Item	Question	Response
1	Can a CISO serve as the Data Protection Officer, or would that role be better placed within the Compliance office?	The choice of who is DPO must ensure that the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. We would say that this suggests a CISO should not be DPO. The DPO must report to the highest management level of your organisation – ie board level and therefore could be a Compliance Officer provided they have the necessary seniority. The role does require that they should have professional experience and knowledge of data protection law which should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.
2	Can you explain more the issue of right to be forgotten as it applies to higher ed? There are certain requirements around retention of data required by DOE that seems to be in conflict with this right.	As a general principle, if there are other legal obligations relating to retention of data, then these take precedence over GDPR. However, even if you have a legal obligation or legitimate requirement to retain data in defiance of a Right to be Forgotten request, you should establish policies around who can see that data and what can they use it for. Remember, the legal basis for what data you hold is separate from the legal basis of how you use it.
3	Can you help me understand how the regulations of GDPR applies to institutions who are under the jurisdiction of U.S. law? I know it applies if there is data stored on E.U. residents, but I don't understand how it is enforceable outside of the E.U.	The simple answer here is that if you are choosing to do business in the EU or if a business in the EU is passing personal data to you, then EU laws apply. As to enforceability, this will be under the aegis of international law which will apply to the US. In fact, if you have an EU presence, then enforcement will be made against that entity. Alternatively, if you don't have an EU presence, then you are supposed to designate a "representatve" located in the EU for precisely this reason.
4	Can you please specify again which individuals' data GDPR applies to?	Anything that identifies a natural person. This would usually be a name and something else eg address, date of birth etc or could be something specific such as an IP address. The reason why you have it is irrelevant; the individual could be a lecturer, student, examiner, plumber etc - GDPR applies in all cases of identifiability.
5	confirm: any personal data collected while a person is at my US institution is *not* covered by GDPR, regardless of their national affiliation.	It depends on why the individual concerned is at your institution and how you gained their personal information. For example, if you have an academic on secondment from an EU university or an EU student placed via an exchange program then GDPR would apply. Alternatively, if they applied directly to you in their private capacity, then GDPR does not apply. They are, however, in all cases subject to US data privacy laws.
6	Could you clarify more about who's data is implicated? If a student is pysically in the U.S. and they provide data, GDPR doesn't appply? If the student then moves to the EU (e.g. for study abroad), then GDPR applies going forward or including data already collected? And if the student returns to the U.S.?	See answer to number 5.
7	Could you expand the obligation under the Right to Forget	See answer to number 2.

Item	Question	Response
8	How do we confirm where our data is being held?	That can a problem but one for which you are responsible. In the first instance, you need to undertake a Data Discovery exercise by asking all your business units to identify what personal data they have/use/access including interaction with any third-parties. Then, for each set of data, you need to establish who has custodianship both for the live version and any develolpment, testing, backup, disaster recovery versions - for this, you will need to interrogate your own IT support resources and all third-parties who "process" your data (remember "processing" includes viewing , storing etc).
9	How do we identify a consultant to help us?	Contact mark Bednarz of PKF O'Connor Davies in New York at mbednarz@pkfod.com or Ian Singer at PKF Littlejohn in the UK at isinger@pkf-littlejohn.com.
10	how does the EU have any authority to impose penalties on a US company?	See answer to number 3.
11	How to spell cribish shield?	Sorry, that's my English pronunciation! I presume you mean Privacy Shield which is the US-established data privacy standard that is accepted by the EU as GDPR-compliant.
12	How will US title IX legistlation relate to the right to be forgotten?	See answer to number 2.
13	If it takes 3 weeks to confirm the breech are you in violation of the 72 hrs response time	No…but. You have to report a breach within 72 hours of becoming aware of it not when it occurs. However, you must have in place appropriate breach detection mechanisms to ensure that you are likely to be aware of a breach in short order.
14	If recruiting applicants over internet for services delivered in the US, does GDPR apply to those applicants? How about applicants for students? Not employment related.	See answer to number 5.
15	If there are EU students enrolled in summer programs at a US university, does GDPR apply to the EU student information gathered by the US university?	See answer to number 5.
16	In my state we have data retention requirements. What about conflicts when EU says remove data and a state in US says retain it?	See answer to number 2.
17	In proving the need to hold a data, what are sufficient reasons? Some people may simply say that their system requests specifics pieces of data which does not seem substatial.	See answer to number 21.
18	our compliance officer says that the EU can not enforce GDPR since we do not have campus location in the EU, can you confirm this or qualiy how it might otherwise apply to our university?	See answers to numbers 3,5 and 26.

