Pulse Secure®

Pulse Secure Solutions and GDPR

Applying Secure Access solutions to demonstrate due diligence and complementary controls towards preventing personal data breach and mitigating GDRP risks.

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 of their personal data back to EU subjects and to simplify international business by unifying the regulation within the EU.

GDPR is part of a wider trend towards more regulatory control around data at a time when organizations are increasingly utilising resources maintained within cloud-based applications that are often not directly controlled by the organization. This move towards hybrid IT will, in many instances, encourage access to application information that may well contain GDPR relevant personal data remotely via a wider array of devices including laptops, desktops, tablets and smartphones. This paper addresses where GDPR impacts information security resources, what additional safeguards IT should consider, and what solutions Pulse Secure offers to organizations to support GDPR compliance.

Challenges

- Ensuring only authorized, authenticated users have access to personal data
- Invoking protected connectivity between users, devices and apps accessing personal data
- Consistent enforcing of active end-point security mechanisms
- Segregating and protecting personal data on smart mobile devices
- Audit capabilities that demonstrate active access controls supporting personal data protection

GDRP Articles on Security of Processing

GDPR is built around 11 chapters including 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. The chapters include key principles, rights of the data subject and the responsibilities of the controller and processor of personal data. Chapter 4, Article 32, "Security of processing" has several articles that outline many technical and policy requirements that IT departments, especially those with responsibility for secure user, application and data access, need to understand and enact to ensure both best practice and regulatory compliance.

Article 32 GDPR* states that the controller and the processor of personal data as defined by GDPR shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This should include, but not be limited to the following:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In addition, the article states that an appropriate level of security should be taken to protect against unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

1. When processing EU personal data, the organization must take into account what are available technical controls, the costs to implement and the nature, scope, context and purposes of processing the data, as well as the risk of varying likelihood and severity for data leakage impacting the rights and freedoms of natural persons. The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security that fits the level of risk, including the following data protection capabilities as appropriate:
   - The pseudonymisation and encryption of personal data.
   - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
   - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
   - A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
2. Assessment should consider the processing risks due to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40* or an approved certification mechanism as referred to in Article 42* may be used as an element by which to demonstrate compliance with the requirements set out in this Article.
4. The controller and processor shall take steps to ensure that any natural person, acting under the authority of the controller or the processor, who has access to personal data does not process them except on instructions from the controller, unless required to do so by Union or Member State law.

Article 32 Impact on InfoSec Organizations

Article 32* suggests that organizations must put in place protections that deliver policy-based and auditable security controls for every user and system that has access to personal data covered by GDPR. Based on "appropriate technical and organizational measures", it can be assumed that in order to "ensure a level of security appropriate to the risk", each organization should at least have:

- Strong user authentication to ensure only persons acting under the authority of the data controller has access to personal data.
- Protected connectivity between users, devices, applications and data stores containing personal data.
- Assurance of active end point security mechanisms for those users and their devices accessing and storing personal data.
- Secure, smart mobile devices with encrypted workspaces that segregate apps and downloaded personal data including means for remote data wiping should the mobile device compromised, lost or stolen.
- Ability to apply consistent policies across mobile workforce devices and IT resources processing and storing personal data whether data resides on mobile devices, on premise, or in cloud-based systems.
- An active, retained and consistently utilized audit trail that demonstrates appropriate technical controls, monitoring and response with regards to access and data protection.

Data Breach Notification

The other major area of concern for IT organizations is Article 34* of GDPR that covers the "Communication of a personal data breach to the data subject." In summary, this article affirms the scope and duties of notification by the controller to the data subject in the event of a data breach. The controller may not have to disclose the data breach if it has implemented appropriate technical and organizational protection measures, unless the controller is compelled to disclose the breach based on the judgement of the supervisory authority. In particular, this section states that:

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33 Section (3).*
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   - appropriate technical and organizational protection measures were in place, and those measures were applied to the personal data affected by the personal data breach, in particular rendering the personal data unintelligible to any person who is not authorised to access it;
   - the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects are no longer likely to materialise;
   - the controller's notification to a data subject would involve disproportionate effort, and in such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require the controller to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Article 34 Impact on InfoSec Organizations

An interpretation of Article 34* suggests that if an organization suffered a personal data breach, for example that of a customer transaction database where unencrypted EU personal data was exfiltrated, then said organization must communicate this breach "in clear and plain language" to every data subject affected. The same would be true if the protection mechanism to secure the session between a device and a cloud-based application was compromised, if a corporate user's end-point device with access to GDPR data processing systems was compromised and resulted in data exfiltration, or a mobile device storing downloaded and unencrypted copies of personal data was lost or stolen.

Article 34 that references the potential to avoid breach notification to the data subject if the breached data was "unintelligible to any person who is not authorised to access it, such as encryption." For this reason, it could be considered best practice for any device that is handling and potentially storing personal data subject to GDPR to maintain some form of protected and encrypted workspace within each mobile device that can be remotely wiped if the device is lost or stolen. However, if secure access controls, such as access authentication, session encryption, and assurance of personal data protection at the end point are not in place to prevent future likely personal data breaches, then the supervisory authority may still compel the controller to disclose a breach incident even if more nominal defences and data obfuscation are in place.

How is GDPR relevant to other compliance frameworks?

