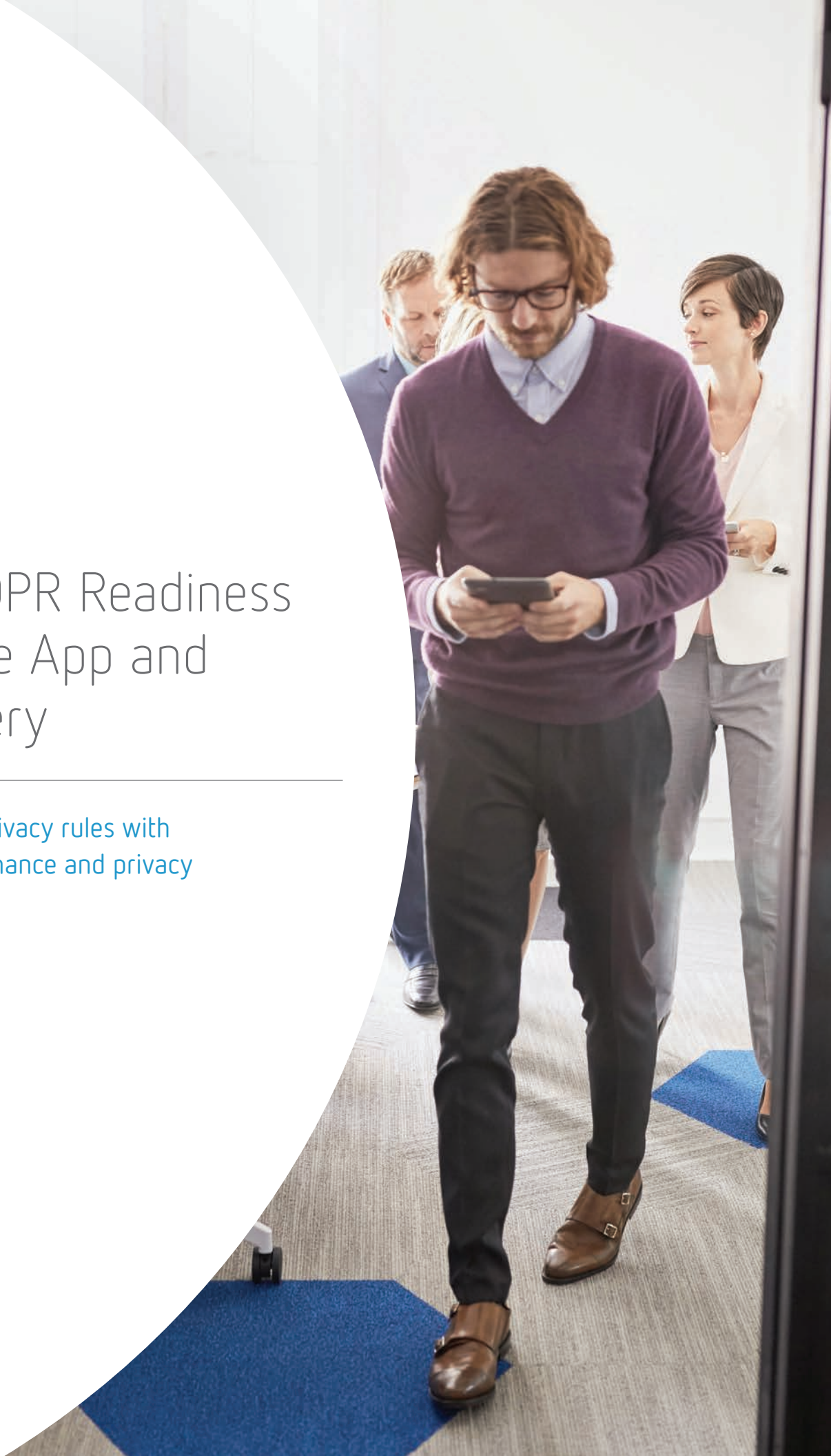
CITRIX®

Achieve GDPR Readiness with Secure App and Data Delivery

Meet new EU data privacy rules with accountability, governance and privacy



Beginning on May 25, 2018, the General Data Protection Regulation (GDPR) will implement a new legal framework in the European Union (EU) for the protection and distribution of personal data. Organizations around the world that serve customers and individuals in the EU will be required to put in place security policies to address different risks and effectively enforce these policies with technical controls—or potentially face fines of up to €10 million or more. While GDPR readiness can pose a significant challenge for many organizations, many of its technical requirements align closely with the security and compliance best practices already supported by Citrix solutions.

Citrix simplifies security and compliance by enabling IT to create a software-defined perimeter that combines secure access to apps and data with contextual control, visibility and behavior analytics across devices, networks and clouds. By extending control beyond the traditional datacenter to mediate user interactions with apps and data, IT can proactively secure, detect, and mitigate risk with intelligence applied to each unique scenario.

This white paper discusses the requirements of GDPR and how they can be addressed with integrated Citrix technologies for contextual access, network security, application security, data security, and analytics and insights.

