



An individual's right to manage personal data and to understand how organizations are using that data is clearly a hot topic and one that is more visible in light of the recent Facebook data privacy scandal.

GDPR provides a timely insight into what data privacy rights are and how far we all need to go to enact effective management of personal information.

Our perspective on the European Union's General Data Protection and Regulation (GDPR)

What is GDPR?

In January 2012, the European Commission set out plans for data protection reform across the European Union (EU) to make Europe 'fit for the digital age'. Almost four years later, agreement was reached on what that involved and how it will be enforced. And the implementation date of May 25, 2018 is now upon us.

How does this European Union legislation impact U.S.-based organizations?

GDPR applies to any organization operating within the EU, as well as **any organization outside of the EU that offers goods or services to customers or businesses in the EU**. If your company, association, or non-profit provides services to or retains data on members, users, sponsors, or other individuals based in the EU, you must comply with GDPR requirements. Among other things, this includes data such as records in your Association Management System (AMS) for current or former members, old meeting registration records, or an individual's continuing education history.

What does GDPR include?

The regulation provides individuals with:

- Control over their rights to data collection, and the use and disclosure of that personal data.
- The right to obtain information about whether - and how - their personal data is being used.
- The right to 'opt-in' to allow use of their data.

Companies, associations, and nonprofits are required to:

- Give prompt notice of data breaches.
- Document their standard practices for processing data.
- Provide a method for receiving, managing, and responding to an individual's request about his or her personal data.

What rights does GDPR grant to individuals?

The regulations state that an individual has the:

Right to be forgotten: An individual shall have the right to obtain from the company or organization the erasure of personal data concerning him or her without undue delay.

Right to restriction of processing: An individual shall have the right to obtain from the company or organization restriction of processing where accuracy is challenged, deletion is not desirable, or legal questions arise.

Right to data portability: An individual shall have the right to receive the personal data concerning him or her, which he or she has provided to a company or organization, in a structured, commonly used and machine-readable format.

Challenging Implementation Questions

Does 'ALL the information' about an individual really include information like membership records, personal preferences, mailing lists, purchase history, education records, conference attendance records, committee participation, forum and blog posts, social media activity, email history, subscriptions, job bank postings, responses, and contact preferences? *Yes.*

If someone requests to be forgotten, does that include forum posts, purchase records for conferences, bookstore items, continuing education, and webinars? *Yes.*

These two questions alone illustrate the magnitude of these regulations and the significant challenges this represents for our clients.

Summary

No matter what U.S. legislation is enacted to address GDPR-like privacy issues, it is certainly in an organization's best interest to move toward 'privacy by design' – building systems and access points to help users manage their online footprint.

As a result, data mapping and data governance will be the first areas of focus as U.S. entities start moving toward protecting an individual's personal information.

It is all about building confidence with the public. And we will all be much more accountable.

What should you do now?

Here are eight action items Potomac Digitek is recommending to our clients.

1. Conduct a Risk Assessment – Document where all of your data resides by creating a data map.
2. Assign a contact - Make someone accountable for this activity (GDPR calls this a Data Protection Officer or DPO).
3. Create a Data Protection Plan – Review and document the measures you are taking to protect an individual's information.
4. Implement measures to mitigate risk – Understand where your data resides, who has access to it, how is it used, and how long you keep it (generally referred to as 'data governance').
5. Test incident response plans – How would your organization handle a security breach?
6. Create a Plan to report GDPR compliance if challenged – Document your GDPR activities, policies, and procedures.
7. Update your website's public privacy policies.
8. Set up a process for ongoing assessment.

Potomac Digitek has carefully researched the new GDPR requirements and is ready to assist our clients with [GDPR Response Packages](#) to help address these action items and other emerging privacy by design initiatives. Please contact your account executive to discuss what level of support your organization may require.

Ultimately, good data management practices are going to become increasingly important to users and management as GDPR and U.S. regulations evolve.

Becoming a good data steward reaffirms that your members can trust you, and that's a valuable benefit.

For more information on GDPR, [click here](#) to access the EU General Data Protection Regulation documentation.

Other News and Notes

The **American Academy of Craniofacial Pain** is committed to the relief of craniofacial pain, temporomandibular disorders and dental sleep related disorders and supporting the advancement of education, research and dissemination of knowledge and skills in these areas. Click here to visit [their new Website](#).

The [Kids After Hours Website](#) went through a few upgrades this month as we greatly reduced the time it took for parents to register their children for after-school activities and camps. Quick improvements to online processes will make a big difference for busy parents. We've also instituted an online waiting list, allowing staff to keep close tabs on interested families and availabilities.

Potomac Digitek was a guest at the **American Council of Engineering Companies** 's 2018 Engineering Excellence Awards Gala. The formal affair was held at the Wardman Park Marriott to recognize 36 outstanding engineering achievements. The submission, evaluation, and selection process for candidate projects is managed annually via software created by PODI. [Click here](#) for information about this year's award winners.

Thank you for your time. More tools and tips from Potomac Digitek are already in the works for next month's newsletter!

Paul Finkel

President
Potomac Digitek
301-590-2770
820 W. Diamond Ave., Suite 200, Gaithersburg, MD 20878