The Complexity Is in the Details

New EU Data Protection Law Promises User Control

feature

Также на русском
www.isaca.org/currentissue

Four years after its introduction, the European Commission has recently come to agreement on the General Data Protection Regulation (GDPR) as organizations around the globe await the details, which should be released soon.

Often described as "fit for a digital age" by its supporters in Brussels, Belgium, the legislation aims to put users in control of their data and harmonize the rules under which private data may be obtained or retained across the 28-nation bloc. The GDPR updates the antiquated 1995 privacy regulation, drafted three years before the founding of Google. In an effort to keep up with technology and address privacy issues important to the European community, the European Parliament came to agreement on the European Union (EU) data protection law in December 2015, with details to be released in the near future and to become enforceable in 2018.

Because this new legislation declares itself applicable to any organization that makes its goods or services available to any part of the EU, it takes little imagination to understand its reach and scope. GDPR is not merely a new version of the 1995 legislation, but a revolutionary new rule set that organizations will need to quickly understand, adopt and comply with or face significant financial consequences.

The fundamental aim of the new regulation is to put users in control of what is stored about them online. "The new rules will give users back the right to decide on their own private data," says Parliament's lead member of European Parliament (MEP), Jan Philipp Albrecht.[1] One prominent feature of the new legislation extends the popular right to be forgotten, a rule active in the EU since 2006, which allows users to demand deletion of their photographs, videos or personal information from any Internet records that allow them to be found by search engines. The right was initially implemented for search engines, but it has now been extended to all web services, including social media sites such as Facebook.

The right to know you have been hacked is a popular component of the GDPR and requires organizations to report to a central authority within 72 hours any data breaches that pose a risk to data owners. Users subject to high-risk breaches are also required to be notified as soon as possible, although the ambiguity of this language causes some to be skeptical of the directive's enforceability.

Critics of the new data-protection regulation take aim at a number of its clauses. One of the most controversial aspects is in the punishment for noncompliance—organizations face fines of up to 4 percent of their annual global revenue for not complying with any part of the GDPR. "Such high sanctions dis-incentivize business and investment," says Intel's global privacy officer David Hoffman.[2] Skeptics are already calling the regulation the latest Silicon Valley shakedown and say it is escalating conflict with technology giants such as Google, Facebook and Microsoft.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Michael Vanderpool, CISA, CISSP
Is an IT auditor with Credit Suisse, based in the city of Wroclaw, Poland. His more than 12 years in information technology experience has been mostly with information security, risk and compliance. With a background in the technology and financial sectors, Vanderpool has performed a variety of IT risk assessments, audits and control reviews for international corporations and banks while utilizing international frameworks such as COBIT®, COSO and ISO 27001. Prior to joining Credit Suisse, Vanderpool worked for UBS and IBM.

Ambiguity in some of the guidelines and language in the GDPR is also a cause for concern. One example is with the requirement that some organizations hire a data protection officer. According to the regulation, small or medium-sized organizations are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity. Under this definition, would companies that conduct background checks be exempt? Such organizations are often targeted by data thieves, and large-scale breaches at this kind of company are not uncommon, but if such organizations define "personnel management" or "recruitment processing" as their core business, they can claim exemption even though they host extensive valuable personal information, sometimes permanently.

"Legal uncertainty and big fines are a toxic cocktail," notes Interactive Advertising Bureau European board member Allan Sorensen.[3] The large, globally calculated penalties for regulation infractions, combined with the (at times) vague wording, cause some to wonder if the regulation is designed more for the EU to make another cash-grab from Google than to protect user data. In response, GDPR sponsor Jan Philipp Albrecht claims, "The only ones who will profit from this law being postponed again and again will be the big data companies from Silicon Valley."

