Technology Spotlight

Sponsored by: **Pure Storage**

Author:

Martin Whitworth

June 2018

Data at Rest Encryption and Key Management in GDPR

GDPR Arrives

The EU General Data Protection Regulation (GDPR) has been a long time in coming. It is the biggest shake-up in European data protection legislation for 30 years and replaces legislation that predates the dotcom boom, Twitter, Facebook, and the cloud.

GDPR establishes a harmonized data protection framework across the whole EU, giving citizens the same data protection rights regardless of where their data is processed. IDC sees this as a positive move, as it removes many of the complexities currently faced by organizations having to comply with multiple local data protection regulations across Europe. GDPR seeks to make Europe fit for the digital age by positioning it to be relevant to the new cloud, mobile, social, and collaborative era of business and removing barriers to market entry, as businesses benefit from a level playing field.

GDPR seeks to make Europe fit for the digital age by positioning it to be relevant to the new cloud, mobile, social, and collaborative era of business and removing barriers to market entry.

Compliance with GDPR is not to be taken lightly: the penalties for non-compliance could reach up to 4% of global annual revenue or €20 million, whichever is the greater. GDPR also introduces mandatory breach notification, the consequences of which must concern executive boards that worry about reputational damage. This really is a game-changer. The prospect of big fines and other severe sanctions (such as restrictions on the processing of personal data) under GDPR motivated a scramble to implement compliance programs before the deadline.

While not being solely about technology, GDPR introduces substantial changes in the way personal data must be governed and protected. We believe that GDPR compliance will transform how organizations approach enterprise data management, storage, governance, and security — and organizations are looking toward security and storage technologies to protect against breaches and limit their exposure to data loss, reputation damage, and financial penalties.

GDPR and Encryption

GDPR is not at all prescriptive regarding the technologies required to enable compliance. However, the text does make specific reference to, and strongly hints at the implementation of, encryption and pseudonymization as approaches to protect sensitive data.

> *In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.*

GDPR Recital 83

In GDPR, encryption is positioned as a mitigation against both data breach and public breach notification.

> *Security of processing*
>
> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*

GDPR Article 32

Encryption is mentioned throughout the text of GDPR (Recital 83, Articles 6, 32, 34), and in each case it is positioned as an approach to mitigate risks in the processing of data. Importantly, GDPR positions encryption as a mechanism that renders personal data unintelligible to unauthorized individuals, which is a mitigating action against both a data breach and the requirement to make a notification of that breach to the data subjects. In other words, encrypted data is not regarded as personal data for the purposes of breach notification.

There are three main reasons why encryption and pseudonymization receive particular attention in the text of GDPR:

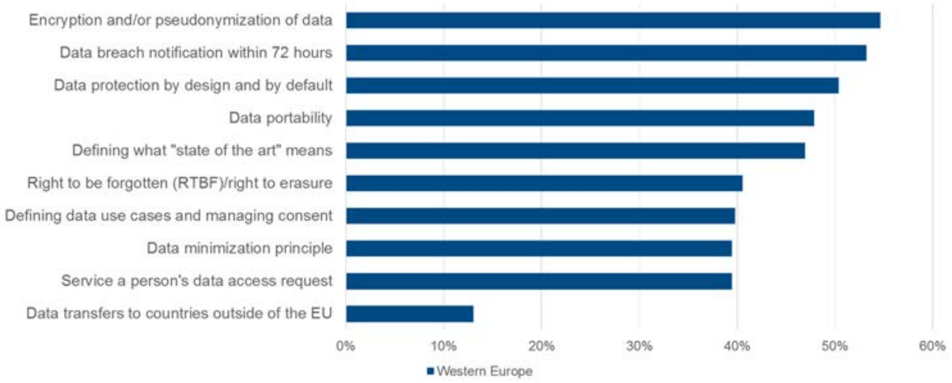
- Encryption can be used to mitigate the risks inherent in systems that store and process data, such as unauthorized disclosure of, or access to, personal data.
- The requirement to notify data subjects (such as consumers or employees) of a data breach is removed if the data is rendered unintelligible using a measure such as encryption.
- The use of pseudonymization can reduce the risks to data subjects while helping data controllers and processors meet their compliance obligations, by minimizing both the exposure of personal data and the opportunities to identify data subjects.

Although not explicitly stated in GDPR, compliance with the extensive rules around data transfers outside the EU can be simplified by encrypting the data and managing keys in-country (including on premises).

Many organizations are therefore examining encryption and pseudonymization technologies, but they quickly discover the complexities and management overheads that can be associated with leveraging the various methods of encryption. They also discover that each method of encryption brings its own set of advantages, disadvantages, and challenges — each of which must be weighed against the identified risks and potential business benefits.

Encryption offers great opportunities to effectively protect personal data but is viewed as a significant challenge. In fact, IDC's GDPR survey identified encryption and pseudonymization as being the most challenging of the GDPR requirements for European organizations (see Figure 1).

Figure 1
Which GDPR Requirement is the Most Challenging?



Source: IDC's 2017 *GDPR Survey*, n = 560

So, What's the Problem With Encryption?

The persuasive benefits of encryption lead many organizations to conclude that they should simply encrypt all (or large parts) of their data — throughout the entire data life cycle (data at rest, data in transit, during processing, backups, archives, etc.). The idea behind this is simplification: encrypting everything avoids onerous data classification and risk assessment exercises. However, encryption is not a panacea for good data management. There are several considerations that organizations must make before they deploy encryption, including the assessment of the data held and an analysis of the legal basis for processing that data. Encryption must not be viewed as an alternative to a comprehensive compliance and risk management program.

Business Functionality

When data is encrypted, the result can have serious unforeseen downsides. Encrypted data may not be usable for normal business processes without application changes — unless seamless decryption is also baked in to the process.

