Bloomberg Law®

Privacy Law Watch™

INSIGHT: GDPR Complicates Admissions Applications for U.S. Universities




By Mark Barnes, David Peloquin, Leslie Thornton, and Nicholas Wallace, Ropes & Gray LLP

The European Union General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, which became effective May 25, 2018, poses compliance challenges for some longstanding admissions practices of U.S. universities that accept applications from students located in the European Economic Area (EEA), which includes the 28 member states of the EU and the three additional countries of Iceland, Liechtenstein, and Norway. Certain provisions of the GDPR could complicate U.S.-based universities' collection of routine application information, including racial or ethnic origin information that universities are required to solicit under applicable U.S. law, as well as criminal history information that many U.S. universities routinely collect.

University applications involve the collection of an array of personal data subject to the GDPR when collected from persons located in the EEA (*e.g.*, the names and contact information of students, their parents, and those who write letters of recommendation). This article, however, focuses on the collection of applicants' racial and ethnic background and criminal conviction history. At this point, it is not clear how the EEA authorities will view these information collection practices and/or whether any U.S. or state laws will be regarded as providing an adequate basis under the GDPR for collecting and processing at least racial and ethnic background information.

Overview of EEA Applications to U.S. Universities The number of EEA applicants to U.S. universities is substantial: in the federal fiscal year ended September 30, 2017, 59,566 F-1 (student) and F-2 (spouse or child of a student) visas were issued to students from Europe. This figure may on the one hand over-count students whose information is subject to the GDPR, as it includes students who are resident in non-EEA European countries (*e.g.*, Switzerland and Russia), but on the other hand it may under-count students whose information is subject to the GDPR because it does not include students who are admitted with J-1 visas for cultural exchange purposes. The number also does not include those who apply and are not admitted to any university and therefore do not receive a visa. See Report of the Visa Office 2017, U.S. Department of State, Bureau of Consular Affairs, Statistical Tables XVI(B) and XVII (Part I).

The unified university application submission system administered by the Common Application adds a further dimension to universities' GDPR compliance analysis. Currently more than 750 universities accept the Common Application, an application portal that allows students to enter basic application information (demographic information, etc.) along with university-specific information for all schools to which the applicant is applying. While the Common Application entity itself would be subject to obligations under the GDPR and considers itself a data ''processor'' under GDPR, the universities that accept the Common Application are also subject to the GDPR with respect to the application data collected on their behalf by the Common Application. *See* The Common Application, European Union GDPR Update. This is because the universities would be considered ''controllers'' of the personal data under the GDPR as they determine the purposes and the means of processing the personal data collected in the applications; in short, the universities oversee the application process itself. *See* GDPR, Art. 4.

The GDPR is relevant to U.S. universities collecting personal information from EEA-based applicants because the GDPR applies to the processing of personal data by organizations not established in the EEA when such organization's processing of personal data is re-

lated to the offering of goods or services to data subjects located in the EEA. *See* GDPR Art. 3(2). By making efforts to recruit EEA-based students, U.S. universities are offering their services to such students. Thus, the information collected from such students during the application process would be subject to the GDPR.

University Application Data Collection Requirements Under U.S. Law U.S. educational institutions that receive federal funds, such as federal loans issued to students, are required to ask students about their racial and ethnic background using a two-part question prescribed by the U.S. Department of Education. The question first asks whether the respondent is Hispanic/Latino and second whether the respondent is from one or more races using five defined racial groups: ''American Indian or Alaska Native, Asian, Black or African American, Native Hawaiian or Other Pacific Islander, and White.'' 72 Fed. Reg. 59266, 59267 (Oct. 19, 2007). While educational institutions are required to ask about race and ethnicity, individuals are not required to self-identify their race or ethnicity. *See id.* at 59,268.

