June 8, 2018

What's trending on NP Privacy Partner

The GDPR is here and being enforced, and the OCR issues a reminder that physical security controls should not take a backseat. Here's what's trending in data privacy and cybersecurity.

Cybersecurity

The GDPR is here and being enforced

The European Union's General Data Protection Regulation (GDPR) just became effective a few days ago, on May 25, 2018. Yet, already Facebook is facing lawsuits regarding its data sharing practices. Max Schrems, an Austrian privacy activist, filed the lawsuits against Facebook, seeking large fines. The lawsuits are by product and include separate suits against Facebook and Facebook-owned WhatsApp and Instagram.

The GDPR requires companies to justify why they are collecting data on European users and states what they intend to do with the data. Companies must receive clear consent prior to collecting any personal information and keep strict records as to any data processing.

Facebook has been preparing for the GDPR over the past year and enforcing new policies to protect users' data, but Schrems argues that these steps are not sufficient. Specifically, Schrems claims that the companies' "all or nothing" approach to privacy—requiring users to click a box to access the service—is a violation of the GDPR. Rather, Schrems contends that the companies should let users decide exactly how their data is used at more of a case-by-case level.

Facebook argues that its privacy measures are GDPR compliant.

Over the past 18 months, companies of all sizes have wondered how the GDPR was going to be enforced. As we expected, it looks like it will take some GDPR-related lawsuits to interpret the regulation and set precedent as to its enforcement. While May 25, 2018, was the effective date, it was not the last we'll hear of the GDPR. – *Jenny L. Holmes*

Healthcare and HIPAA

OCR issues a reminder to continue focus on physical security controls

Last month, the Department of Health and Human Services Office for Civil Rights (OCR), in its *Cybersecurity Newsletter*, urged health care providers, health insurers and others regulated by HIPAA to not lose sight of the need to provide physical security controls over health information. As referenced in the OCR guidance, failing to do so can have significant consequences. For example, in 2016, the University of Mississippi entered into a $2.75 million settlement with OCR after OCR's breach investigation indicated that the University failed to implement physical safeguards to restrict access on its workstations.

The HIPAA regulations require that covered entities and business associates secure their workstations by limiting access to authorized users. "Workstations" is broadly defined and refers to laptop or desktop computers, any other device performing similar functions and electronic media stored in the immediate environment of the computers or devices. OCR interprets this definition to encompass portable devices such as tablets and smart phones.

In its guidance, OCR acknowledges that physical security controls are not a one-size-fits-all solution and what is appropriate will vary based on the particular organization. An organization should look to the required security risk analysis and resulting risk management plan to dictate the physical controls required to address the organization's needs. OCR also encourages organizations to consider certain questions, including whether the organization has an up-to-date inventory of all of its electronic devices and their locations and whether its employees are properly trained regarding the use of the organization's physical security controls.

OCR also notes that many physical security controls are inexpensive to implement, citing the modest costs of privacy screens over computers, as well as port or device locks. The guidance also describes simple measures that an organization can take to enhance its physical security controls, including moving workstations to private areas and storing electronic equipment in locked or secured areas.

The OCR *Cybersecurity Newsletter* can be found here. – *Valerie Breslin Montague*

For more information, please contact:

- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485