TeachPrivacy

A Guide to GDPR Training

by Daniel J. Solove

Introduction

With the powerful new EU General Data Protection Regulation (GDPR) and huge potential fines looming on the horizon, organizations are scrambling to step up their privacy programs to become compliant.

The GDPR requires workforce privacy awareness training.

I have spent a lot of time reviewing the training requirements and thinking about training in light of these new developments. Below is some information and advice about global privacy awareness training in light of the GDPR.

GDPR Privacy Training Requirements

Under Article 39, the GDPR includes among the tasks of the Data Protection Officer (DPO) “awareness raising and training of staff involved in the processing operations.”

Under Article 47, in connection with Binding Corporate Rules (BCRs), the GDPR requires “the appropriate data protection training to personnel having permanent or regular access to personal data.”

Training is also required by the US-EU Privacy Shield Framework.

The GDPR doesn’t say a lot more about what training should entail. It doesn’t specify the topics that should be included.

I have thought extensively about this issue, and I believe that the training should focus around the Fair Information Practice Principles (FIPPs) as covered by the organization’s privacy policy. Because of the GDPR’s requirements as well as requirements in various laws and regulations in the US and around the world, the privacy policies of many global companies have a surprising amount of similarities — at least at the level that the general workforce needs to know.

The goal of the GDPR training requirement is not to make the workforce experts on the GDPR. Training on the mechanics of the GDPR should be given to a smaller subset of employees who have advanced privacy roles or must deal extensively with issues involving knowledge of GDPR. Regarding the larger workforce, the goal of creators of the GDPR is to improve the way privacy is protected in organizations. Training should thus focus on the role of the workforce in data protection.

Key Elements to GDPR Training

I recommend avoiding getting bogged down in the details of each specific law or rule and to focus on privacy conceptually. By this, I don't mean that training should be overly theoretical and abstract. To the contrary, it should be practical. But the core of the training should focus on the three dimensions:

(1) Motivation: Why should people care?

(2) Definition: What is personal data?

(3) Responsibilities: What should people know about the way the organization handles privacy? What should people do in their jobs to protect data?

Motivation

If people don't care, they won't pay attention and won't change their behavior. People need to understand why privacy matters and the concrete implications that violations of privacy can have on individuals, on the organization, and on the workforce members involved in a violation. People pay a lot more attention when they are told why they should be paying attention.

Definition

People need to know what data is covered. People must learn roughly how to identify personal data and sensitive data. A challenge here is that the GDPR has a definition of personal data that is different from how US law defines it. US law defines it in many different ways.

People don't need to know each particular definition — otherwise, their heads would spin. The key goal here is to get people to understand that a lot of data that they might not think is personal data in fact can be personal data. Data that alone is not identified to a particular person can be combined with other data and become identified to that person. So it isn't possible to provide a comprehensive list of all personal data.

My strategy here is to deepen people's understanding and teach them enough so that they ask when they are uncertain and avoid making false assumptions.

Responsibilities

People need to be taught what they should know about how an organization handles its responsibilities for protecting data as well as their role in the process. This can be accomplished by teaching people what protecting privacy entails more conceptually. By this, I mean that training should focus on the Fair Information Practice Principles (FIPPs). The FIPPs are the backbone to most privacy laws, and despite all the differences in privacy laws around the world, the FIPPs have widespread consensus.

What FIPPs should be discussed?

FIPPs Regarding Data Collection – principles about lawful and limited data collection.

FIPPS Regarding Data Processing and Use – principles such as data quality, limited access, confidentiality, data minimization, purpose specification, and security.

FIPPs Regarding Individual Knowledge and Participation – individual rights such as access and correction, as well as the obligation to provide notice to individuals. Consent should also be covered, and the training should note the range of different approaches and which are used under which circumstances.

FIPPs Regarding Transfer and Sharing – sharing data across borders or with third parties.

FIPPs Regarding Accountability – internal policies and procedures for ensuring data protection; the role of the DPO (or CPO).