In addition to these federal requirements, some state laws require universities to request from applicants certain racial or ethnic origin information. For example, California law requires state agencies that collect demographic data regarding ancestry or ethnic origin—which would include California State University—to ''use separate collection categories and tabulations for each major Asian and Pacific Islander group, including but not limited to, Chinese, Japanese, Filipino, Korean, Vietnamese, Asian Indian, Hawaiian, Guamanian, Samoan, Laotian, and Cambodian.'' Cal. Gov. Code § 8310.5. Thus, even though universities that are considered California state agencies are already required to request from applicants ancestry and ethnic origin information pursuant to the federal regulations described above, California state universities must also collect more detailed information with respect to Asian and Pacific Islander populations.

As for information pertaining to criminal convictions, federal law does not require universities to ask for such information in the application process. *See* Albert Jung, *Ban the Box in College Applications: A Balanced Approach*, 26 Cornell J. of L. and Pub. Pol. 171, 177 (2016) (noting that, ''[t]he current federal law neither explicitly prohibits nor allows colleges to make an admission decision based on an applicant's criminal records''). Nevertheless, collecting criminal conviction information has become widespread within the last decade, as the Common Application began asking such questions in 2006. The Common Application asks questions about both misdemeanor and felony convictions and guilty adjudications in the juvenile system. *See* Judith Scott-Clayton, *Thinking 'Beyond the Box': The Use of Criminal Records in College Admissions*, Brookings Institute (Sept. 28, 2017). The collection of such information has recently come under scrutiny from advocacy groups and the media, which have raised concerns that the information collected creates an inequitable barrier to enrollment for persons who do not pose a threat to campus safety and reinforces the disparate impact of the criminal justice system on racial minorities. *See, e.g.*, The Editorial Board, *College Applications and Criminal Records*, The New York Times (Mar. 14, 2015); Scott-Clayton, *Thinking 'Beyond the Box'*.

Now, in addition to these policy challenges, universities face a legal challenge to collecting criminal conviction information from EEA-based applicants due to the GDPR.

Application of the GDPR to Collections of Racial and Ethnic Origin Information Racial and ethnic origin are considered ''special categories'' of personal data under the GDPR, along with personal data revealing political opinions, religious or philosophical beliefs, or trade union membership as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *See* GDPR, Art. 9(1). In addition to having a basis to process such data under Article 6 of the GDPR, an additional basis under Article 9 of the GDPR is required in order for the processing of special categories of personal data to be lawful. *See* GDPR, Art. 9(1), *see also Guide to the General Data Protection Regulation, Lawful Basis for Processing,* United Kingdom Information Commissioner's Office (advising that, ''[i]f you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9.'').

The GDPR provides a variety of bases that legitimize the processing of special categories of personal data, including, for example, the data subject's explicit consent, the necessity of the processing for the purposes of carrying out the obligations and exercising specific rights of the controller or data subject, and the necessity of processing to protect the vital interests of the data subject or of another natural person, among others. ***However, in the university admissions context, the data subject's explicit consent likely would be the only applicable basis for the processing of racial or ethnic origin information.***

Designing a GDPR-Compliant Consent for Collection of Racial and Ethnic Origin Information in a University Application The GDPR's text and interpretive guidance should be taken into account in designing a GDPR-compliant consent for the collection of racial and ethnic origin information required by U.S. law. As a general matter, in order to be valid under the GDPR, consent must be a ''freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'' GDPR, Art. 4(11). The Article 29 Working Party (WP29), an EU body that issued non-binding guidance on data protection law prior to the implementation of the GDPR, has interpreted each of the elements of consent.

First, according to WP29, in order to be ''freely given,'' the data subject must be able ''to refuse or withdraw his or her consent without detriment.'' Working Party, *Guidelines on Consent under Regulation 2016/679* (Apr. 10, 2018). In the context of an admissions application, this implies that consent is an appropriate basis for the processing of information concerning an applicant's racial or ethnic origin only if consideration of admission is not in any way contingent on the applicant's having provided consent to the university's processing of racial or ethnic origin information for admission purposes. Therefore, an applicant who declines to provide racial or ethnic origin information and declines to consent to the processing of that information must under the GDPR be treated no differently during the application process from an applicant who provides his or

   ISSN 0000-0000

her racial or ethnic origin information and consents to the processing of that information.

