GDPR: A sign of what's to come?

LUCY HARR

The EU's General Data Protection Regulation could become a new privacy model for U.S. institutions.

AML. BSA. SAFE. OFAC. Add another ingredient to the alphabet soup: GDPR. Although the European Union's (EU) General Data Protection Regulation—or GDPR—may not be in your credit union's compliance cupboard now, the regulation is taking privacy protection to a new level.

GDPR went into effect in May 2018 and aims to harmonize data privacy laws within the EU.

With 133,000 members in 200 countries and territories, United Nations Federal Credit Union not only serves members in Europe, it has offices in Europe and European employees.

As a result, the Long Island City, N.Y.-based credit union realized GDPR would affect its operations.

"Every country had different requirements regarding the use of data," says Manisha Shah, first vice president, deputy general counsel, at the $5.5 billion asset credit union. "GDPR addresses the lack of coordination that existed."

In Europe, privacy is seen as a fundamental right, which is different than the view held in the U.S. However, that's beginning to change.

"Until recently we were giving away information in the U.S.," says Lee Painter, principal in the CliftonLarsonAllen information security services group. "And when it was revealed what Facebook and Google were doing with data, we weren't too happy about it."

Facebook and Google data scandals were not the genesis for GDPR. But tech companies' proven appe-

tite for customer data contributed to the success of lobbying efforts to pass it, Shah says.

The impact on credit unions

Strict privacy laws already exist in the U.S. for financial institutions and health-related organizations, says Lance Noggle, CUNA's senior director of advocacy and counsel.

For example, severe penalties await those failing to comply with the Graham-Leach-Bliley Act, which requires financial institutions to explain how they share and protect customers' private information, and the Health Insurance Portability and Accountability Act. Violations of either can result in steep fines or imprisonment.

But merchants and other organizations may not suffer any financial consequences for data breaches—at least not yet.

GDPR marks a major shift in privacy regulations and it's changing the privacy landscape, Painter says. Any company that does business in the EU or with EU citizens may be affected.

Misusing or inadequately protecting an individual's data could result in strict monetary penalties.

But how does GDPR affect credit unions?

For most credit unions, it shouldn't impact operations now, says Andrew Price, regulatory counsel for the World Council of Credit Unions.

"You probably need something more substantial than a member's incidental use of an ATM in the EU," Price says. "But credit unions operating in Europe—those serving the military or airlines—may need to be in compliance."

'CREDIT UNIONS OPERATING IN EUROPE—THOSE SERVING THE MILITARY OR AIRLINES—MAY NEED TO BE IN COMPLIANCE.'

ANDREW PRICE

To figure out where to start on its GDPR compliance plan, United Nations Federal hired an EU-based law firm to conduct a readiness assessment.

"As a credit union, we were used to looking at data with a focus on security," Shah says. "We wanted outside counsel to apply a different lens to focus on data privacy."

From there, the credit union conducted a gap analysis to understand what it would take to comply with GDPR and devised a project plan that included creating a data map. This identified the credit union's data and the flow of that information.

"We realized we needed to explicitly state, 'We are in the United States,'" Shah says.

United Nations Federal also had to identify all vendors who had access to their data and ensure their compliance through contract addenda.

Finally, the credit union updated its privacy policy and account documentation, added a cookie disclosure on its website, and trained key individuals to respond to data subject access requests.

While GDPR may not affect current operations at your credit union, it's not something credit

Focus

- **GDPR** may set off a wave of new privacy regulations in the U.S.
- **Treat GDPR** as a standard against which to measure your own data security practices.
- **Board focus:** Educate directors and members about the value of their personal data and why the credit union may need to be more restrictive.

GDPR

unions can ignore.

"Strictly speaking, GDPR is not a direct influence on most domestic credit unions and their everyday operations," says Jeffery Lauria, vice president of technology at iCorps Technologies, an information technology consulting and outsourcing firm.

"That said, GDPR can be treated as a standard against which to measure your own data security practices," he says. "Considering GDPR is currently one of the most restrictive data policies in the world, other entities—be they businesses or governments—will look to GDPR as a model to follow."

