particularly important in a schools context.

* **The DPO must be *properly*, and *promptly*, *involved* in all issues related to the protection of personal data at the school.**

This runs from policy (at the outset) and overseeing privacy impact assessments, to dealing with requests from individuals (e.g. subject access) and whether and how to report data breaches to the ICO (which is mandatory within 72hrs if a certain threshold is reached) or affected individuals. Ultimately these decisions are for the school to make as data controller – hence the requirement for the DPO to be "*properly* [i.e. meaningfully] *involved*", i.e. to advise and inform, rather than having fully delegated responsibility.

* **The DPO can be an existing member of staff, or appointed to take on more than one role: being DPO does not have to be his/her sole responsibility...**

This is consistent with the idea of course that a school can make an external appointment, or that one person can be DPO to several schools – provided there is sufficient access, in both directions, in each case (and sufficient independence from the interests of the governors / trustees / top company).

* **…however, a DPO must take sole responsibility for that role.**

Responsibility is not the same as liability (rather the opposite – as explained below, the liability is ultimately with the school). What this means is that you cannot share the role across two or three staff members: the ICO expects a single person as their point of contact.

This is in contrast to a more flexible team approach if your school does not make the formal appointment. Either way, depending on the size of your school, you may want data "champions" across several relevant departments (*administration / governance, IT, development, archives, legal/compliance, safeguarding, teaching staff etc.*) to assist the role.

* **The DPO must be independent, not too senior or conflicted…**

EU working party guidance is clear that senior management, and specifically the heads of key departments like IT and HR, could be too conflicted to carry the role effectively and objectively. Similarly, bursars (and head teachers) are likely to be too aligned in their interests with the school to qualify: a DPO must speak truth to power, and make recommendations often against the organisation's short-term reputation or commercial interests.

* **…however, the DPO must have clout within the organisation.**

They need to report to the highest level of management – the head, bursar and governors – and organisations are legally obliged to give them support, access, training and resources. As a compliance requirement, a DPO must be appointed “*on the basis of professional qualities*” and not simply appointed within the organisation based on who is willing to take on the role.

Therefore schools might understandably wonder who at their organisation could possibly qualify, and indeed what they might expect to be paid on top of their existing salary.

* **The DPO's independence is protected at law.**

Ultimately the DPO’s duties are as much to the ICO and to the public (the school’s “data subjects”) as they are to the school. GDPR states that DPOs “shall not be dismissed or penalised… for performing his [or her] tasks” – something approaching "whistle-blower" type protections – and should not “*receive any instructions*” in how to carry out those tasks.

In practice that definition of “instructions” may need to be explored: as above, it is ultimately for the data controller (school) to make decisions about whether to report a breach, disclose or amend a record, agree the terms of a contract with a data processor (e.g. cloud service provider), or go ahead with a major IT revamp or fundraising campaign. But the practical consequences of leaning on a DPO not to disclose something under a subject access request or ignoring a recommendation (e.g. concerning breach reporting or the impact of a new measure) could be serious in enforcement terms.

* **The DPO has considerable record-keeping responsibilities.**

This is not only a practical burden on the individual, but it is a core part of the accountability aspect of a school's GDPR compliance. Ultimately, if the school goes ahead with a major new project that might impact on individual privacy (e.g. marketing, CCTV, or monitoring), there should be a paper trail evidencing that this was thoroughly considered; and if a school has taken advice against a DPO's recommendation, the fact ought to have been recorded. The ongoing duty to assess and record the privacy impact of a decision continues even after the event.

* **When appointed, the DPO’s details must be published and notified to the ICO.**

The DPO's task includes a duty to "*cooperate with the supervisory authority*". One of the key tensions of the role is likely to be how the DPO balances duties to his or her paymaster with those to the regulator.

In summary, therefore, although designed to improve data protection practices at an organisation, the role of DPO brings with it considerable compliance and operative burdens in itself. For organisations like schools that are relatively small but extremely complex, and lacking substantial resources, it may be more attractive to adopt a more flexible approach than diving in to appoint a DPO.

1. **If we decide not to appoint a DPO, what *do* we have to do?**

As above, the ICO has not issued a clear position on DPOs and independent schools. Where the ICO is clear, in which regard ISBA and its lawyers are fully in agreement, is that any school will need to appoint a suitably trained, capable and competent person to take on the role of compliance lead at the organisation.

This person will require knowledge of data protection law, as well as being plugged in to the culture and structure of the school. In any event, the record keeping and accountability requirements of GDPR (as merely hinted at above) will need to be in place whether or not the person leading the charge is called a "DPO". So in fact, a school would want to go most of the way to appointing a role with all the qualities – and many of the responsibilities – of a DPO.

In doing so, the school would be well positioned to "flip" the role to a more formal appointment in the event that the ICO decided, down the line, that the Article 37 GDPR (the relevant section) had the effect of catching independent schools; or that such an appointment was always good practice in the sector; or if your school grew in size, or changed in structure, or started intensive monitoring. But there is a clear attraction in the meantime in waiting to see how the position pans out for others.

There is also a benefit in not having to appoint a new role; or allowing an outsider to have access to the school's most sensitive systems; or notably increase the burden and complexity of a valued existing employee's role. That is especially so, given the highly competitive employment market for individuals qualified to take on the DPO role (as either a full-time position or consultant) – and indeed the conflicting requirements about the person's required level of seniority, which does not lend itself well to an organisation the size of the average independent school.

1. **If we are not appointing a DPO, what do we call them?**

There is a final twist to this guidance.EU working party guidance is clear that to appoint anyone in a compliance lead role who is not intended to be a DPO, it must be clear to all (the public and the ICO) that this is indeed not intended. Calling them a DPO, or anything too close (School DPO, Officer for Data Protection, Data Processing Officer etc.) is therefore unwise and could well have the effect of requiring compliance to the high GDPR standard.

Consider more imaginative (but descriptive) variations like Compliance Officer (Data), Privacy Officer, Head of Data Protection and so on.

**Farrer & Co**

**October 2017**