Item	Question	Response
19	Should a US University contracting with a EU University for student exchange ask the EU University to declare compliance with GDPR?	Definitely. Under GDPR, both Data Controllers and Data Processors are equally liable so you are potentially equally at risk if they are in breach. Also remember that you need to demonstrate compliance with Privacy Shield or equivalent otherwise you are both breaking the law.
20	Study abroad programs - does GDPR only apply if EU citizen enrolled (vs US students only going to EU to study)?	It is a misconception to regard the GDPR as applying only to EU Citizens. It applies to anyone to whom EU laws are applicable which would include US Citizens working/studying in the EU.
21	Talk a bit more about consent. Like most institutions, we have hundreds of forms for multiple purposes. Must we ask for consent on every form? What about data that is gathered that the student is unaware of until later, like judicial information?	There are three main likely relevant legal bases for asking for and using personal information. Consent is one but more likely you would rely on "performance of a contract" as you cannot process their application or provide the tuition without the information you are asking for. So long as the individual concerned has a clear understanding of why they need to give you the information and provided you only use it for that purpose then you don't need separate "consent". The third legal basis is "legitimate interests" which may include things like checking government or commercial databases eg credit rating, criminal records. However, under GDPR, you must inform the data subject of all uses of their data such as in these circumstances. You don't need their consent if you can justify the reason why you are doing it but you cannot do it without informing them of the fact.
22	THat last point is contradictory to what we hear from NACUA and other associations. The question about the person from London who applies for the job in the US, and this isn't covered by GDPR. This isn't what we have been advised at all.	I have now spoken to the Information Commissioner in the UK and they have confirmed my interpretation of the situation. As I posited, if I'm in the US on holiday or as an ex-pat, see a course I'm interested in offered by a US institution and sign up for the course then there is no way that GDPR applies – only US data protection laws. Therefore, my logic says that, if I see the same course and sign up on the same website and just happen to be in London when I do so, GDPR still doesn't apply as there is no difference in engagement or outcome. The ICO has confirmed this is also their view. Also, see answers to numbers 5 and 26.
23	Under GDPR can you still charge for Transcripts?	I don't understand the question, I'm afraid.
24	What about EU students who apply to a US school and then take online courses from the US instituion?	See answers to numbers 5 and 26. Distance learning may be a grey area if the provision of the service is deemed to be located in the EU. My view would be that unless the course is not specific to the EU or to the individual, then you are probably OK.
25	What about person from EU but working for your organization in the US?	See answer to number 5.
26	What about someone from France applying to attend UCLA? Isn't that data from the French person covered by GDPR since it originates in the EU? This is a big issue for universities	See answer to number 5. However, you need to be careful that you don't target eg French students in your marketing either through direct mail, advertising language, tailored websites, country-specific domain names for websites and so on. Otherwise, you may be deemed as "selling" in the EU and therefore GDPR may become relevant.

Item	Question	Response
27	What are the implications regarding US based Universities who keep their data in the US?	See answer to number 5.
28	What authority will a EU govt have in accessing a fine on an American company for violation of GDPR? And what leverage do they have to collect it?	See answer to number 3.
29	What of a student applying to a US institution on a US based website?	See answer to number 5.
30	Who do you think will be the entity to enforce this?	If you are processing GDPR-relevant data, you will need to register with a Data Privacy Regulator in an EU country eg the UK. They will then be the enforcer for any data breach.