> **"There are clearly many stakeholders caught in the crosshairs of the GDPR."**

Medical research organizations have come out against the regulation, claiming it would slow or even halt their ongoing data-driven research efforts. More than 50 patent organizations and medical research charities have written to MEPs about concerns with overly restrictive data laws. Some organizations claim that the changes to the law may be unworkable at best and illegal at worst, especially for large-scale projects.[4]

Although many medical researchers are content with the latest changes to the regulation's wording, there are clearly many stakeholders caught in the crosshairs of the GDPR. Even organizations making early attempts at compliance with the new rules have their hands full. Each of the 28 bloc nations will interpret the EU regulation independently, and in some cases there is discretionary leeway in defining actual laws. For instance, the minimum age a child can use social networking sites without a parent's express approval must fall between ages 13 and 16, but the specific age can be defined by each country.

The early stated goal of creating a "one-stop shop," i.e., a single point of contact for any complaints about a company, suggests that the offending company's main point of presence in the EU is the country's regulator who would handle the complaint. Due to voiced concerns, however, it is now permitted that any nation's regulator can file a complaint with the main point of presence's regulator, depending on where the complainant resides and where the complaint is filed. As Johannes Caspar, the head of Hamburg's data protection authority in Germany says, "The mechanism laid down in the data-protection regulation establishes a hyperbureaucratic procedure that will lead to more complexity and longer procedures."[5]

Access to one's own data allows users to see exactly which data are being retained by a web site and how they are being used. The right to data portability (which many critics label a boondoggle) allows users to download their personal data and preferences for import and use on another web site. Data portability has been controversial and many claim it neither facilitates data protection nor belongs in the regulation. Its references have already been minimized in the most recent regulation summaries, and many expect it to be left out of the final draft altogether. One scenario illustrating this requirement would involve customers of a shopping web site to be able to download their shopping preferences and upload them to a competitor site. Depending on each shopping web site's product

categories, hierarchies and naming taxonomy, this process, which might sound simple in the halls of Parliament, creates real-world hurdles for technology architects, and critics claim it adds no value to the stated fundamental goal of the regulation to protect user data.

As an illustration of the data portability requirement, imagine owning Pizza Company A, which takes orders online. Customers have an online profile, which contains their address, phone number and order history to make new delivery orders fast and efficient. Customer John Smith calls and demands to be provided with his profile and history so that he can order from Pizza Company B. The new regulations require that the information be sent to him. Does this new process add value to Pizza Company A? Does it serve to protect John Smith's data? And unless Pizza Company B's pizza offerings are exactly the same as Pizza Company A's, the history will serve little purpose to Pizza Company B when it takes his first order. The process does, however, increase John Smith's data exposure (through additional email transmissions) and places a new burden on Pizza Company A, which, according to the new regulations, is required to provide data provision service to (nonrevenue-generating) ex-customers.

The challenge in complying with European Commission directives is well known to technology companies. Since Article 17 of the Data Protection Regulation's release in 2012, technology companies have struggled to maintain compliance with the right-to-be forgotten requirement while still providing their users a positive online experience. For example, eBay has struggled to implement the strict requirement to immediately delete users' data, made exceptionally difficult because of the number of databases in which that user data resides.

Also in the crosshairs of the GDPR is the practice of profiling users, a widespread practice online that allows web sites to gather and categorize information about their visitors, allowing them to tailor the web site experience and present more relevant ads. Beyond just use for advertising though, technology has been used by insurance companies to monitor and reward safe driving behavior and by social media sites to recognize and tag photographs containing the faces of their users. Such implementations will now require consent for each use, and all companies will now be required to disclose to each web site visitor:

- Why users are being profiled
- Into what categories (buckets) they are being sorted
- Who can access the data
- The logic involved in these determinations
- The consequences of such processing

While some of these new requirements are already commonly seen in such disclaimers as, "We use your information to enhance your shopping experience," the required disclosure of the actual logical algorithm used is particularly groundbreaking. As Alvaro Bedoya, executive director of the Center on Privacy and Technology at Georgetown University (Washington DC, USA) Law Center, says, "Right now, so much of our online lives are determined by algorithms that are totally opaque. The right to access the 'logic' behind data processing could be a significant step forward in opening that black box." Technology companies such as Google often view their algorithms as their most valuable trade secrets. The disclosure of specific logical formulas is viewed by many as a thinly veiled attempt by the European Commission to see behind the curtains of how these companies operate.

