EU Privacy Regulations' Impact on **Information Governance**

Two recent European Union (EU) privacy actions – The General Data Protection Regulation and the invalidation of the U.S. Safe Harbor Framework – as well its ruling about EU citizens' "right to be forgotten," are changing the way organizations in other countries must govern the personal information of EU citizens. These actions also may be providing the urgency required for some organizations to initiate or improve information governance (IG) programs, bringing IG to the forefront of organizational strategy.

Teresa Pritchard Schoch, J.D., IGP, CRM, CIPP, CIP

The recent swift passage of the European Union (EU) General Data Protection Regulation (GDPR) – a comprehensive update of its 1995 Data Protection Directive – and the October 2015 EU invalidation of the U.S. Safe Harbor Agreement, which had allowed U.S. companies to self-certify that they provide adequate protection for personal data transferred to them from other countries, have U.S. organizations scrambling to determine what this means for the way they govern EU citizens' personal information.

The following provides information about the new GDPR and the Safe Harbor Agreement invalidation that will help readers determine their course.

The GDPR

The GDPR's chief effects on U.S. organizations are that it:

- Applies to EU citizens' personal data, regardless of where it is collected, stored, or processed – whether inside or outside of the EU
- Requires that data subjects give explicit, informed consent before their data may be processed
- Defines personally identifiable information (PII) as any information that if combined with another available piece of information would allow an individual to be identified
- Requires organizations to notify those whose data has been breached within 24 hours of the breach

For more details about the GDPR, see the sidebar "Major Provisions of the EU General Data Protection Regulation."

The U.S. Safe Harbor Framework

The EU invalidation of the Safe Harbor Agreement, whose seven principles for handling EU citizens' PII in accordance with EU law were developed by the EU in an agreement with the U.S. Department of Commerce, was based on the U.S. government's ability to access private data in the United States without any recourse available to EU citizens.

It held that an EU citizen has a right to bring action against a U.S. company if he or she believes that his or her privacy is being jeopardized, regardless of that organization's certification under Safe Harbor. (See the seven principles of the Safe Harbor Agreement in the sidebar "The U.S. Safe Harbor Framework.")

On October 16, 2015, the EU's Article 29 Working Party, which includes representatives from all EU Data Protection Authorities, released its guidance on the judgment of the European Court of Justice indicating that enforcement against U.S. companies will start at the end of January 2016.

On October 20, 2015, the fallout from the EU's decision continued, as Israel announced that it also considers the Safe Harbor Framework invalid for future data transfers. Other nations will likely follow suit, as Europe has seemingly established itself as the global leader in defining privacy rights of the individual.

Impact on U.S. Data Laws

While some U.S. federal statutes address private information – for example, the Privacy Act of 1974 (5 U.S.C. §552a), the Gramm-Leach-Bliley Act (15 U.S.C. §§6801–6809), the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.), and the Children's Online Privacy Protection Act (15

Major Provisions of the EU General Data Protection Regulation

Scope: EU law would apply to EU citizens' personal data, even if the data is collected, stored, processed, etc. outside of the EU.

Definitions and conditions to consent: Data subjects would have to give explicit, fully informed consent to anyone processing personal data.

Profiling: Restrictions on profiling would mandate a highly visible right to object.

Right to compensation: EU citizens would have the right to seek compensation for monetary and nonmonetary damages from any data processing considered unlawful by the EU.

Sanctions: Fines for noncompliance could reach 100 million euros or 5 percent of a firm's annual worldwide business, whichever is greater.

Permission: An organization must obtain permission from an EU DPA and inform the affected person before complying with a non-EU country government's request to disclose personal data processed.

Breach notification: The notice of breach requirement is set at within 24 hours of breach.

PII definition: Personally identifiable information (PII) includes personal information as any information that if combined with another available piece of information would allow the identification of an individual. Information does not need to be assimilated to be considered PII.