Organizations need data protection, but more importantly they need to function as businesses. Using encryption must not get in the way of this, and so traditional approaches to encryption are not always suitable for this environment. In fact, the problem is much broader: organizations use copies of personal data for a variety of purposes, such as analytics, reporting, and testing. Encrypted versions of this personal data could render these purposes impossible (by preventing processing and analysis of encrypted data) and could hinder competitiveness.

Organizations need data protection, but more importantly they need to function as businesses. Using encryption must not get in the way of this.

Traditional encryption approaches also introduce a potentially significant overhead in terms of processing — usually associated with the application, or input/output subsystem, needing to constantly encrypt and decrypt data during processing. If implemented in software, this performance overhead can be significant, and can also have an effect on overall response times (extended latency and round-trip times for information flow). This can have a severe impact on application and systems performance — again impacting the ability to deliver business functionality or services.

Cost

Because of business process requirements, application-level encryption can often require storing multiple versions of encrypted data — as different applications often require access to different views of the same data and may require using, and managing, many different encryption keys. When data is encrypted at the application layer, all data reduction benefits are lost in the storage layer as encrypted data cannot be compressed or reduced, thus leading to increased storage costs and inefficiencies. Optimizing storage costs, datacenter footprint, and power consumption around storage is extremely important in today's enterprises.

Key Management

Encryption is not trivial. In particular, key management is not trivial. Many organizations naively believe encryption is a relatively straightforward process involving algorithms. In fact, encryption is more about the process of managing keys: get this wrong, and not only is encryption pointless, but there is significant potential for catastrophic data loss. The consequences of losing keys drive organizations to take regular backups of their keys, which of course also must be secured. Few industry verticals, let alone specific organizations, have a strong history of managing encryption keys. Beyond financial services, telecommunications, and the defense sector, most industries have limited experience in using encryption within their business processes. Many organizations avoid encryption purely due to the complexity of key management.

Skills and Resources

Cryptographic, and key management, skills and experience are very specialized and in short supply. Most organizations are not able to build and retain a specialized cryptographic function and nor should they — it is not their core competence. This resource and skills shortage situation is further exacerbated when we consider the need to understand cryptographic implementations in an ever-growing number of network connected devices. One key mitigation for the shortage of available skills and resources is to introduce the capability to automate many of the tasks associated with the management and operation of cryptographic solutions.

Scenarios Where Encryption Works Best ...

The effective use of encryption includes understanding its implications and, as such, should be planned and deliberate. It can be a powerful tool to protect data — for compliance and for protecting intellectual property (IP).

Encryption works best when:

- Simple (but not simplistic) or transparent key management is deployed
- Data encryption and decryption are not application-dependent activities
- It works across all technology platforms, from legacy mainframes to the Internet of Things
- It works at scale and provides coverage across all data classes
- It does not introduce business affecting performance impacts

Pure Storage Approach to the Encryption Challenge

Figure 2
Pure Storage FlashArray

Source: Pure Storage

Pure Storage tackles the issue of encrypting and securing data at rest by achieving a high standard — one that provides transparency/invisibility to the user and zero management and performance overhead. It also provides operational visibility and management of the FlashArray via an accessible, cloud-based, management platform.

Data Security

The Pure Storage approach to securing data at rest is via its Purity Operating Environment running on the FlashArray product, and on the related Purity Operating Environment used on FlashBlade. Providing a high-availability storage solution, with industry-leading data reduction capabilities, these storage systems also provide a secure data protection environment.

The FlashArray product uses an always-on FIPS 140-2 certified implementation of the AES-256 algorithm to encrypt all data and metadata stored on the array. This data encryption occurs transparently to the accessing applications and without impact to performance, while maintaining industry-leading data reduction capabilities.

Key Management

The Pure Storage FlashArray manages the keys used both for device locking and data encryption autonomously, including regularly refreshing them without administrative intervention. This feature removes the need for key management activities to be performed by the users — allowing them to focus instead on the data and the business applications. It also eliminates the need for specialist skills in cryptography and key management, and eliminates the likelihood of human error in key management.

The internal key management uses three layers of dependent keys and supports activities including automatic key rotation, periodic key regeneration, and unreadable partitioned keys that are spread over several FlashArray flash modules.

Additional Data Security

Optionally, Pure Storage provides two external key mechanisms by which the FlashArray can be completely locked down:

- USB connected Spyrus Rosetta II Smartcards. A FlashArray can be completely locked with the removal of the smartcard and power loss to the array. Additionally, data can be made permanently unrecoverable by the physical destruction of the smartcards.
- Key Management Interoperability Protocol (KMIP) remote key server. A FlashArray can be locked down by revoking a remote key and powering off the FlashArray.

Conclusions

Compliance with GDPR, and managing the associated risks, can be difficult and has many facets to it. The regulatory requirements are broad ranging and cut across all areas of the organization, including functions such as IT, HR, finance, procurement, and marketing. Data security cannot solve all the concerns and issues that GDPR raises. Consent, the right to be forgotten, and data portability are just some examples of GDPR requirements that are beyond data security.

However, implementing data at rest encryption is a useful approach to ensure that personal data has a core level of protection. GDPR places encryption at the heart of data protection and security, and understands that encryption is a mitigating factor should a breach occur.

Enterprises must understand the complexity that accompanies encryption and key management in their environment and make risk-based selections of appropriate solutions.

Organizations must be aware, though, that encryption is not always free, in terms of the impact to processing and utility of the data, nor is it trivial. Enterprises have to understand the complexity that accompanies encryption and key management in their environment and make risk-based selections of appropriate solutions.

GDPR compliance may be tough, but it can be substantially simplified using transparent data at rest encryption and key management.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.