TRANSFORM SECURITY
DATA PROTECTION
SOLUTION OVERVIEW

IT MANAGEMENT AND THE GDPR: THE VMWARE PERSPECTIVE

Introduction

This Solution Overview is intended for IT personnel interested in the VMware perspective on the implications for IT of the forthcoming General Data Protection Regulation (GDPR) which is due to become enforceable in the European Union from 25th May 2018. Further, we aim to show where the VMware portfolio can help customers to implement solutions for data protection use cases, which in turn, may form part of an organization's efforts to comply with the GDPR.

The GDPR – What Is It?

The General Data Protection Regulation (Regulation [EU] 2016/679) is a regulation which will strengthen and unify data privacy rights for persons within the European Union (EU).

The GDPR also addresses the export of personal data outside EU borders. Its primary objectives are to give control over personal data – any identifiable information such as name, address, and national identifier numbers – back to the individual as a basic right and to simplify the regulatory environment for international business by harmonising data protection legislation within all EU countries.

The GDPR extends the scope of current EU data protection law to non-EU organizations who are processing EU personal data The harmonisation of data protection legislation should make it easier for non-EU organizations to comply, but this comes at the potential cost of a strict data protection compliance regime, with severe penalties for non-compliance.

Definitions

The GDPR approach to data protection has a wide scope, encompassing legal definitions and public policy about an individual's rights regarding the privacy and protection of personal data. VMware does not provide legal advice on GDPR compliance to its customers and strongly recommends that they consult appropriate process consultants and legal advisors on this subject.

The detailed definition of many of the terms used can differ widely between IT management professionals (who are broadly engineers), and privacy experts (who often have legal, compliance or public policy backgrounds), which can cause significant confusion between key stakeholders in the teams working towards GDPR compliance in an organization[1].

Except for page 6, ("The GDPR Overview"), the intention of this document is to give a VMware perspective on data protection for IT practitioners. For the sake of clarity to an IT audience, the definition of data protection used in this document will follow the familiar ISO/IEC IT definition of data protection[2] (ISO/IEC 2121404), which many IT practitioners use in practice and for compliance initiatives[3].

The concept of GDPR readiness assumes that the entire organization must comply with the law. From an IT compliance perspective, the GDPR is more nebulous; there are currently no familiar controls and configuration requirements mandated under the GDPR that are similar to ISO, SOC 1, or PCI certifications. Conversely, the scope of the GDPR doesn't encapsulate all the scope of IT data protection. It is therefore critical that the ongoing communication taking place between the teams of privacy experts and IT professionals. Constant monitoring and clarification will help to ensure that each party understands exactly the other's meaning and intent.

The Intersection of IT and the GDPR

The GDPR is comprised of 99 Articles governing the public policies designed to protect personal data. Only a handful actually relate to IT data protection and cyber-security.

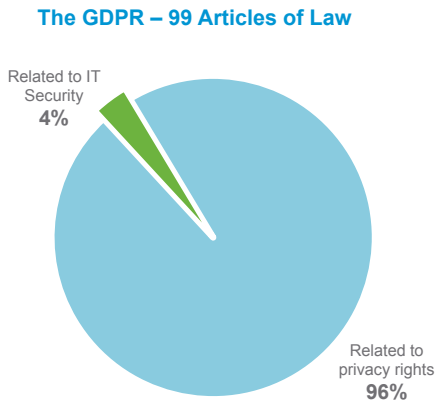

CHART 1: GDPR 99 Articles of Law

Specific IT data protection solutions have generated a lot of interest in the IT security community because, despite being addressed by only a small number of the 99 Articles, the IT security market overall is exploding. Gartner forecasts €70B in annual global expenditure in 2018[4] and both cyber-security breaches and applicable legislation continue to trend upwards (including a big increase in fines and penalties under national laws).

Additionally, protecting personal data is just one part of a comprehensive IT data protection strategy. Financial information unrelated to personal data, intellectual property and many other data, while equally important to an organization, are out of scope for GDPR data flow mapping.

1. For additional clarity, IT will refer to any function within IT from IT Operations, CISO, InfoSec, etc. whereas Organization refers to the whole of the legal, public or private organizations.
2. ISO/IEC Information Technology Vocabulary. ISO/IEC 2121404 Data Protection Implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en. Whereas the GDPR roughly identifies this definition as "Security."
3. The definition for IT Storage differs in that it specifies business continuity and disaster recovery (BC/DR).
4. Forecast: Information Security, Worldwide, 2015-2021, 1Q17 Update 18 May, 2017, Gartner, Inc. Calculation to Euro based on ESD amount of 100, 258.

How Are Organizations Preparing for the GDPR?

