EU GDPR - May 25th, 2018

On 25 May 2018, the European Union General Data Protection Regulation (EU GDPR) will affect every organization that processes EU residents' personally identifiable information. This EU wide law will impact how users get hold of data stored about them and change how organizations both protect and store their data. It has been introduced to help protect confidentiality, integrity and availability of data and carries fines for those organizations who do not comply.

Who does the EU GDPR effect?

Cyber theft is a massive problem and the EU GDPR is recognition that there is significant personal risk associated with storing personal data.

This new law has been passed by the EU and does **not** require each individual country to impose the law separately.

The GDPR applies to all member states of the EU but its reach goes further to those organizations who hold personal data about EU residents even if not in the EU. Brexit is irrelevant.

Preparing for GDPR and the fines

- Identify whether the organisation is a data controller or data processor. Does the GDPR apply to the organisation?
- Identify data, (Personal identifiable information (PII)), what its used for, and where is it stored?
- Assign Data Protection officer and embed procedures
- Protect Personal identifiable information (PII)**
- Detect and breaches and threats and report within 72 hours. Ensure incident response is implemented and tested
- Recover data and remediate where possible

Penalties: 4% of Annual global turnover or 20M Euros – whichever is greater.

Example…

Whilst Tesco Bank recently had to pay back £2.5M into bank accounts following an attack, if they had been fined under the EU GDPR, their fine could have been as high as £2.5B!

How can Ivanti Help?

Ivanti helps organizations work towards EU GDPR compliance by protecting data (PII) from cyber-attacks in the first instance. Many of the ransomware attacks and data breaches seen recently have involved phishing attacks targeted at users and the endpoints.

Ivanti Application Control, Endpoint Manager and Patch for Endpoints, helps implement the SANS Top 5 recommendations against ransomware attacks:

1. Inventory of Authorized and Unauthorized Devices

Ivanti Endpoint Manager

https://www.ivanti.com/products/endpoint-manager

2. Inventory of Authorized and Unauthorized Software

Ivanti Application Control

https://www.ivanti.com/products/application-control

3. Secure Configurations for Hardware and Software

Ivanti Endpoint Security for Endpoint Manager
https://www.ivanti.com/products/endpoint-security

Ivanti Application Control
https://www.ivanti.com/products/application-control

4. Patching applications (including 3rd party non-Microsoft apps)

Patch for Endpoints
https://www.ivanti.com/products/patch-for-endpoints

Patch for SCCM
https://www.ivanti.com/products/patch-management-for-sccm

Patch for Windows Servers
https://www.ivanti.com/products/patch-management

5. Removal of administrative rights without effecting productivity

Ivanti Application Control
https://www.ivanti.com/products/application-control

Where can I find out more about the EU GDPR?

Visit the official EU GDPR website at: http://www.eugdpr.org/ to find out more information regarding the regulation involved, the process itself and to access quotes, videos, articles and other related resources.

www.ivanti.com
1.800.982.2130
sales@ivanti.com