



While we are not IT experts, and do not play them on TV, occasionally IT and compliance merge. This is one of those times, mostly due to the volume of questions we have been receiving on whether, and how, the European Union’s General Data Protection Regulation (GDPR) impacts financial institutions. The GDPR became effective on May 25, 2018. As its name implies, it is not a U.S.-based regulation. So, why the fuss? Well, if your institution falls under the GDPR, you could have significant compliance responsibilities to undertake, administer and maintain.

What’s the gist of the rule? Essentially, the regulation grants rights and protections to the EU’s citizens with respect to their personal information. “Personal information” could include the normal information you obtain to identify a customer (e.g. name, address, social, date of birth), but could also extend to items like passport information, email addresses, photos, usernames, passwords, etc.

The question is: Do you obtain, retain, process or otherwise handle personal information for citizens of the EU? The first place you are likely going to look is at your current customer base. Any time you collect request materials for a BSA Exam or a BSA audit, you are asked to provide a listing of customers who are not U.S. citizens and those who reside outside the U.S. Which of these customers are U.S. citizens residing outside the U.S. and which of them are actually citizens of the EU? You’ll want to focus on those who are actually citizens of the EU.

If you go through this exercise and don’t identify any customers who are citizens of the EU, you’re not done. You’ll have to review other methods through which you may obtain personal information of EU citizens. Examples may include, but not be limited to:

- Tracking cookies attached to your website.
- Prepaid card offerings.
- Online account opening platforms.
- Online application platforms.
- Withdrawn, rejected or otherwise non-originated transactions.

If you find that you have collected, currently house or retain any personal information for EU citizens, you will need to address your GDPR compliance responsibilities. MetaCompliance has a free, downloadable version of [GDPR for Dummies](#) that walks you through compliance responsibilities once you have determined that you have – in whatever capacity – personal information for EU citizens.