Data Risk Assessment

Consultants, outside advisors and existing internal privacy experts can all play a role in helping organizations to prepare for a personal data flow mapping. The outcome of such a mapping activity helps to clarify the data lifecycle of personal data as it flows through the organization. This kind of lifecycle-based approach helps organizations to document how they process personal data—from when and how the data enters the organization—throughout the data "life" to when it is deleted or destroyed. For example, when a customer fills out a web form to learn more about a service that the organization offers, they will enter their name and contact information. The path of that record can be followed and documented throughout the organization to understand who has access to it and how it is protected. The four key questions organizations need to answer, before being able to assess risk and GDPR readiness are as follows:

CHART 2: GDPR Readiness Assessment Process

Step One: A data inventory involves both a business processes analyst and a trusted advisor, who together can determine what personal data exists in an organization.

Step Two: Personal data is mapped throughout the data lifecycle, from how and where data is collected to when it is deleted or destroyed. This effort typically involves all the functional groups interacting with that data throughout its lifecycle.

Step Three: Identifies the technologies, processes and people that an organization currently uses to protect personal data.

Step Four: Involves the assignment of accountability to the groups responsible across the business or IT service such as payroll processing or HR.

The business then documents gaps and shortfalls, analyzes risk and creates a remediation plan where necessary. This process can then help to provide a clear-status on organizational readiness for the GDPR and will inform IT.

While the data mapping audit process will be similar for all organizations, the path to readiness for the GDPR varies as each organization's processes are unique to them. Consequently, each journey to GDPR readiness differs. For a deeper look at a business-wide readiness plan, please view the documentation coming from the national agencies within the EU responsible for GDPR governance (example: this guide from the UK Information Commissioner's Office).

How Can GDPR Preparation Be Made Proactive

IT can begin preparation by mapping data security use-cases to the data lifecycle. Using a basic data lifecycle as illustrated data below, IT can map any personal data from the first stage, collection, through the final stage, deletion, then identify existing security measures and potential improvements.

Using data access as an example, IT can explore access control, identity management, application access and network access. Examples of questions to explore around personal data as follows:

- Which users have access to what data?
- How is data accessed on mobile devices?
- What types of data can cross which networks?
- Can IT protect the access and usage of personal data from the data center to the end user?

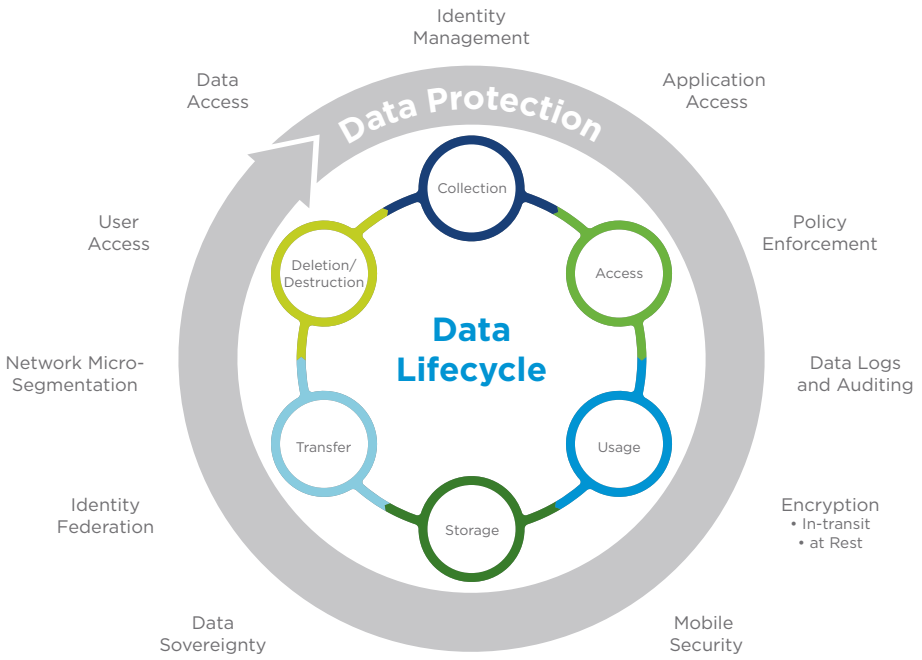

CHART 3: Data Lifecycle and Data Protection

The data lifecycle approach helps create data protection security checkpoints across many of the use cases IT is preparing for in relation to the GDPR.