"Sensitive data" definition: The EU definition of "sensitive data" relating to background such as religion, national origin, medical history, sexual orientation, etc. is more specific than before. Holding this type of information will require more stringent security, since the impact of dissemination is considered more egregious.

U.S.C. §§6501–6506) – the U.S. federal government has not yet approached the issue of individual privacy in the electronic age at the same intensity as the EU. Instead, U.S. states are addressing duties applicable to the handling of private information.

The U.S. Safe Harbor Framework

In 2000, the EU entered into an agreement with the U.S. Department of Commerce to develop a set of principles against which U.S. companies could self-certify that they would adhere to the following seven principles when handling information that contained personally identifiable information (PII):

Notice: Organizations must notify individuals about the purposes for which they collect and use information, the types of third parties to which it discloses such information, and how an individual can limit those activities.

Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, an affirmative or explicit (opt in) choice must be given.

Onward transfer (transfers to third parties): To disclose information to a third party, organizations must apply notice and choice principles.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate unless the burden of providing access would be disproportionate to the risks.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: There must be (a) readily available and affordable independent recourse mechanism(s) so that each individual's complaints and disputes can be investigated and resolved and damages awarded, where applicable.

On October 6, 2015, the European Court of Justice invalidated the Safe Harbor Agreement (Case C-362/14, *Maximillian Schrems v* [Irish] *Data Protection Commissioner)* without providing a grace period for the 4,200 U.S. organizations that had self-certified under the agreement.

At present, most states define *PII* as an individual's first name (or first initial) and last name *in combination with* one of three types of information: Social Security number, driver's license or state identification card number, or financial account or credit card number, with or without any required code/number/password that would permit access. This is less restrictive than the DGPR, which says it is PII even if it is not combined with the other available piece of information.

Most states also specifically include medical information, electronic signatures, taxpayers' information, and biometrics. (Georgia and Maine include any information sufficient to be used for identity theft.)

In 2003, California became the first state to require notification of the breach of *unencrypted* personal information by any governmental entity or commercial enterprise doing business in that state. California law requires disclosure to an individual "any time there is a reasonable belief that there has been an unauthorized acquisition of computerized data that compromises the security, integrity or confidentiality of an individual's information. Disclosure must be made as expediently as possible." (Cal. Civ. Code §§56.06, 1785.11.2, 1798.29, 1798.82; Cal. Civ. Code. §§1275–1289.5.)

Within days of the EU's court case that invalidated the U.S. Safe Harbor Framework, California enacted the Electronic Communications Privacy Act, heralded by the American Civil Liberties Union as a landmark victory for digital privacy. (Among other things, it requires law enforcement to get a warrant from a judge before accessing electronic information about who people are, where they go, who they know, and what they do.)

With 47 states having previously enacted data breach laws modeled on California (and Massachusetts) laws, U.S. state laws will probably continue to reflect the privacy requirements established by the EU in the upcoming months and years.

Impact on Information Governance

These two actions in the EU may help us build the business case for information governance (IG), providing the urgency required to bring the stakeholders to the table and the numbers to show the risks and costs of improperly governed information. Protection of privacy becomes the starting point for the discussion, the camel's nose in the tent to bring IG to the forefront of organizational strategy.

Perhaps the greatest threats to privacy are data breaches. 2015 was the year of the U.S. data breach, as major U.S. retailers (e.g., Neiman Marcus, Target, Michaels, Home Depot), financial institutions (e.g., Citibank, JP Morgan), health providers (e.g., Anthem, United HealthCare), and

the federal government (e.g., Office of Personnel Management, IRS) suffered breaches of private information.

