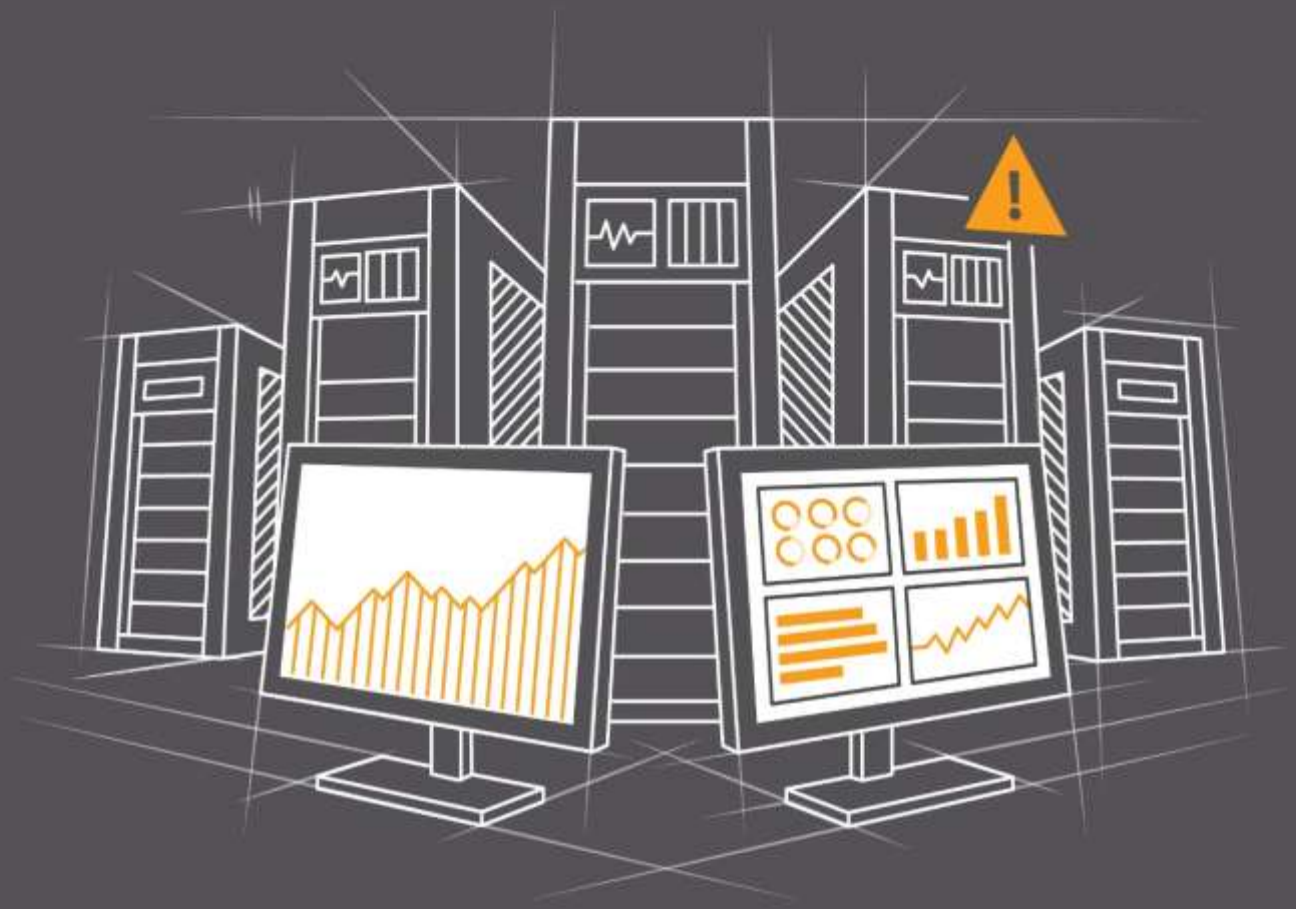
solarwinds



GDPR – WHAT IS IT AND HOW CAN SOLARWINDS HELP?

If your organization is based in the EU, or provide goods or services to the EU, you've probably heard a lot about the General Data Protection Regulation (GDPR) compliance lately. In this post, I'd like to educate the THWACK® community on some of the GDPR requirements and how SolarWinds products such as Log & Event Manager (LEM) can assist with GDPR compliance.

WHY THE NEED FOR GDPR?

In December 2015, the EU announced that the GDPR was being implemented in place of the Data Protection Directive (DPD), the current EU data laws. The DPD was first established over 20 years ago, but it has not kept up with the seismic changes in information technology and is no longer sufficient for today's technologies and threats. The shortcomings of the DPD have become apparent and the EU saw the need to replace it.

THE SHIFT FROM DIRECTIVE TO REGULATION

A defining change which comes with the launch of GDPR is a shift from a directive to a regulation. DPD was a directive, meaning a set of rules issued to member states, but each country can interpret and implement the rules differently. GDPR is a regulation, which requires countries to implement the regulation without any scope for varying interpretations. It removes any ambiguities on organizations' data protection responsibilities. GDPR paves the way for data privacy as a fundamental right for EU citizens. The implementation deadline for the regulation is May 25, 2018, so organizations are certainly against the clock to implement the necessary policies, procedures, and systems to ensure they are compliant.

WHAT EXACTLY IS PERSONAL DATA?