Of course, universities often consider racial and ethnic origin in making admissions decisions in order to ensure a diverse student body and to implement their affirmative action policies. Therefore, persons who do not provide racial and ethnic information may not, in truth, receive the same benefit in the admissions process that they would have had they provided race and ethnicity information. This makes the collection of race and ethnicity information from EEA-based applicants risky, and U.S.-based universities can argue only that those applicants from the EEA who decline to consent to giving their race and ethnicity information are treated no worse than other applicants from other countries who also refuse to provide this information—although this argument is somewhat circular. Moreover, the ''no detriment'' concept would appear to preclude any admissions policy or practice in which a student's application is not considered at all if he or she declines to provide race or ethnicity information, because in such a circumstance the student would face the ultimate detriment as a result of his or her failure to provide consent, *i.e.*, denial of admissions.

Second, the WP29 guidance explains that in order for consent to be ''specific,'' the data subjects must be ''specifically informed about the intended purposes of data use concerning them.'' *Id.* at 12.

Third, and similarly, in order for consent to be ''informed,'' WP29 emphasizes that data subjects must have information accessible to them regarding the purposes of processing *before* they are asked to provide consent. *See id.* at 13 (stating that, ''[p]roviding information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent''). WP29 goes on to note that at least the following information should be provided to the subject:

- the controller's identity,
- the purpose of each of the processing operations for which consent is sought,
- what type of data will be collected and used,
- the existence of the right to withdraw consent, and
- information about the use of the data for automated decision-making, where relevant.

See id. at 13. Thus, to satisfy both the second and third elements of consent, the admissions process must explain to the applicant the identity of the university as the controller, the purpose for which his or her racial or ethnic origin information is collected, and of the right to withdraw consent. It is unlikely that universities will make automated decisions based on the racial or ethnic data, especially given U.S. Supreme Court precedent holding that ''race or ethnic background may be deemed a 'plus' in a particular applicant's file, yet it does not insulate the individual from comparison with all other candidates for the available seats.'' *Regents of the University of California v. Bakke*, 438 U.S. 265, 317 (1978). Thus, notice of automated decisions is unlikely to be required in the consent.

In order for the consent to be valid, this information should not be buried in the privacy notice provided to subjects during the admissions process, but should be made readily available to the applicant at the time he or she is asked to furnish consent for this processing of racial or ethnic information as a special category of personal data. Read together with GDPR Art. 7's requirement that the request for consent be clearly distinguishable from other matters discussed in the form, this would suggest setting apart the request for racial or ethnic origin information (and any other special category of personal data requested from applicants, such as religious affiliation or LGBT status) from other informational items requested as part of the application process. Moreover, preceding the request for racial or ethnic origin and other special category data, the form should include an explanatory paragraph that provides all of the information required for a valid consent.

Fourth, the WP29 guidance notes that in order for consent to be ''unambiguous,'' the data subject must take a clear affirmative act, which may, in the online context, include filling an electronic form or using an electronic signature. *See id.* at 17. Thus, an applicant's completion of the racial or ethnic origin field(s) in the online application could provide the ''clear affirmative'' act necessary for the consent to be explicit, provided the consent is freely given, specific, and informed as noted above.

If universities adhere to the guidelines discussed above, they may be able to meet all the requirements to obtain subjects' explicit consent to the processing of their racial or ethnic origin information. When universities rely on a third-party entity to collect applicant information and obtain a GDPR-compliant consent, they should examine their contractual arrangements with the third party to ensure that the third party has agreed to obtain all required consents and, preferably, to indemnify the university for any losses it suffers if the third party fails to do so.

