CAPINTECH

How the New GDPR Data Privacy Standards May Affect Your Nonprofit

By Allison Ward, Partner

The European Union's comprehensive new regulation governing privacy practices goes into effect on May 25, 2018. U.S.-based nonprofit organizations shouldn't assume they are exempt, even if they do not operate in the EU.

That's because Article 3 of the General Data Protection Regulation (GDPR) states that organizations that collect personal data or behavioral information from individuals in an EU member country are subject to GDPR requirements.

Overview of the New Regulation

GDPR is the most meaningful change to European privacy regulations in more than 20 years. It replaces the outdated Data Protection Directive enacted in 1995.

Sparked by public concern over privacy, GDPR is designed to protect all EU citizens' private information and to provide consistency in data privacy rules among EU member countries. It focuses on obtaining consent for personal data collection and use and allowing individuals to access their data or request that it be deleted (the "right to be forgotten"), among other standards. It also sets a 72-hour window for breach reporting.

The consequences for noncompliance include fines of up to 4% of annual global revenue or 20 million euros (equivalent to $24.6 million U.S. as of this writing) — not to mention reputational damage.

Under GDPR, personal data includes any information related to a person, or "data subject," that can be used to directly or indirectly identify the person. This includes:

- Name
- Photos
- Email addresses
- Social media posts
- Medical information
- Bank details
- IP address

While the regulations are complex, at a high level GDPR requires that organizations:

- Obtain consent that is "freely given, specific, informed, and unambiguous" prior to collection of personal information from a data subject
- Restrict data collection to specific, explicit, and legitimate purposes
- Limit data retention to requirements for business purposes
- Provide data processing transparency
    - Maintain data security, confidentiality, and integrity
    - Adhere to breach notification requirements
    - Designate a Data Protection Officer
    - Perform a data protection impact assessment

Data subjects have the right to:

- Access their data
- Object to the use of their data
- Be forgotten (have their data erased)
- Rectify their data
- Receive their data and transmit it to another controller

Does GDPR Apply to You?

Any organization that has or processes the personal data of an individual who lives in the EU is required to comply with GDPR. The regulation does not apply to EU

citizens who are outside the EU at the time the data is collected.

While this obviously affects nonprofits with a physical presence in the EU, it may also apply to your organization if you:

- Exchange data with anyone in the EU
- Have employees, service recipients, donors, or grantees in the EU
- Collect, view, process, or store the personal data of individuals who live in the EU
- Have a web presence that targets or references EU users
- Have URL extensions for EU states

For example, GDPR may apply to:

- Nonprofits that contract with other organizations or companies based in the EU
- Nonprofits that receive contributions from EU-based individuals or organizations
- Higher education institutions with study abroad programs or online courses taken by students who live in the EU

Even if your organization doesn't have a compelling reason to adhere to GDPR standards, they should be considered a best practice.

Next Steps

We recommend that all nonprofit organizations carefully consider their interactions with EU residents to determine if GDPR applies to them. Seek qualified legal counsel if you believe it might.

Even if your organization doesn't have a compelling reason to adhere to GDPR standards, however, they should be considered a best practice. A data breach can have a significant and long-term impact on an organization's operations, finances, reputation, and donor trust.

Please contact us with questions or for assistance with assessing and strengthening your organization's cybersecurity controls.

About the Author

Allison Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services for nonprofit organizations, financial institutions, health facilities, educational institutions, and a variety of other organizations. She stays current on changing threats to design review procedures to aid clients in implementing appropriate controls to protect against evolving cybersecurity threats. Allison speaks on information security topics for various banking, state CPA, and non-profit societies.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. For over 50 years, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.