In the middle of the 2017/2018 academic year, General Data Protection Regulation (GDPR) came into force. Educational Establishments faced an influx of alleged Data Protection breach claims. With a new academic year having just begun, Educational Establishments cannot afford to forget their regulatory obligations.

Obligations

GDPR requires personal data to be processed in a manner that ensures its security. Under GDPR, data, and how it must be processed, is categorised twofold:

**Article 5 GDPR – Personal Data:** Any information that can identify a student or their family. As well as including the obvious ones (students’ names, addresses, contact details) this also includes disciplinary records, progress reports and grades/marks. This type of data must only be collected for specified and legitimate purposes, must be kept up to date and kept in a form which permits identification of individuals for no longer than is necessary.

**Article 9 GDPR – Special Categories:** Any sensitive data including students’ race, ethnic origin, religious beliefs, health records, dietary requirements, biometric data (such as fingerprints), information relating to a student’s sex life or sexual orientation etc. There is an express prohibition preventing data which falls within this category from being processed/shared unless one of the exceptions set out in paragraph 2 of Article 9 applies. The exceptions include where the student has given their express consent for the data to be processed or processing the data is necessary for reasons of public interest.

**Routes to Redress**

Where a student has a complaint relating to an Educational Establishment’s alleged breach of GDPR, they have a number of routes open to them to seek recompense:

**Internal Complaints:** A student should commence a complaint by first referring it to the Educational Establishment itself to be dealt with under its complaints procedure.

**Office of the Independent Adjudicator:** Higher Education students with a complaint can refer their complaint to the Office of the Independent Adjudicator.

**Information Commissioners Office (ICO):** The ICO has the power to investigate alleged breaches of GDPR and can issue financial penalties and prosecutions.

**Civil Claim:** A student has the option of pursuing a civil claim for breach of GDPR/Data Protection against an Educational Establishment. In usual circumstances, a student will have 6 years from the date of the alleged breach to bring a claim, although there are a few minor exceptions to this.
A civil claim should always be seen as a last resort and other routes to resolution should be encouraged by Educational Establishments.

**Issues of Quantum**

Where complaints are pursued through the ICO, it does not have any powers to award compensation. It does however have the authority to impose fines. Such fines can be large if it considers a serious breach has been made.

In civil claims, compensation is often sought on the basis of the distress caused to the Claimant by the breach. Awards for claims for distress are fairly low. For context, in 2016 awards of between £2,500 and £12,500 were awarded (under the Data Protection Act) to six asylum seekers when their personal data was inadvertently published on the Home Office website. There is currently little in the way of case law which provides guidance as to how much compensation will be awarded for breach of GDPR. Though, it is likely a court would assess compensation on the same basis it did when assessing claims involving a breach of the Data Protection Act.

Fines issued by the ICO and awards for compensation under civil claims are commonly assessed by reference to the seriousness of the breach. This is established by looking at how widely the data in question was shared and the nature/sensitivity of the data shared.

**Protecting against claims**

There are some very straightforward ways Educational Establishments can protect themselves against GDPR/Breach of Data Protection claims:

1. Knowledge is power: Understand the Legislation, the grounds upon which data can be shared and when data must be protected;
2. Train teachers and staff members so that they also know the Legislation;
3. Have Data Protection policies in place;
4. Use resources provided by the government such as “Data Protection: toolkit for schools” available from Gov.uk.

**How Beale & Co can help**

We have experience in defending GDPR claims. Recent cases we have dealt with include achieving a favourable commercial settlement on behalf of a private school which had made an unauthorised disclosure of a student’s sensitive data and successfully obtaining the withdrawal of a GDPR breach claim made against a University because it had been brought out of time.

We have also helped Educational Establishments manage requests for disclosure pursuant to Subject Access Requests. This is a relatively common strategic approach by Claimants and potential Claimants.

---

For further information please contact:

**Giles Tagg**  
Partner  
+44 (0) 117 428 9306  
g.tagg@beale-law.com

**Sarah Hinton**  
Solicitor  
+44 (0) 117 428 9326  
s.hinton@beale-law.com