Examples of how the VMware portfolio can help to address data protection gaps:

Date Category	VMware Security Portfolio	Capability
Data Access Data Transfer	VMware NSX®	Allows for the creation of security policies restricting data transfer across unauthorized networks
Data Access	VMware Horizon®	Provides policy creation and enforcement of role-based access to data
Data Access	VMware Workspace ONE™	Provides Identity verification and management
Data Access	VMware Airwatch®	Enforces mobile access policies to applications and data
Data Access Data Transfer	VMware Workspace ONE™	Allows verification and validation of people, applications, and devices
Data Transfer	VMware vRealize®	Policy creation and enforcement of VM provisioning and transfer
Data Usage	VMware vRealize®	Provides policy creation, automation and enforcement
Data Storage	VMware vSphere®	Enables data encryption at rest
Data Storage	VMware vSAN™	Enables data encryption at rest
Data Storage	VMware Airwatch®	Allows for data encryption or at the end-point
Data Storage	VMware vSAN™	Provides for data storage and policy automation
Data Storage	VMware Airwatch®	Provides governance and enforcement of data storage on mobile devices
Data Transfer	VMware NSX®	Enables Data Encryption in-transit
Data Usage	VMware NSX®	Provides for data privledges policy automation
Data Usage	VMware vRealize®	Provides logging and auditing
Data Deletion	VMware vSphere®	Provides for data virtual machine deletion
Data Deletion	VMware Airwatch®	Provides for end user device deletion

CHART 4: Subset of VMware Security Portfolio Capabilities

GDPR Overview

fieldfisher

GDPR At-a-glance

- Expands the scope of EU data protection
- Better harmonizes the laws across the EU
- Applies to certain organizations who processes EU personal data outside of the EU
- Enhances obligations of transparency and introduces an accountability obligation for organizations with the potential for fines for non-compliance
- The law will be implemented on May 25, 2018

What Changes Will the GDPR Bring?

For organizations that use or process EU personal data the GDPR introduces a number of significant changes as follows:

1. **Expansion of scope:** For the first time certain requirements and obligations will be placed directly on data processors, in addition to those obligations on data controllers. Additionally, the GDPR expands the territorial scope of application of EU data protection law to capture any processing of personal data of data subjects residing in the EU, where the processing relates to the offering of goods or services to them, or the monitoring of their behaviour.
2. **Transparency:** A need for organizations to be more transparent to data subjects about the way in which they handle data and the ability to respond to queries from data subjects who wish to exercise their rights under the GDPR. These rights include, the right not to be subject to automatic decision making (including profiling) in certain circumstances, the right to be forgotten, the right to restriction of processing, and in certain situations the right to data portability.
3. **Penalties for non-compliance:** Potential fines for non-compliance have increased, with the potential for fines of up to €20 million or 4% of the total global annual turnover (revenue) of the preceding financial year, whichever sum is the greatest.
4. **Accountability:** Organizations who handle EU personal data are to be held accountable for that data. This obligation comes in many forms and complying with this principle of accountability needs consideration across an organization.

The impact of these changes has the potential to affect enterprises and public bodies both inside and outside of Europe. Companies caught by the changes should be fortifying their data protection policies and process, identifying compliance and technology gaps and planning to handle data privacy regulations on a global basis.

While compliance has several meanings, compliance within the context of the GDPR extends governance across the entire organization as it relates to personal data and data privacy. Appropriate data protection security processes, controls and technologies to support data privacy objectives, systems compliance and technical compliance will all contribute.

Source: Fieldfisher (Silicon Valley), LLP

GDPR From 2018-On

Three functional areas key to ongoing GDPR compliance are broadly illustrated below.

CHART 5: Ongoing Data Privacy Compliance

GDPR Program Management

Data privacy and compliance will work to maintain the GDPR program and keep the organization in alignment with the GDPR.

Data Privacy Advisors

Experts in legal, business process, and audit partners guide organizations on myriad changes now and in the future.

IT Data Protection

The CISO works with IT groups to ensure IT policies and security align with the organization's compliance goals.

Clearly, while IT has a large role in data protection the, the whole organization is responsible for maintaining compliance with the GDPR.

A Transformative IT Approach to Security

The old approach to security was to bolt on a point solution for each security gap. Today, we are at the point of diminishing returns. More spend no longer equates to more security and too much complexity eventually leads to rigidity in IT at a time when agility is required.

VMware can help to provide ubiquitous security from the hybrid cloud to the end user, and across the data lifecycle. We do this by embedding security into the hypervisor and extending that through to the end-user, reducing the complexity of managing IT security.

This approach gives you a powerful platform on which to build, run or manage any application, anywhere and for creating a more secure environment on which you can create competitive dissonance while staying in compliance.

Conclusion

Preparing for the GDPR can appear daunting at first. Business process analysis, data mapping, and gap analysis are just the start. Legal guidance will become part of the "new normal" in IT as data privacy laws become both more stringent and more standardized across the world. Taking an approach across the data lifecycle gives IT the opportunity to do three things; align with the way the business looks at data protection, identify security gaps along the data lifecycle, and help to protect people's personal information from their devices to the data center.

For more information phone your VMware representative or VMware Accredited Partner.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-GDPR-Solutions-Brief_072417_v6 7/17