California privacy impacts

That's already the case in Califor-

PREPARE FOR AN INCREASED PRIVACY FOCUS

To prepare for the possibility of more stringent data privacy requirements, Rita Fillingane, vice president, research and collaboration, at the California and Nevada Credit Union Leagues, suggests taking these steps:

›**Determine** when and what personal information the credit union or credit union service organization (CUSO) may be collecting about covered consumers.

›**Verify** how you store personal information and for how long.

›**Inventory** all third-party providers that may access or obtain personal information while providing services to the credit union. Verify that contractual requirements are consistent with the California Consumer Privacy Act and modify them if they do not comply with the law accordingly.

›**Establish** a toll-free telephone number and web address for consumers to submit opt-out requests. If providing a web link, make sure the link does not violate other laws, such as the Americans with Disabilities Act.

›**Prepare** consumer-facing notices.

›**Update** the credit union's or CUSO's policies.

›**Create** a process for deleting any personal information not covered by other state and federal privacy requirements.

›**Develop** a process on how to respond to consumers' inquiries regarding their personal information.

Jeffery Lauria, vice president of technology at iCorps Technologies, offers additional tips regarding General Data Protection Regulation (GDPR) compliance:

›**Conduct** a risk assessment and inventory and review your consumer touch points. Documenting workflows is important, as is how your applications store data with other services.

›**Ensure** your opt-in language is unambiguous and adheres to GDPR consent standards.

›**Focus** on user data. Data transfers must be made in a secure and private manner, preferably encrypted.

›**Document** all compliance efforts. GDPR requires maintaining clear user records, especially demonstrations of consent. Keep a thorough, time-stamped record of all relevant documents.

›**Amend** your data protection plan. Do your standard practices align with those put forth by GDPR? Have you checked that your mobile devices are also compliant? Implement controls and processes for what your credit union says it does with data and how you protect it.

›**Consider** hiring a data protection officer to assist with preparation, such as testing incident response plans.

›**Leverage** the cloud. Cloud application security services can identify applications and services used by all devices on your network, allowing you to oversee your users' activity.

›**Implement** unified threat management, which provides more centralized security management for streamlined oversight.

›**Conduct** a data audit. Data often is stored across a number of different platforms. Try to migrate your members' information to a few secure platforms with built-in security and automatic back-up.

nia, which passed the California Consumer Privacy Act (CCPA) of 2018. The new law, which becomes effective Jan. 1, 2020, largely reflects the GDPR protections and has comparable consequences.

"The CCPA will affect credit unions and credit union service organizations (CUSOs) that meet the definition of 'business' under the CCPA," says Rita Fillingane, vice president, research and collaboration, at the California and Nevada Credit Union Leagues.

The CCPA defines "business" as an organization doing business in California that collects consumers' personal information, directs how it's used, and meets one of three thresholds:

1. It has annual adjusted gross revenues over $25 million.

2. It buys, receives, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices annually.

3. It derives at least 50% of its annual revenues from selling consumers' personal information.

Credit unions and CUSOs meeting this business definition will be required to comply with any CCPA provisions outside the scope of the Gramm-Leach-Bliley Act and the California Financial Information Privacy Act.

Credit unions and CUSOs not in compliance with the CCPA regulations could face potential regulatory penalties and litigation by private citizens.

"In short, if a business is subject to CCPA, any data breach could expose it to significant monetary penalties," Fillingane says.

Many experts believe similar regulations will eventually be instituted throughout the U.S.

"GDPR is a sign of things to come," Lauria says. "While GDPR is not always applicable to domestic firms, the degree of regulation will be a reality for U.S.-based businesses sooner rather than later.

"By embracing GDPR-like standards, your credit union will be better positioned to weather coming regulatory changes because you will have already adapted," he continues. "That means you will be ahead of the competition and avoid down time if any complications should arise."

'IF A BUSINESS IS SUBJECT TO CCPA, ANY DATA BREACH COULD EXPOSE IT TO SIGNIFICANT MONETARY PENALTIES.'

