SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for Everyone

GDPR

Overview

You may have heard of a new law called GDPR, or the General Data Protection Regulation. This law was developed by the European Union and takes effect 25 May 2018. It applies to any organization that handles the personal information of any resident in the European Union (EU), regardless of where in the world that organization is located. GDPR requires organizations to maintain the privacy and security of any EU resident's personal information. To ensure compliance with GDPR, some key principles need to be understood and implemented.

People have a right to privacy. Organizations need to respect their privacy by restricting what personal data they collect and process and by safeguarding that data. Privacy obligations apply to any information, either by itself or used with other pieces of information, that could identify an individual person living in the European Union. This information could be items such as addresses, passport numbers, driver's license numbers, financial details, biometrics, union memberships, medical history, location data, or information relating to a person's sexual, religious, or political orientation. The regulation applies to a 'natural person,' meaning a living individual. Here are some of the main tenets of GDPR that should be followed:

Personal data for individuals shall be processed lawfully, fairly, and in a transparent manner.

People need to be told what is being collected and for what purpose.

Personal data shall be collected for specified, explicit, and legitimate purposes. It shall not be used for any other reasons that conflict with these purposes.

Personal data shall only be kept and processed for as long as it is required for that purpose and for no longer than that.

Personal data must be kept up-to-date and accurate.

People have the right to receive a copy of their data, or can request that their personal data no longer be used. In some cases, they can have it deleted entirely.

Organizations must implement appropriate security measures to protect personal data against accidental or unlawful destruction, loss, alteration, or disclosure.

In addition, organizations need to ensure all staff members who handle personal data are properly trained in how to secure and protect that data.

The protection measures that are in place to secure personal data must ensure a level of protection appropriate to the sensitive nature of the data. As the risk associated with data becomes greater, so should the effort and expense of measures to protect the data. These measures should be regularly reviewed and updated as appropriate. Well-documented records about privacy and security decisions and measures help to show compliance with the requirements. In addition, organizations are legally bound to employ measures, such as contracts and due diligence reviews, to protect personal data when transferring it to external third parties or parties outside the European Union. Finally, in the case of a personal data breach, organizations shall report the breach within 72 hours after becoming aware of it. Failure for organizations to comply with GDPR can result in fines up to 4% of their global revenue, making GDPR one of the most financially costly global regulations in the world.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Brian Honan *is CEO of BH Consulting, an independent cybersecurity and data protection consulting firm based in Dublin, Ireland. Brian has acted as a special advisor to Europol's Cybercrime Centre (EC3), is founder of Ireland's first CERT, and sits on the advisory board for several innovative security companies. Find Brian at www.linkedin.com/in/brianhonan or Twitter @brianhonan.*

Resources

GDPR Overview for Individuals and Organizations:	http://gdprandyou.ie
The GDPR Regulation:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! Translations and Archives:	https://www.sans.org/u/D88