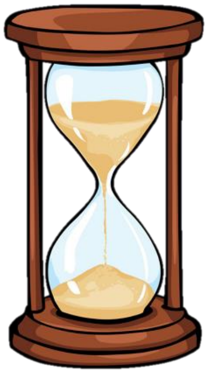
In the coverage of the FIPPs, the Privacy Shield principles will get covered, such as notice, choice, and access (individual knowledge and participation); security, data integrity, purpose limitation (data processing and use); and onward transfer (transfer and sharing).

An organization's policies are typically built around the FIPPs. These policies (and BCRs if the organization has adopted them), should be consistent with the GDPR and the privacy laws in all countries where the organization does business. The FIPPs are where the circles of the Venn diagram all intersect. If trainees understand them, then they have a solid grasp of what it means to protect privacy.

Right to Data Portability

Right to Erasure

Length of Training



The GDPR, as akin to most privacy laws, doesn't specify any particular length for the training. Obviously, training for just a few minutes wouldn't be sufficient, but training does not have to go on for hours.

A common mistake I see in training programs is that they are often too long and bombard people with a lot of information they don't need. The human attention span is very short. What matters more than time is the content of the training and how effectively and memorably the information is taught.

Frequency of Training

There is no definitive answer, as the GDPR, like most laws, doesn't say. The most common practice is to do the training annually.

People forget quickly. I personally love a sustained and periodic awareness campaign, one that has short training bursts each quarter or every two months. But more periodic training might be a challenge for many organizations.

Consequences for Inadequate Privacy Awareness Training

The consequences of inadequate privacy awareness training are bad. Very bad. Inadequate training can lead to more privacy incidents, which can damage an organization's reputation. There are big fines. GDPR's potential fines are gargantuan. And, there will be a cavalcade of regulators from various US federal agencies and state attorneys general and the EU and other countries. In short, it's a world of pain!

Inadequate training is low hanging fruit to a regulator. It's an easy thing that regulators can use to find fault. Inadequate training is one of the most common things that I've seen regulators go after. I expect enforcement of the GDPR to be the same. Lack of training shows lack of respect for the law, and what regulators hate most is when they sense organizations aren't respecting the law.

So I strongly recommend: Don't make it easy for the regulators to find fault. Don't make their fines bigger. Don't let your organization be an easy target. The choice is simple: Train . . . or pain!

Training for GDPR vs. BCRs and the Privacy Shield

The GDPR covers more organizations than BCRs or Privacy Shield, as many organizations fall under the GDPR's wide scope. Under Article 3, the Regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

BCRs and the Privacy Shield are mechanisms for transferring data about EU citizens to the US. An organization can do business in the EU without transferring personal data to the US. If they want to transfer personal data about EU citizens to the US, they must use one of the mechanisms for doing so: (1) BCRs, (2) Privacy Shield, or (3) model contracts.

So those organizations that gather data about EU citizens will be covered by GDPR's training requirement. Those organizations that transfer data about EU citizens to the US will also be covered by the training requirements for BCRs or Privacy Shield.

The content of the privacy awareness training for the GDPR, Privacy Shield, and BCRs will overlap a lot. The main difference is that for Privacy Shield, the training should touch upon the Privacy Shield principles. Because these principles are designed to protect data in light of GDPR, the privacy awareness for GDPR and Privacy Shield need not diverge too much. For BCRs, the awareness should be on the rules that an organization adopts, but these, too, will need to be consistent with GDPR.

About the Author

Professor **Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world's leading experts in privacy law, Solove has taught privacy and security law for 15 years, has published 10 books and more than 50 articles, including the leading textbook on privacy law and a short guidebook on the subject.