What GDPR means to your organization

Applying to all organizations within the EU or organizations that control or process the personal data of individuals in the EU, the GDPR strengthens and harmonizes data protection laws across EU nations. The regulation mandates a high level of responsibility and accountability for these organizations while giving individuals greater control over their data through measures including pseudonymization, data minimization and controls around data collection, processing, storage and accessibility. The goals of the GDPR are to give individuals better control over their personal data, and ensure that companies are taking steps to mitigate the risk of damaging data breaches, including unauthorized access inside the organization.

Under the GDPR, individuals will have rights including the ability to access their personal data; rectify inaccuracies or omissions; request deletion or removal of data once it is no longer required; restrict the processing of their data; and object to the use of their data. The scope of the data to which the GDPR applies is broad and comprehensive, encompassing any information relating to an identified or identifiable natural person, whether the data has been provided by the individual, observed by systems such as web browsers and social media platforms, derived through straightforward processes such as transactional history, or inferred through complex processing.

A recent study reveals a low level of preparedness among affected organizations—as well as a high level of anxiety. According to *The Need for a New IT Security Architecture: Global Study on Compliance Challenges & Security Effectiveness in the Workplace*,[1] published by Ponemon Institute:

[1] https://www.citrix.com/it-security/resources/ponemon-security-study.html

- While 67 percent of respondents are aware of the GDPR, only about half of organizations represented in this research have allocated budget and started to prepare for these new regulations.
- Of those respondents who are aware of the GDPR, the biggest concern is the potential fine. Breaches of some provisions could lead to fines of up to 20 million euros or 4% of global annual revenues whichever is greater. For other breaches, the authorities could impose fines on companies of up to 10 million euros or 2% of global annual revenues whichever is greater.
- 74 percent of respondents say complying with the GDPR will have a significant and negative impact on their organizations, such as large potential fines and increased territorial reach of the regulations.

Such concerns are understandable given the extensive requirements of GDPR, which include both organizational and technical measures. On the organizational side, policies mandated by the GDPR include keeping records of data processing activities, reporting any data breaches that the organization becomes aware of, responding to customer requests for information about their data as well as requests for its deletion as appropriate, and in certain circumstances, appointing a data protection officer.

Required technical measures include capabilities for secure remote access to data and the secure transfer of data. If data is shared either within the organization or with other organizations, it must be kept secure. Organizations with multiple data repositories, whether on-premises or in the cloud, must apply these measures comprehensively. To demonstrate compliance with GDPR, organizations must also implement comprehensive governance measures to minimize the risk of breaches, uphold the protection of personal data, and ensure and demonstrate that the technical and organizational requirements of GDPR are being met.

The Information Commissioner's Office (ICO) of the U.K. offers guidance with particular relevance for GDPR compliance: organizations should "ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle." Examples cited by the ICO include projects such as:

- Building new IT systems for storing or accessing personal data
- Developing legislation, policy or strategies that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes[2]

In following these principles, the ICO recommends taking a "privacy by design" approach that promotes privacy and data protection compliance from the start, calling this "an essential tool in minimizing privacy risks and building trust."[3] By using IT systems with privacy embedded in their design and architecture, organizations can take proactive

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

"Organizations should ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle."

The Information Commissioner's Office (ICO) of the U.K.

steps to enforce end-to-end privacy by default, rather than seeking to achieve protection through add-on technologies applied on a piecemeal basis to systems that lack inherent security. With unified, contextual security built into their core, Citrix digital workplace solutions support the privacy-by-design approach recommended by the ICO.

How Citrix security aids GDPR readiness

Citrix solutions can facilitate GDPR readiness by providing a foundation of confidentiality, integrity and availability across all types of on-premises, hybrid cloud and public cloud IT environments. The Citrix situational approach to security and compliance centers on four tenets:

- Whenever possible, centralize apps and data in the data center or cloud so that enterprise data is not stored on devices.
- When sensitive data must be distributed, mobilized or utilized offline, ensure it is protected in a secured enclave.
- Precisely control access to resources with context-aware policies based on user, device, location, application and data sensitivity.
- Provide visibility and management capabilities that unite your entire IT infrastructure to deliver application and data-specific security.

These principles are embodied in integrated Citrix technologies for contextual access, network security, application security, data security, and analytics and insights to support GDPR compliance across the five following areas:

Access to personal data

The GDPR requires that organizations control and restrict access to personal data. With Citrix, organizations can control and secure access to applications and their data through multi-factor authentication. Group-based and user-based access policies are complemented with contextual controls that adapt access privileges dynamically based on a user's detected current device, location and network on an application-by-application basis.

Data encryption in transit

The GDPR calls for the encryption of personal data in transit. To prevent data from being compromised as it travels over networks, Citrix solutions encrypt communications between endpoints and centralized data. As a result, organizations can allow secure remote access to virtual applications and desktops for employees as well as contractors, vendors, partners and other third parties, governed by contextual access controls, without putting data at risk.

