Steps to take following a data breach: reporting, criminal charges and injunctions

Student and staff files will be full of personal data, much of which may be particularly sensitive such as health information (known under the data protection legislation as “special category” data).

26 July 2021

Student and staff files will be full of personal data, much of which may be particularly sensitive such as health information (known under the data protection legislation[1] as “special category” data). Here we outline what universities need to do when a data breach occurs.

Your obligations

As data controllers, universities have an obligation under the data protection legislation to ensure that this personal data is processed consistently with the data protection principles and only shared with third parties if there is a lawful basis for doing so. Furthermore, as much of this sensitive information would also have been provided to universities in confidence, it cannot be shared with third parties without the consent of the person, unless it is required by law or can be justified in the public interest (such as to prevent serious harm to the person or others).

Unfortunately, it is not uncommon for data breaches to occur either due to the malicious actions of a third party or human error. In relation to the latter, this usually occurs when redactions have not been properly applied or made at all, or where certain information is shared despite this not being strictly necessary for the particular task at hand. In such situations, it is important for data controllers to immediately consider taking the following steps.

Reporting obligations

First, you should consider whether the data breach poses a risk to people. If it’s likely there will be a risk, then you must notify the Information Commissioner within 72 hours of becoming aware of the breach, where feasible. Reporting the matter to the ICO also allows you to bring the matter to the attention of the ICO’s Criminal Investigations Team if an offence under the Data Protection Act 2018 may have been committed (for example, if the personal data has been obtained or retained without your consent). If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, you must also inform those individuals without undue delay.

Informing the police

Once you have satisfied your reporting obligations, you should also consider notifying the police and/or pursuing civil action to prevent the confidential information from being used or shared more widely. It is of course a matter for the police to investigate whether any criminal offence has been committed, but if you can present sufficient evidence of an offence then, subject to it being in the public interest, the police should instigate criminal proceedings. The police could also use their search powers to obtain and retrieve the confidential information in question, which will often be a key aim for your institution.

Obtaining an urgent injunction in civil proceedings

Civil proceedings are also a good option to prevent the confidential information from being used or disclosed further. If you need to act quickly then you will need to seek an interim injunction before the substantive claim is filed. This will require you to satisfy the *American*

Cyanamid test, namely that: (1) there is a serious issue to be tried (see below); and (2) damages are not an adequate remedy; and (3) the balance of convenience favours the grant of an injunction.

Establishing a breach of confidence

In relation to the substantive claim, the essential ingredients of the tort of breach of confidence, as set out in *Coco v Clark* [1968] FSR 415, are that (i) the information is confidential in quality; (ii) it was imparted so as to import an obligation of confidence; (iii) there has been, or will be, an unauthorised use of that information to the detriment of the party communicating it. This includes confidential information that has been obtained by improper or surreptitious means, but will also cover situations where it has been obtained by mistake – for example when confidential information is inadvertently disclosed in response to a request under the data protection legislation or Freedom of Information Act.

Where a public body (which, depending on the context, may include a university) claims confidentiality in a document, the damage required to establish a claim for breach of confidentiality will be assessed by reference to the public interest. For an illustration of how these principles have recently been applied by the courts, see: London Borough of Lambeth v AM (No. 2) [2021] EWHC 186 (QB).

Contact us

Browne Jacobson's public law team frequently advises public bodies in respect of breaches of confidentiality. Its lawyers are experienced in liaising with the Information Commissioner and police in respect of possible criminal offences and commencing civil proceedings to restrain the unlawful use of confidential information. Please contact us with any questions about the immediate steps you can take to bolster your approach to data protection or if you would like any further information on what to do in the immediate aftermath of a data breach.

[1] Namely, the Data Protection Act 2018 and UK GDPR

Contact

Matthew Alderton

Partner

matthew.alderton@brownejacobson.com

+44 (0)330 045 2747

Related expertise

Services

Data protection and higher education

Data protection and information sharing in academy schools and trusts

Data protection and privacy

Information law

© 2024 Browne Jacobson LLP - All rights reserved