The territorial scope of the GDPR remains one of its most controversial aspects. With its stated reach being any organization that makes its goods or services available to any subject in the EU, the European Union could soon be regulating the Internet. Popular web sites such as Google and Facebook will either need to offer a different program to European customers or evolve their global services to become compliant. And with just one infraction of the rules resulting in a potential

Enjoying this article?

- Read ***Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function.*** *www.isaca.org/2015-privacysurvey-*
- **Learn more about, discuss and collaborate on privacy/data protection in the Knowledge Center.** *www.isaca.org/topic-privacy-data-protection*

4 percent revenue fine (for Google this is currently US $3 billion), companies face some difficult decisions in the coming months.

With its stated objectives being "to strengthen privacy rights and boost Europe's digital economy," many critics claim the regulation misses the mark entirely. While there are some components that effectively address privacy concerns, other aspects are extremely expensive and difficult to comply with, leaving technology companies with difficult decisions to make in the coming months when it comes to serving their European customers. Even those who decide to alter their services in order to comply with the new regulation face some daunting challenges in the next 24 months. "The scale and breadth of the EU's changes to privacy rules will deliver unprecedented challenges for business and every entity that holds or uses European personal data both inside and outside the EU," explains Stewart Room, head of data privacy at PwC.[6] "Most companies will be shocked at the scale of the new rules and the work that needs to be done before the laws take effect in two years—it is not much time for the magnitude of the internal changes that will be required."

As is common with European Commission rulings, the regulation will now face additional scrutiny and transposition when the 28 bloc nations absorb the individual requirements into their national laws in the coming months. While the GDPR is scheduled to take effect in 2018, it is not difficult to imagine even further delays if individual member countries cannot reach internal agreement on the required implementation and enforcement of the ruling.

It will be particularly interesting to see the Irish reception of the regulation, as Ireland is the European home to many foreign technology companies. A 2013 criticism of the regulation by the Irish presidency centered on the lack of a risk-based approach in drafting the regulation. Where actual risk is found to be lower, the Irish wanted the amount of regulation to be minimized. The presidency also voiced concern over the "needs of micro, small and medium-sized enterprises (SMEs)."[7]

So, as the 28 bloc nations receive the details of the draft in the coming weeks, no one should be surprised to see further debate about the GDPR, which was initially proposed in 2012. It all boils down to the details, and details have been known to hide unwelcome surprises.

Endnotes

1 European Parliament News, "New EU Rules on Data Protection Put the Citizen Back in the Driving Seat," press release, 17 December 2015, *www.europarl.europa.eu/news/en/news-room/20151217IPR08112/New-EU-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat*

2 Dow Jones Business News, "EU Privacy Law Has Broad Implications," Nasdaq, 17 December 2015, *www.nasdaq.com/article/eu-privacy-law-has-broad-implications-20151217-00441*

3 Dwoskin, E.; "EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies," *The Wall Street Journal*, 16 December 2015, *www.wsj.com/articles/eu-data-privacy-law-raises-daunting-prospects-for-u-s-companies-1450306033*

4 European Parliament, debate transcript, Strasbourg, France, 11 March 2014, *www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-013&language=EN&ring=A7-2013-0402*

5 Fioretti, J.; "EU Data Protection Reform May Promise More Than it Delivers," *Reuters*, 5 January 2016, *www.reuters.com/article/us-eu-dataprotection-idUSKBN0U41CQ20160105*

6 BBC News, "EU Data Laws Threaten Huge Fines," 16 December 2015, *www.bbc.com/news/technology-35110909*

7 Hunton & Williams, "Irish Presidency Reports on Progress of the Proposed EU Regulation," Huntonprivacyblog.com, 26 March 2013, https://*www.huntonprivacyblog.com/2013/03/26/irish-presidency-reports-on-progress-of-the-proposed-eu-regulation/*