Student information in the US and EU

Andrew Cormack, Chief Regulatory Adviser, JANET(UK)

Abstract: A comparison of the legal requirements on handling students' personal data under the European Data Protection Directive and the US Family Education Rights and Privacy Act.

Table of Contents

1. Introduction 2
2. The Laws 2
   2.1 FERPA 2
   2.2 Data Protection Directive 3
3. Protecting Personal Data 3
4. Permitted Disclosures 4
5. Directory Information 6
6. Conclusions 7

1. Introduction

It is often said that Europe and America are very different in their treatment of information about individuals. Europe's privacy law divides the world into two halves – countries that provide adequate (by European standards) protection for personal data and those that do not. America is in the latter category.

However in the case of information about students held by universities and colleges, the requirements of the respective laws may be somewhat closer. This paper compares the US *Family Education Rights and Privacy Act* (FERPA) with the European *Data Protection Directive* (95/46/EC) and concludes that, although there remain significant differences in the treatment of FERPA's "Directory Information" and of information relating to disciplinary matters, FERPA appears to provide sufficient flexibility that a US university might choose to exercise its FERPA rights in a way that provided similar protection of students' personal data to that required by the European Directive. In view of the increase in exchange of students and educational resources across the Atlantic, choosing to do so may ease some of the legal obstacles.

This paper is not intended as, and should not be taken as, legal advice. Those who wish to exchange student data between Europe and the USA should consult their own lawyers.

2. The Laws

2.1 FERPA[1]

"The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education". FERPA therefore applies to information about students in the great majority of educational institutions in the USA. It does not apply to information about other personal information held by those institutions, nor to institutions (if any) that do not receive funding under Department of Education programmes.

[1] See http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

2.2 Data Protection Directive[2]

Directive *95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (the *Data Protection Directive*, or DPD) applies to all individuals whose personal data is processed (which includes collection) in a country of the European Union. It therefore applies, among others, to all staff and students of European universities and colleges and probably also to those studying courses from those universities and colleges in other parts of the world.[3]

3. Protecting Personal Data

Both laws recognise that both the accuracy and privacy of personal data relating to education are important.

To ensure accuracy, both give the individual the right to inspect (FERPA s99.10, DPD Art 12(a)) and correct (FERPA s99.20, DPD Art 12(b)) their own records. For an individual who is under 18 years old and in primary or secondary education, FERPA gives these rights to the individual's parents (s99.5(a)). The European Directive does not contain specific provisions for children, but the guidance[4] of the Article 29 Working Party indicates that some of their rights may be exercised by their parents until they reach the age of 18.

To ensure privacy, both laws require that information is protected against unauthorised access (FERPA s99.31(a)(1)(ii), DPD Art 17(1)). Both restrict the authorised disclosure of information by listing disclosures that are permitted and prohibiting any others unless the individual gives consent (FERPA s99.30, DPD Art 7). FERPA expresses permitted disclosures as a detailed list in s99.31 of those to whom information may be disclosed whereas the Directive specifies in more general terms the purposes for which disclosure is permitted (Articles 7 and 8). However, as discussed in the following section, these different forms of specification appear to have broadly similar effect. Both also impose controls to ensure that those to whom information is disclosed may not themselves disclose it further (FERPA s99.33, DPD Art 16). FERPA is somewhat stricter in requiring that a record be kept of most permitted disclosures (those for which records are not mandated, such as judicial access, appear likely to create their own records)(FERPA s99.32) and also in stating that the individual's consent must be expressed in writing (FERPA s99.30).

The major difference between FERPA and the Directive is FERPA's category of "Directory Information". As discussed below this contains a significant amount of information that in Europe would be considered personal data, therefore requiring protection and having

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
[3] See Article 29 Working Party Opinion 8/2010 on Applicable Law http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf
[4] Opinion 2/2009 on the protection of children's personal data http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

restrictions on further use. However FERPA (s99.31(a)(11)) allows directory information to be published without consent and, once published, neither US law nor practice appears to place any restriction on subsequent re-use. None the less, disclosure of directory information appears to be only permitted, not required, so an educational institution subject to FERPA could choose instead to treat directory information in the same way as other personal information and thereby approach much more closely the European requirements.