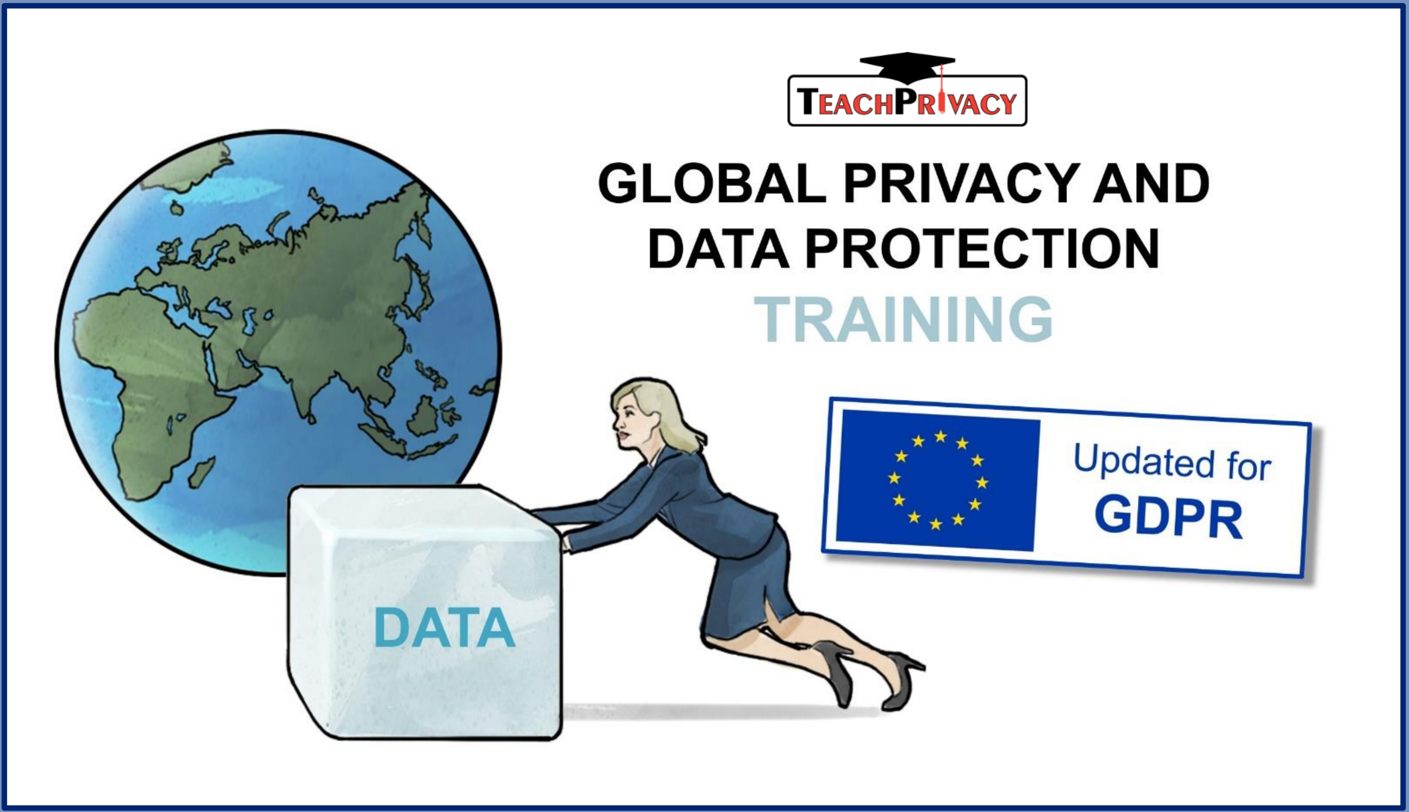
His LinkedIn blog has more than 1 million followers.

Professor Solove organizes many events per year, including the Privacy + Security Forum, Oct. 4-6, 2017 in Washington, DC.

About TeachPrivacy

TeachPrivacy was founded by Professor Daniel J. Solove. He is deeply involved in the creation of all training programs because he believes that training works best when made by subject-matter experts and by people with extensive teaching experience.

TeachPrivacy has a library of nearly 100 training courses that cover a wide array of privacy and security topics including global privacy, EU privacy, the life cycle of personal data, PII, Privacy by Design, HIPAA, FERPA, PCI, phishing, social engineering, and many others.



www.teachprivacy.com