1. Have you ever been in a situation where the security or confidentiality of the personal data of our European customers, partners or employees might be compromised? Where your desire to process such data quickly and efficiently may conflict with the need to fully protect individual privacy, as required by European Union law?

2. It happens to many of us and it can be very stressful as we struggle with making the best decision.
3. Imagine that a small number of records of a European Union (EU) customer—maybe only a hundred or so—are being processed by employees in your department. While they are working, one of your processors notices something and asks you if some of the data may have been acquired without valid consent from the individuals involved. You quickly discover there was no consent given.

4. Do you immediately report this issue and risk exposing our organization to potentially serious fines by doing so? Or do you spend some extra time trying to determine if there are other bases for processing the data, potentially creating damaging business delays?
5. It can feel like a no-win situation.

6. The good news is that by the end of this brief video, you’ll have the tools to confidently make the best choice in these kinds of situations. You’ll make the right choices for both yourself and for the organization, avoid potential fines and legal consequences, and feel a whole lot better in the process.
7. The first step to understanding the EU’s privacy law, called the General Data Protection Regulation, or GDPR, is being able to DEFINE what it is.

8. The GDPR regulates how businesses must handle the personal data of individuals (students, customers, employees, etc.) living in EU countries—no matter where the businesses are located. This is to ensure that the personal data we process will be managed lawfully and kept confidential and secure.
9. There are several lawful bases for processing data. These include:
   • Having consent to process the data from the individual to whom it pertains.
   • Having a requirement to process the data in the fulfillment of a contract.
   • Having a legal obligation to process the data.

10. • Being in a situation where there is a vital interest to protect an individual’s life.
    • Performing a task relating to the public interest for a government agency or other entity.
    • AND Whenever processing is necessary to the legitimate interests of our organization or a third-party affiliate.
11. Our goal is to ensure that data is secure, from the time it is collected, through its transfer to and from customers or third parties, until it is destroyed when it is no longer current or needed.

12. The law includes many specific requirements, so it is imperative that all employees who handle personal data attend comprehensive training.
13. Once we know what the GDPR is, what’s next? Well, we have to UNDERSTAND our responsibility for following the requirements of this privacy law in the course of our daily work. Some examples include making sure that we have a lawful basis to process the data; making sure that individuals are able to access their data and understand how it is being used; and making sure that those individuals have the opportunity to have their data erased, upon request, once their data is no longer needed.

14. The exceptions to this would include when data is needed to fulfill a legal obligation; for reasons of public interest in the area of public health; or for archiving certain historical research, scientific or statistical information.
15. It is important that we only process personal data for the purposes for which consent was granted or for which there is another lawful basis for processing, that we not transfer data to another entity for sub-processing without ensuring that entity also complies with GDPR requirements and that we always protect the security of personal data.

16. The last step is making sure that, whenever we encounter a situation where there is a potential GDPR violation – such as a data breach – or a request by an individual for his or her data, we REPORT it to our Compliance Officer or Data Protection Officer IMMEDIATELY. This way they can notify the Supervisory Authority without undue delay and not later than 72 hours after becoming aware of it, as required by the GDPR.
17. Failing to adhere to the requirements of GDPR can subject our organization to legal action and potentially serious fines. Reporting also helps our organization take the necessary steps to preserve the confidentiality of the data and investigate and correct the conditions leading to the violation or breach.

18. In summary, we must be able to DEFINE what the GDPR is, we must UNDERSTAND what is required of us, and we must REPORT any violation or breach situation to our Data Protection Officer, Legal or Compliance Office immediately. Three simple steps to confidently making the best decision.
19. Back to the situation involving the consent for data use, it’s now probably pretty clear that, because we don’t have consent from the individual, you should take the time to investigate if there are any other legal bases for our organization to process the data we have.

20. If there are no other bases by which to legally process the data you have, you will need to immediately report this situation to your Data Protection Officer or the Compliance Office so it can be addressed, including notifying the proper authorities and individuals as appropriate.
21. In the short run, it may feel like you’re creating damaging business delays by taking extra time to investigate other bases for processing the data, but in the long run you’ll avoid the potential consequences of violating the law, and your reputation for doing the right thing among your colleagues will remain intact.

22. Now, doesn’t that make you feel better already?
23. If you have any questions about the GDPR, our company’s data privacy and security policies, please contact our Data Protection Officer, Legal, Ethics or Compliance office (GDPR@duke.edu). We’re here to help.

For more questions about GDPR or any other privacy or compliance matter, please contact Duke Privacy (GDPR@duke.edu)