Although this guidance is designed to help address the regulatory compliance under GDPR, the broad requirements GDRP stipulates are mirrored in data protection specifications within other business and regulatory compliance mandates including, but not limited to:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPPA)
- Federal Information Security Management Act of 2002 (FISMA)
- Gramm Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)

Alongside these compliance frameworks are a growing number of country- and industry-specific regulatory frameworks that, in common with GDPR, mandate security of sensitive, financial and personal data. These often include regulations around the acquisition, transit, storage, processing and destruction of data plus security controls for users and devices with access to such data. Most stipulate some form of access control, data protection (including encryption) and audit capability along with responsibility to disclose to authorities and end users the nature of security breaches and/or data loss.

How Pulse Secure Solutions Support GDPR

Pulse Secure provides an easy, comprehensive and integrated set of Secure Access solutions that can serve to demonstrate due diligence and complementary controls towards preventing personal data breach. The solution set covers access authentication, protected communications, enforcement of endpoint defences, mobile device data containerisation, as well as network access visibility and IOT security.

Enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforces to securely access applications and information in the data center and cloud while ensuring business compliance. The Secure Access portfolio is comprised of integrated virtual private network (VPN), network access control (NAC), virtual application delivery controller (vADC) and mobile security technologies.

Pulse Connect Secure

Pulse Connect Secure offers the most reliable, feature-rich SSL VPN that provides seamless, protected connectivity across corporate and personal mobile devices to corporate data center and cloud resources and applications.

- Clientless access, strong authentication, host checking for endpoint security compliance, granular policies, virtual desktop access, mobile device management (MDM) integration, and extensive audit functionality
- Authenticated and compliant access to on premise and cloud applications enabling SSO and SAML to such applications as Office365 and Salesforce.com
- Verification of endpoint security defences, patches, registry settings, configurations and specified applications being installed, updated and active
- Advanced features to orchestrate always-on, application-activated, and mobile VPN capabilities with multifactor and certificate-based authentication
- Extensive visibility and logging to enable auditing and response to security anomalies and compliance violations

Pulse Workspace

Pulse Workspace is an extensive mobile application and device management solution that segregates personal and corporate application and data while preserving native user experience and low administrative overhead. Organizations can deploy corporate and sanctioned apps, secure connectivity, and ensure corporate data in transit and at rest is protected on Android and Apple mobile devices.

- Simple, yet powerful containerisation and data leakage protection for corporate apps and data that doesn't invade the device owner's privacy
- Designate which users and apps gain VPN access to network and cloud resources and data through their mobile device
- Workflow automation to pre-configure apps, accounts, settings, certificates and compliance checks according to role and data protection requisites
- Granular policy compliance and enforcement such as negating rooted or jailbroken devices, password strength, mobile app-triggered VPN, and more
- Retained control of data in transit and at rest with immediate means to revoke access and remotely wipe corporate data and apps within the container
- Extensive visibility and logging to enable auditing and response to security and data protection issues

Pulse Cloud Secure

Pulse Cloud Secure is designed to provide a mobile workforce anytime, protected access to hybrid IT environments by enabling single sign-on (SSO) from mobile devices to cloud resources and SaaS applications with strong authentication and device compliance.

- Extensive endpoint MFA integration combined with SAML 2.0 based SSO for cloud access, as well as Kerberos Constrained Delegation and NT LAN Manager for legacy data center application access
- Broad interoperability with third-party identity and access management (IAM) vendors with means to serve as a SAML Identity Provider (IdP) and as a SAML Service Provider (SP) for deployment flexibility and seamless user experience
- Verification of laptops, iOS and Android device protection mechanisms to ensure authorized users with trusted devices have cloud and data center access
- Scalable, centralized control through Pulse One to enable consistent policy management, visibility and audit for data center and cloud access authorization and compliance

Pulse Policy Secure

Pulse Policy Secure is a next-generation Network Access Control solution that provides visibility, policy-based control, and enforcement of users, endpoints and IOT devices accessing or operating on a corporate network. The solution provides access intelligence, compliance, audit and threat response of devices accessing network resources that process and store personal data.

- Simplified administration and deployment leveraging configuration wizards and Pulse VPN policies
- Agent and agentless endpoint visibility, streamlined guest management, and automated Windows, MAC, smartphone, tablet and BYOD onboarding
- Dynamic endpoint and IOT device discovery, classification, inventory, monitoring and contextual access enforcement with granular compliance policies
- Strong mitigation capabilities supporting 802.1X port-level and L2-L4 enforcement, automated and user-directed endpoint remediation, network quarantine and blocking, and IOT security
- Interoperability with popular network and wireless switches, NGFW, SIEM and EMM tools

Cover Your GDPR Control GAPS

The Pulse Secure solutions provide an easy, comprehensive and integrated approach to extending your organization's Secure Access capabilities. The approach allows for consistent policy-based access visibility, secure connectivity, data protection and audit across users and their mobile devices, and data center and cloud applications and resources that process and store personal data. By implementing Pulse Secure, organizations can further demonstrate due diligence for GDPR and technical preventative measures to mitigate personal data breach. For more information visit https://www.pulsesecure.net/solutions/.

* Sections in this solution brief have summarized GDRP articles. For complete and direct specifications regarding GDPR, visit: found http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf, https://gdpr-info.eu/art-32-gdpr/, https://gdpr-info.eu/art-33-gdpr/, and https://gdpr-info.eu/art-34-gdpr/.

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.