GDPR defines a very broad spectrum of personal data. Personal data is no longer limited to information such as name, email, address, phone number, etc. GDPR also classifies online identifiers such as IP addresses, web cookies, and unique device identifiers such as personal data. Even pseudonymous data is included. This is personal data which has been technically modified in some way, such as hashed or encrypted. Worth noting that the rules are slightly relaxed for data that is pseudonymized, which provides an incentive for organizations to encrypt or hash their data. GDPR defines personal data as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's *** life or sexual orientation." (GDPR Article 9, page 124)

MY ORGANIZATION IS NOT BASED IN THE EU—WHY SHOULD I CARE ABOUT GDPR?

Although it is an EU regulation, it is not limited to the EU. GDPR will affect organizations on a global scale. The regulation will apply to any organization that offers goods or services to EU citizens. If a company based outside the EU is storing, managing, or processing personal data belonging to EU citizens, they will need to ensure GDPR compliance (GDPR Article 3, page 110). According to a recent PwC study, a staggering 92% of US multinational companies have listed GDPR compliance as data-privacy priority. A significant percentage of those organization plan to spend $1 million or more on GDPR.

DATA CONTROLLERS VS. DATA PROCESSORS

Controller – "The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

Processor – "A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller." (Article 4, GDPR page 112)

Under the DPD, data processers had very little responsibilities to company, whereas GDPR places joint responsibility for both data controllers and data processors to comply with the regulation. As an example, if an organization (controller) outsources its payroll to an external payroll company (processor), even though the payroll company is managing and storing data on behalf of the controller, they are now required to comply with GDPR. This will impact controllers and processors alike. Controllers will have to conduct reviews to ensure their processors have a framework in place to comply with GDPR. Processors will have to ensure they are compliant.

DATA BREACH NOTIFICATION – GDPR ARTICLE 33 (PAGE 53)

The Data Protection Directive didn't require organizations to notify authorities of any data breaches. GDPR defines a personal data breach as the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed." It's worth remembering that personal data now includes IP addresses, web cookies, unique devices identifiers, and more. The GDPR also now requires organizations (or controllers, as they are known in GDPR) to report data breaches within 72 hours. If this deadline is not met, you will have to explain the reasons for the delay. If you are a data processor, you must report the breach to the controller. The controller then notifies the "supervisory authority." Data subjects must also be informed when a breach poses a high risk to their rights and freedoms. However, if the controller had implemented protection measures such as encryption on the data, then the data subject's rights and freedoms are unlikely to be at risk.

INDIVIDUAL RIGHTS

GDPR provides EU citizens with increase personal data rights. Just some of these individual rights include Consent (Article 7), Right to Erasure (Article 17), and Data Portability (Article 20).

Organizations will require consent when collecting personal data of EU citizens. The type of data and retention period will need to be stated in plain language that citizens can clearly understand. Data controllers will be required to prove that consent has been provided by the subject.

Individuals also have the right to erasure, meaning subjects can request controllers to delete all information about them, provided the controller has no reason to further process the data. There are exceptions if the data is used for legal obligations—for example, financial institutions are legally obliged to retain data for a certain period of time. If a data controller has shared personal data with third parties, the onus is on the controller to inform those third parties of the data subjects request to erase the data.

Data Portability allows data subjects to receive the personal data they provided to a data controller in a structured, "machine-readable" format. This portability facilitates data subjects' ability to move, copy, or transmit data easily from one service provider to another.

WHAT HAPPENS IF WE DON'T COMPLY?

If your organization is not compliant with GDPR, it can receive fines of up to €20 million or 4% of global annual turnover for the preceding financial year (whichever is greater). These penalties apply to both data controllers and processors. (Article 83, section 5)

HOW CAN SOLARWINDS HELP?

GDPR will likely require organizations to implement new policies, procedures, controls, and technologies—it may even require you to hire a Data Protection Officer, in certain cases. While no single technology can meet all the requirements of GDPR, SolarWinds can certainly assist with some of the requirements.

ARTICLE 32: SECURITY OF PROCESSING

This section of GDPR requires organizations to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk." SolarWinds® Patch Manager can be used to identify and update missing patches and outdated third-party software on your Windows® servers and workstations. Patch Manager also enables you to inventory your Windows® machines and report on unauthorized software installations on your network.

Article 32 also requires "regular testing the effectiveness of technical measures for ensuring security of the processing." SolarWinds LEM can be used to validate the controls you have put in place.

Please see here for more information: Article 32

ARTICLE 33 AND 34: NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY AND COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

SolarWinds Risk Intelligence (RI) is a product that performs a scan to discover personally identifiable information across your systems and points out potential vulnerabilities that could lead to a data breach. RI can audit PII data to help ensure it is being stored, in accordance to the requirements of GDPR. The reports from RI can be helpful in providing evidence of due diligence when it comes to the storage and security of PII data.

As mentioned previously, if a personal data breach occurs, the controller must notify the supervisory authority within 72 hours. It is vital that breaches and threats are identified as quickly as possible.

LEM can assist with the detection of potential breaches thanks to features such as correlation rules and Threat Feed Intelligence. LEM's File Integrity Monitoring and USB Defender® can monitor for any suspicious file activity and also the detect the use of unauthorized USB removable media. If an incident occurs, LEM's nDepth feature can be leveraged to perform historical analysis. LEM also includes best practice reporting templates to assist with compliance reporting.