The impact of these types of data breaches includes:

- Lawsuits
- Fines and penalties
- Loss of customer loyalty
- Loss of revenue
- Erosion of share price
- Negative publicity
- Damage to "brand equity"
- Damage to company reputation
- Increased operations costs
- Loss of intellectual property

Even a year ago, insurance companies were not concerned about these impacts and considered them remote. Now, premiums are becoming prohibitively expensive, with one insurance company recognizing that risks can be reduced with improved IG. It specified its expectations for organizations that want to maintain their current rates:

- Improved classification scheme
- Improved privacy policy
- Improved records management policy
- Improved system of data deletion

As RIM program components, these are areas all organizations should seek to improve. A mature records management system includes a formal information classification scheme, coordinated with many other security and operations practices, to provide the decision-making tools needed to ensure that the privacy, confidentiality, integrity, and availability requirements of information assets are satisfied based on business needs, ongoing legal actions, and regulatory requirements.

Improving Data Classification

A records management system develops a usable, fully considered, integrated, and supported data classification schema to meet the needs of enterprise security, privacy, and compliance requirements. With properly classified information, the organization can select and apply appropriate security controls to like information – which is especially important for private and confidential information – across the company consistently.

Improving Privacy, RIM Policy

As mentioned earlier, PII under the GDPR is any information that *if* combined with another available piece of information would allow an individual to be identified. It does not need to be assimilated with that other available piece of information to be considered PII. This means that a piece of information an organization would not normally view as a record on its own would need to be treated as PII.

This information would need to be governed according to the appropriate protection and retention requirements. Specifically, under the GDPR, the organization would need to:

- Maintain the data subject's consent for collection and use
- Protect the data from unauthorized access
- Retain the data for the appropriate length of time and dispose of it subject to the EU's limitations on the length of time it can be kept
- House it in a manner that would allow immediate access to it and action to meet the EU's quick data breach notification requirements

Now premiums are becoming prohibitively expensive, with one insurance company recognizing that risks can be reduced with improved IG.

These requirements call for IG protocols that either automatically tag PII as business records or expand the definition of a record to specifically include any information containing PII.

Improving Defensible Disposition

RIM professionals have long wondered what it is going to take for some organizations to realize that "keeping it all" is not a sound retention policy. Even some organizations moving toward storage budgets in the $100 million range seem unable or unwilling to develop a defensible disposition framework that would help reign in their costs and risks.

By diligently identifying the 28%-30% of an institution's information that constitutes *records* (as identified in the 2012 Compliance, Governance and Oversight Council's survey) – that is, information that 1) is necessary for the continuation of the business, 2) could have evidentiary value, or 3) is required to be maintained under statutory or regulatory mandates – the remaining 70%-72% can be defensibly targeted for deletion, enabling greater control over storage growth, decreasing storage needs and costs, and limiting the extent of the damage in the event of a breach.

Because of the heightened responsibility surrounding PII, it will become even more vital for businesses to determine what information meets "defensible disposal" criteria; nonexistent information cannot be breached.

The fact that dark data – which Gartner defines as "information assets that organizations collect, process and store in the course of their regular business activity, but generally fail to use for other purposes" – could contain PII should be a strong motivation for organizations to address defensible disposal to avoid allegations of negligence in PII breaches. But systematic deletion of non-record data needs to be accomplished in a manner that ensures protection of private data, as defined by EU law.

A Triple Threat

The European Court of Justice's 2014 determination that its citizens have the "right to be forgotten" is yet another reason organizations must be mindful about how they collect, protect, and defensibly delete PII. This ruling allows any EU individual to request a copy of any information an organization has that relates to that individual. Any organization that keeps it all without knowing what "it all" is will be unable to meet these requests.

Taken together, the EU's recent activity related to PII triple-underscores the need for organizations to improve their RIM programs. They must be able to 1) meet the requirements of protecting PII under the GDPR in the absence of Safe Harbor and producing PII under the Right to Be Forgotten; 2) protect all data – especially PII – to prevent the catastrophic results of a data breach; and 3) defensibly dispose of data to reduce risks and costs. **END**

Teresa Pritchard Schoch, J.D., IGP, CRM, CIPP, CIP, can be contacted at tschoch@thinkbrg.com. *See her bio on page 47.*