4. Permitted Disclosures

FERPA contains a detailed and exhaustive list of the circumstances in which personal data about a student may be disclosed without the student's consent. The Data Protection Directive takes a higher level view, giving in Articles 7 and 8 a list of criteria that may make processing (which includes disclosing) of personal data legitimate. Article 8 relates to the narrower category of Sensitive Personal Data, defined in Articles 8(1) as personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership" or "concerning health or sex life". Article 8(5) further limits the processing of "data relating to offences, criminal convictions or security measures".

The Directive gives national legislatures some flexibility around these criteria, so it is not possible to state that the FERPA disclosures will all be permissible in every European country. However the following table lists the disclosures permitted by FERPA (note that a number of these are subject to further restrictive conditions) and indicates which criterion in Article 7 or 8 is likely to be applied to that process by European national laws on information about students. Where there are significant differences between the two regimes, these are highlighted by italics and discussed below the table. Other than where the purpose of the disclosure clearly requires sensitive personal data, the table assumes that only non-sensitive data will be disclosed and therefore that an Article 7 criterion is sufficient.

Disclosure	**FERPA**	**DPD criterion likely to apply**
To officials within the school who have legitimate interests	99.31(a)(1)	7(b) necessary for the performance of a contract to which the data subject is party
To another school in connection with the student's enrolment there	99.31(a)(2) & 99.34	7(b) necessary for the performance of a contract to which the data subject is party
To authorities conducting audits or evaluations of state funding programmes	99.31(a)(3) & 99.35	7(c) necessary for compliance with a legal obligation, or 7(e) necessary in the exercise of official authority
In connection with financial aid to the student	99.31(a)(4)	7(b) necessary for the performance of a contract to which the data subject is party
To state or local officials where permitted by law	99.31(a)(5) & 99.38	7(c) necessary for compliance with a legal obligation

To organisations conducting studies for educational agencies or institutions on testing, teaching or student aid	99.31(a)(6)	7(f) necessary in the legitimate interests of the educational organisation and not overridden by the individual's fundamental rights. FERPA's detailed specification of the agreement between the organisations appears likely to create a data controller/data processor relationship under Article 17.
To accrediting organisations to perform those functions	99.31(a)(7)	7(b) necessary for the performance of a contract to which the data subject is party
To parents of a dependent student	*99.31(a)(8)*	*According to section 152 of the Internal Revenue Code of 1986,[5] a "dependant student" can be up to 24 years old. It is unlikely that someone as old as this would be considered a child under European law, so disclosure to parents of these students is unlikely to be permitted unless it is covered by some other purpose.*
To comply with a judicial order or subpoena	99.31(a)(9)	7(c) necessary for compliance with a legal obligation
In connection with a health or safety emergency	99.31(a)(10) &99.36	7(d) necessary to protect the vital interests of the individual, or, for sensitive personal data 8(c) necessary to protect the vital interests of the individual or another person where the individual is physically or legally incapable of giving consent
To the student (or the parent of an under-18 year old)	*99.31(a)(12)*	*There is no directly equivalent general provision in the Directive, however Article 12 entitles an individual to obtain a copy of their data that is processed and Articles 10 & 11 require an organisation to inform the individual what types of data are being processed.*
To the victim, of the outcome of a disciplinary hearing following an alleged crime of violence or a sexual offence	*99.31(a)(13) & 99.39*	*Article 8(5) states that processing of data relating to offences may only be carried out under the control of the appropriate legal authority, or if national law provides suitable safeguards for processing by others. Whether these FERPA disclosures are permitted will therefore depend on national, rather than European, law.*
Of the outcome of a disciplinary hearing where an alleged perpetrator of a crime of violence or sexual offence was found to have breached the organisation's rules or policies	*99.31(a)(14) & 99.39*	
To the parent of a student under 21 of a violation of law or policy relating to alcohol	*99.31(a)(15)*	*As above, processing of data relating to crimes is controlled by national law. Disclosure of breaches of policy by those aged between 18*