RITA FILLINGANE

Third-party compliance

It's not enough for your credit union to be compliant. Lauria advises credit unions to check with third-party partners to make sure they're complying with GDPR regulations.

As part of its compliance plan, United Nations Federal includes a GDPR addendum in its vendor contracts. The addendum also addresses NCUA's Part 748, which U.S. vendors know they cannot avoid.

The rule requires a credit union's information security program to be designed to ensure the security and confidentiality of member information.

It also calls for "a credit union's service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines."

On the other hand, some vendors also are adding GDPR clauses into contracts because they're concerned about their GDPR compliance liabilities.

"If you find these in your vendor contracts," advises WOCCU's Price, "you need to talk to counsel."

CO-OP Financial Services is working with its clients who determine they need to be GDPR- or CCPA-compliant to meet their needs and those of members, says Layna Braze, enterprise compliance manager.

"CO-OP Financial Services has implemented an information security program designed to protect CO-OP systems and data," Braze says.

"The program is aligned with internationally and nationally recognized best practices in information security. This includes the protection of customer information, the systems that hold customer information, and how customer information is transmitted," she says.

Although the new privacy rules are complex, it comes down to knowing what data you have, where it lives, and how you're going to protect it.

"In general, credit unions need to

have a better idea of what type of member data they are maintaining, handling, and sharing," says Jeff Owen, chief operations officer for Rochdale Paragon Group.

"While we are not aware of any specific fines, lawsuits, or findings pointed at credit unions at this point, it seems certain these types of regulations and rules will begin impacting credit unions in the near future," he says.

As a financial cooperative, Lauria says it's imperative that credit unions communicate to all parties the value in adopting GDPR-like data policies.

"Educate your board and members about the value of their personal data and why the credit union as a whole wants to take a more restrictive approach," he says.

"Most of the changes will be internal, and the majority of your members will not see them. However, it is the board's job to empower members to take control of their personal data and communicate how the credit union is taking similar precautionary steps."

Resources

- CUNA compliance resources: *cuna.org/compliance*
- CliftonLarsonAllen: *claconnect.com*
- CO-OP Financial Services: *co-opfs.org*
- iCorps Technologies: *icorps.com*
- Rochdale Paragon Group: *rochdaleparagon.com*
- World Council of Credit Unions: *woccu.org*

CUNA CALLS FOR ROBUST DATA SECURITY STANDARDS

The time has come for new federal protections regarding the use and security of data held by businesses and entities, CUNA says in letters it sent to the House Energy and Commerce Committee and the Senate Committee on Commerce, Science, and Transportation.

The letter to the House Energy and Commerce Committee states:

"Since Americans' personal information has become so valuable in the aggregate to businesses and criminals worldwide, the time has come for new federal protections regulating the use and security of data held by all businesses and entities. Europe's General Data Protection Regulation (GDPR) and California's California Consumer Privacy Act (CCPA) show that foreign governments and states aren't willing to sit on the sidelines and neither should Congress. Action is required to ensure that all Americans can enjoy robust protection of their most important personal data from misuse and theft."

CUNA notes the insteacurrent gaps in data protection and privacy laws hurt consumers and businesses because bad actors can misuse information.

"Although data security is a major issue for credit unions, we realize the problem is much bigger than the financial services industry with robust privacy and data security requirements for all industries becoming increasingly necessary," the letter reads. "The cornerstone of any new privacy requirements should be robust data security requirements for business and other entities that collect consumers' personal information."

CUNA believes any new privacy law and/or data security requirements should:

- **Cover** both privacy and data security.
- **Cover** all companies that collect, use, or share personal data.
- **Be based** on protection of data to prevent from theft and misuse. Disclosure after the fact is important, but it's not a substitute for adequate protection.
- **Provide** mechanisms to address the harms that result from privacy and security violations, including data breaches. Individuals and companies should be afforded a private right of action, and regulators should be able to act against entities that violate the law.
- **Preempt** state law to simplify compliance and create equal expectation and protection for all consumers, with a goal to create a national standard for all to follow.

GDPR