Application of the GDPR to Collections of Criminal Conviction History Information Criminal conviction information is not considered a special category of personal data under the GDPR, but separate heightened requirements apply for the processing of such information. In order to process data on criminal convictions and offenses, the GDPR sets forth two requirements: (i) a controller needs a basis for processing the personal data under Article 6 of the GDPR and (ii) the processing must be (a) carried out only under the control of ''official authority'' or (b) authorized by EEA or member state law providing for appropriate safeguards for the rights and freedoms of data subjects. *See* GDPR, Art. 10.

First, in order to process this type of data, a university would first need to show an Article 6 basis for processing, such as legitimate interest. Under the legitimate interest balancing test, a university would need to demonstrate that its need to know of an applicant's criminal conviction history—for example, to protect against future criminal acts by the individual—outweighs the individual's interest in keeping such information private.

Second, even if a university can show that it satisfies the legitimate interest balancing test under Article 6, it would also need to show that its processing of such information is done under the control of an ''official authority'' or as authorized by EEA or member state law. The term ''official authority'' is not defined in the GDPR, however guidance from the United Kingdom's

Information Commissioner's Office (ICO) suggests that the term is intended to cover ''public functions and powers'' that are ''laid down by law.'' *Guide to the General Data Protection Regulation, Public Task*, ICO. The ICO guidance goes on to state that ''laid down by law'' means that the function is set forth in statute, statutory guidance, or common law and notes that organizations acting under ''official authority'' will most often be public organizations or those vested with public powers by a government agency. *See id.* Because U.S. law generally does not require the collection of criminal conviction information, it seems unlikely—at least according to the UK ICO interpretation of Article 10—that a university could rely on the ''official authority'' basis for processing criminal convictions. While this guidance would apply to both public and private universities, private universities would likely face even greater suspicion under the interpretation set forth by the ICO, as they are not public organizations.

Assuming the ICO interpretation is correct, this would leave EEA or member state law as the only potential basis for a U.S. university to process criminal conviction information. Given the specific reference to EEA or member state law, it's unlikely that any reliance on U.S. federal or state law (even if any *were* to require the collection of criminal conviction information) could satisfy this requirement. That said, if a university were to face such a conflict of U.S. law and the GDPR, the university arguably could contend that its processing is authorized by law and thus in line with the spirit of the requirements of Article 10. This argument would likely be viewed more favorably by EEA regulators if the relevant state or federal law placed some defined limitations on the university's use of the information in order to protect the privacy of data subjects.

Whether EEA regulators would credit such an argument is uncertain. As a policy matter, such reliance would seem contrary to EEA supervisory authorities' general goal of extending EEA-style data protections beyond the borders of the EEA. Indeed, fears about the U.S. government's surveillance efforts through the National Security Agency have been at the core of privacy litigation such as the *Schrems* case, in which the Court of Justice of the European Union invalidated the EU-U.S. Safe Harbor for data transfers. *See* Judgment of the Court, Case C-362/14 (Oct. 6, 2015). Accordingly, EEA authorities may be skeptical of reliance on U.S. law as a basis to process criminal conviction information.

Consequently, U.S. universities' ability to continue to collect and process criminal conviction information of persons located in the EEA as part of the admission process is far from clear. While a path for such processing is not stated under the GDPR, such processing is also not expressly forbidden. Until greater clarity is offered by EEA regulators, U.S. universities will have to decide whether to continue collecting criminal conviction or offense data from EEA applicants, understanding the possible risks of doing so.

Conclusion Given the numerous students from the EEA admitted to U.S. universities, and the corresponding or greater number of applications received from the EEA, the GDPR poses challenges to U.S. universities seeking to comply with EEA data protection law. While universities can likely tailor their application to obtain valid consent—for those applicants willing to consent—to the processing of racial and ethnic origin information, there is not a clear path to permit universities to continue collecting criminal conviction information from applicants located in the EEA.

Authors' Information

Mark Barnes, David Peloquin, Leslie Thornton, and Nicholas Wallace are attorneys at Ropes & Gray LLP.

The views expressed in this article are those of the authors and not necessarily those of Ropes & Gray or its clients, or of Bloomberg Law.

  PRA ISSN 0000-0000