[5] http://www.irs.gov/taxpros/article/0,,id=98137,00.html

or controlled substances		*and 21 appears only to be permitted if it falls within criterion 7(d) necessary to protect the vital interests of the individual*
Concerning sex offenders and others required to register	99.31(a)(16)	Provided the disclosure is required by national law, it will be covered by 7(c) necessary for compliance with a legal obligation
Of de-identified, or re-coded records or information	*99.31(b)*	*It is not clear what degree of de-identification is required to allow a record to be treated as non-personal data under European law. In particular where 'opaque' identifiers are attached to information, as permitted by 99.31(b)(2) there is considerable variation and occasional contradiction in European guidance and case law. The Article 29 Working Party has an Opinion on the Concept of Personal Data.*[6]

It therefore appears likely that most of the disclosures permitted by FERPA would also be permitted by European data protection law. There are two areas – disclosure to the individual data subject and disclosure of de-identified or re-coded data – where European law might introduce additional restrictions that do not appear to be present in FERPA. Only four of these FERPA disclosures are likely to be prohibited, or at least significantly more restricted, by most European jurisdictions: those relating to alleged breaches of laws or policies relating to alcohol, controlled substances, violent or sexual crimes and disclosure to parents of adult children. In these areas a US educational organisation might need to modify its normal practice to comply with European law.

5. Directory Information

The major difference between FERPA and the Data Protection Directive appears to be in the category of Directory Information, defined in s99.3 as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed". According to s99.37 it appears that each educational institution can decide which information it will place in this category, so the lists of information in s99.3(a) and (c) are indicative only (and explicitly do not prevent other types of information being treated as Directory Information):

> "(a) Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g. undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended.

[6] Opinion 4/2007
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

(c) Directory information includes a student ID number, user ID, or other unique personal identifier used by the student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password, or other factor known or possessed only by the authorized user."

It is clear that most of this information falls within the Data Protection Directive's definition of personal data: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Art 2(a)). If exercised, therefore, the right granted by FERPA s99.31(a)(11) to disclose this information without consent or any of the other legitimising purposes would be likely to breach of the Data Protection Directive and its national equivalents. Furthermore, once disclosed there appears to be no law or practice that would restrict the further use of Directory Information by anyone who received it, unlike the Data Protection Directive that regards even published personal data as still benefitting from protections.

Fortunately FERPA appears to provide three ways to resolve this considerable difference. s99.37 requires an organisation to publish a list of information it considers to be Directory Information and to allow students to opt-out of having this information disclosed. Such opt-outs must be respected, though a former student cannot retrospectively opt-out if they did not do so during the period of their study. An organisation subject to FERPA can therefore either:

a) Choose not to disclose Directory Information, or

b) Declare a local definition of Directory Information that does not include anything falling within the EU personal data definition, or

c) Treat students subject to EU law as having opted out of disclosure of Directory Information (this option still allows the school to disclose students' names, identifiers and e-mail addresses within their classes, which may not match European practice).

6. Conclusions

It therefore appears that while FERPA permits some disclosures that would be contrary to EC law, it does not require them (however, other federal and state laws may do so). If a university or college subject to FERPA can choose not to disclose information in those circumstances it might thereby achieve protection close to the European approach. In particular, when handling Directory Information FERPA provides a number of mechanisms that would permit a university or college not to disclose this information. Furthermore since FERPA already requires organisations to have processes to implement opt-out requests by US students, it does not appear that treating all European students as having opted out should require any new processes.

Such an approach might allow a US university or college to provide similar protection of students' personal data to that required in Europe. Unfortunately at present there seems to be no mechanism for having this formally recognised by European law since the current 'safe

harbor' scheme[7] is only open to commercial companies, not to educational organisations. European universities wishing to transfer student information to universities or colleges in the USA are therefore likely to have to continue to perform individual assessments of the adequacy of protection of that information under EU law.

[7] http://www.export.gov/safeharbor/