Data isolation and protection

To further strengthen data protection and mitigate the risk of breaches as required by the GDPR, Citrix provides comprehensive measures for application and data security including centralization, containerization, inspection and segmentation. Citrix solutions are built on a centralized architecture that keeps data in the datacenter, where it can be accessed remotely by both employees and authorized third parties without being exposed to risk on a user's endpoint. Centralization also enhances data protection by enabling simpler, more efficient and consistent management of system backups, patches and configurations. This helps organizations keep up to date with the latest protection against ransomware and other threats, and aids data recovery in the event of an incident. For mobile devices such as smartphones and tablets, containerization keeps business and customer data separate from any of the user's own data that the device may contain. Network inspection helps organizations deter attacks against critical business services and prevent data leakage. Within the datacenter, IT can apply network segmentation to isolate the personal data of each customer from other customers, from back office applications, and from the rest of the IT infrastructure.

Data encryption at rest

As the GDPR seeks to protect customers from unintended disclosure of their data —either by insiders or by a third party— Citrix solutions assist in enabling organizations to protect and encrypt data wherever it is stored. IT can prevent

data from residing on the endpoints by keeping data encrypted in the datacenter and mitigating against data loss and leakage due to lost, stolen or destroyed endpoints. On mobile devices, including bring-your-own (BYO) personal smartphones and tablets, containerization makes it possible to separate personal and business apps and their locally stored associated data. Customer data on mobile devices is encrypted and controlled by IT to prevent it from leaking in the event a smartphone or tablet is lost or stolen. Business-grade file sharing and content collaboration tools enable users to work productively with customer data without resorting to less-secure consumer services. Built-in security capabilities such as digital signatures, digital watermarks and information rights management (IRM) enable IT to maintain comprehensive, multi-layered protection wherever and however customer data is used.

Records of processing activities

The GDPR calls for organizations to maintain complete records of the processing of personal data. Citrix solutions provide visibility and auditability of user access to track exactly how and by whom personal data has been accessed. By securing and reporting on the movement of data from end to end between the datacenter and the endpoint, organizations can better meet GDPR guidelines.

Maintaining GDPR compliance with Citrix solutions

For more than a quarter-century, Citrix has been trusted by organizations across every industry, including the most highly regulated sectors, to protect sensitive business information without compromising workforce productivity. Citrix provides a secure infrastructure for application and data delivery, giving IT powerful options to control application and data access across any device, network and cloud.

Citrix offers an integrated secure digital workspace solution, which includes best-of-breed technologies for application and desktop delivery, networking, mobility and file sharing for secure delivery of apps and data. The solution offers organizations the flexibility to choose deployment in the cloud, with a service provider or fully on-premises.

Citrix can help support GDPR guidelines through the following secure technologies.

Citrix XenApp and XenDesktop – Secure delivery of virtual applications and desktops
Applications, desktops and their associated data are centrally managed and secured in the datacenter. IT can dynamically apply context aware security to the associated application or desktop based on granular control policies to enable secure, remote access from any device. Organizations facing data sovereignty requirements can use data centralization to allow remote access from other geographies without allowing data to leave their territory.

Citrix NetScaler – Secure remote access and web application protection
IT gains end-to-end control, visibility and encryption for network and application traffic to ensure secure delivery of applications and data. IT can enforce granular access control through contextual access policies based on user, device, location and network. Web applications and sites are protected from both known and unknown attacks. Additionally, the web application firewall, DDoS protection, and URL filtering aid in achieving compliance.

Citrix XenMobile – Enterprise mobility management
Corporate data and applications can be containerized on mobile devices, including BYO smartphones and tablets, and wiped remotely by IT to protect customer data in the event that the device is lost or stolen. Any user-owned content a device may contain is kept separate from business content and is unaffected by the remote wipe capability. Additionally, through the Citrix micro-VPN capabilities, data in transit is encrypted.

Citrix ShareFile – Enterprise file sync and share
Access to personal data on-premises and in the cloud can be controlled and secured through multi-factor authentication, password policies, mobile security and network security capabilities. All data within ShareFile is encrypted at rest and can be further protected through IRM and DLP. IT can set data sharing policies to further restrict

and control access to personal data. If a mobile device or laptop is lost or stolen, any ShareFile data it contains can be wiped remotely by IT. Data access tracking and auditing capabilities simplify GDPR compliance across multiple resource locations.

Conclusion

While the GDPR represents a significant challenge for organizations, its technical provisions align with established best practices for data privacy and protection, as well as with the security principles on which Citrix solutions are built. Citrix can help organizations across every industry, including the highly regulated government, financial services and healthcare sectors, meet internal and regulatory requirements for security and data protection. As organizations around the world prepare for the GDPR, Citrix secure digital workspace solutions can enable a simple approach to achieve compliance without impeding productivity.

To learn more about security and compliance with Citrix secure digital workspace solutions, please visit citrix.com/secure.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States