Tech Note

Pulse Secure Solutions and GDPR

Guidance for Pulse Secure customers and partners to understand how our Secure Access portfolio relates to the European Union's General Data Protection Regulation

What is the General Data Protection Regulation?

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The primary objective of GDPR is to give control back to EU subjects over their personal data and simplify the regulatory environment within the EU.

When does it come into force and which countries does it cover?

GDPR became enforceable on 25th of May, 2018, and unlike a directive, it does not require any enabling legislation to be passed by national governments and is directly binding and applicable. It is also important to note that GDPR is not exclusive to the 28 EU member states. The law states:

> *"The new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU subjects. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations."*

What are the key requirements of GDPR?

GDPR is built around 99 articles of law and the final version of the regulations, released 6 April 2016, can be found at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. Key areas that should be considered include:

- Applies to all companies worldwide that process personal data of EU citizens
- Widens and codifies the definition of personal information for citizens
- Tightens the rules for obtaining valid consent to use personal information
- Makes a data protection officer (DPO) mandatory for certain organisations
- Introduces mandatory privacy impact assessments (PIAs)
- Introduces a common data breach notification requirement
- Introduces the right to be forgotten for EU citizens
- Expands liability beyond data controllers to all organisations handling personal data
- Requires privacy to be included in systems and processes by design

What are the penalties for non-compliance or regulatory breaches?

To summarize, all organizations who hold personal data on an EU subject must comply. They also must adhere to a strict data protection compliance regime or risk penalties of 2% of revenue for a minor infringement or 4% for a major infringement or €20m, whichever is greater.

What is the Pulse Secure solution?

Pulse Secure provides easy, comprehensive and integrated Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. Enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. The solution suite is comprised of integrated virtual private network (VPN), network access control (NAC), virtual application delivery controller (vADC) and mobile security technologies.

What are some GDPR considerations for Pulse Secure solutions?

- For the operation of its VPN, NAC and vADC products and service, Pulse Secure gathers and stores a limited set of operational data that includes IP address of users, network locations and websites along with the MAC addresses of connecting devices.
- All this information is held in an encrypted format and only accessible to authorised IT systems administrators through standard login and password control that can be supplemented by two-factor-authentication where required.
- Based on SNMP logging settings defined by the customer, Pulse Secure VPN and NAC activity logs, which captures IP addresses and sites accessed, can be stored on Pulse One which offers administrators centralized management (cloud based deployments).
- Pulse Secure maintains logs of IP and MAC address information used for service delivery and security compliance. This activity log data includes the username which could allow a correlation to be made between a user and the websites that have previously visited. These logs are typically forwarded to security information event mangement (SIEM) systems for further analysis and longer-term retention.
- Pulse Secure does collect anonymised sample data from its hardware appliances and cloud services that is used for diagnostics and product development tasks. This information *does not* contain personal data of European Union (EU) citizens as defined by GDPR.

GDPR advice for IT administrators of Pulse Secure solutions

Pulse Secure believes that its products, with regards to data protection, comply with the legal requirements of the GDPR and other national security standards such as FIPS-140.

However, administrators should be aware that as a critical component to secure access between users, devices, network resources and cloud applications, Pulse Secure technologies gather detailed user activity information which are stored in activity logs. The information processed and stored is typical of the majority of other network security solutions.

These logs are used for implementing and monitoring cyber security control and for troubleshooting any incidents. However, these same tools can be used by authorised IT administrators to correlate the identity of individual users through connected directory service (e.g. Microsoft Active Directory) along with the websites users visit from activity logs. This capability is generally available to IT administrators using most VPN, NAC and vADC products with enterprise and Internet Service Providers.

As such, all organisations and service providers should ensure that all staff with access to Secure Access systems capable of accessing user profiles and browsing history are made aware of legal and privacy restrictions including GDPR. Pulse Secure advocates regular security and policy training for data handling staff and agreement to a formal code of conduct.

Retaining data following Pulse Secure device replacement

Although not directly stipulated by GDPR, in the context of retention and destruction of personal or sensitive data, some organisations may wish to keep the hard disks within Pulse Secure Appliances prior to a hardware replacement. While our hardware warranty does not allow for tampering with appliance components such as the hard disk, Pulse Secure offers a "Keep Your Hard Drive Service" Service which is available as an optional add-on for End Users with a valid Pulse Secure Gold or Platinum Support contract. For more details, visit the customer success website at: https://www.pulsesecure.net/services/gold-support/keep-your-hard-drive/

In the event of a hardware failure, customers that have purchased the "Keep Your Hard Drive Service" will have the option to remove and keep the hard drive of the failed unit before shipping the failed unit to Pulse Secure. Pulse Secure's Global Support Team will provide instructions for removing the hard drive when working on the Return Material Authorization (RMA) Case. Full details of the service are available via your local Pulse Secure Partner or Pulse Secure field sales manager.

For more information on how Pulse Secure can help you with GDPR readiness and ongoing Secure Access, please visit https://www.pulsesecure.net/

About Pulse Secure

Pulse Secure, LLC offers the easiest, most comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.