Optimizing GDPR readiness with IBM Z

The General Data Protection Regulation

General Data Protection Regulation (GDPR) has been in effect since May 25, 2018. This major legislation change affects organizations dealing with personal data in Europe, but also at a global level by the extra-territorial nature of the GDPR. For example, an organization that does not have a footprint in the EU but offers goods or services, or monitors the behavior of data subjects in the EU would be bound by the GDPR.

The GDPR gives individuals greater control of their personal data and imposes strict rules on those hosting and processing this data—regardless of where that data resides. It also introduces rules relating to the free movement of personal data within and outside the EU.

Failure to comply with the GDPR can potentially lead to significant financial penalties, loss of trust and ultimately damage to an organization's reputation.

At minimum, the regulation includes:

- Data protection accountability. Organizations must demonstrate that considerable security measures are in place to protect users' private data.
- Data subject's right to access, rectification, erasure and portability. Organizations need to validate the individual's identity, swiftly produce personal data it processes, and correct, erase or transfer data on request.
- Data breach notification. A personal data breach "leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" must be reported to the supervisory authority within 72 hours.

GDPR describes significant changes in potential penalties with fines of up to €20 million or 4 percent of total annual turnover of the preceding financial year, whichever is higher.[1]

What do business leaders think about GDPR

According to a survey conducted by Ovum analyst firm[2] on "Data Privacy Legislation Impact on Enterprises" responding business leaders are deeply pessimistic about the potential consequences of new data privacy regulations.

- 52% said "they think it will result in business fines for their company, and two-thirds expect it to force changes in their European business strategy"
- Over 70% "expect to increase spending in order to meet data sovereignty requirements, and over 30% expect budgets to rise by more than 10% over the next two years"[2]

[1] European Commission – Enforcement and sanctions https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en

[2] Ovum report "Data Privacy Legislation Impact on Enterprises", https://www.ovumkc.com/login

© 2019 IBM Corporation

The cost of a data breach
Based on IBM sponsored Benchmark Research conducted by Ponemon LLC "2018 Cost of a Data Breach Study - Global Overview"[3], the average cost of a data breach globally is $3.86 million in 2018, a 6.4 percent increase from the 2017 report.

The report determines that the average global probability of a material breach in the next 24 months is 27.9 percent (a breach that involves a minimum of 1,000 lost or stolen records containing personal information).

The Ponemon report also indicates that an average number of 24,615 records had been breached by country or region in 2018.

According to a survey conducted by Gemalto, now a Thales Company, "2017 The Year of Internal Threats and Accidental Data Breaches", relatively few data breaches occurred where encryption was used. These events constituted 3.12 percent (2017) and 4.19 percent of the total breaches (2016).[4]

These issues have prompted many enterprises to reevaluate the effectiveness of their IT infrastructure and processes to help support their GDPR compliance activities.

IBM Z® – Best fit for security
IBM Z hardware and software solutions are intended to help enterprises handle encryption, access controls and monitoring through to incident breach readiness and reporting.

By design IBM Z provides security capabilities to help customers manage mission critical solutions. Many organizations agree that encryption must be part of their overall strategy for protecting and securing sensitive data. Companies considering encryption also recognize that protecting only the data that is required to achieve compliance is a minimum threshold, and that a move from selective encryption (protecting only specific types of data) to pervasive encryption (encrypting all data) is needed.

Extensive use of encryption can be one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates. Encrypted data is useless to attackers without an encryption key, and in the event of a security breach, encrypted data can potentially reduce the need to report such an incident to a supervisory authority without undue delay.

How encryption can help you to prepare for GDPR readiness
Recital 83 of the Regulation (EU) 2016/679 of the European Parliament and of the Council indicates how encryption can play a significant role in GDPR readiness.[5]

- (83): 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. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

[3] 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security - Independently conducted by Ponemon Institute LLC, https://www.ibm.com/security/data-breach?cm_mmc=Search_Google-_-Security_Optimize+the+Security+Program-_-WW_NA-_-%2Bcost%20of%20a%20%2Bdata%20%2Bbreach%20%2Bstudy_b&cm_mmca1=000000NJ&cm_mmca2=10000253&cm_mmca7=9055324&cm_mmca8=aud-311016886972:kwd-417449382928&cm_mmca9=_k_EAIaIQobChMIs7-R9P2I4gIVUjPTCh034g1jEAAYASAAEgI4rvD_BwE_k_&cm_mmca10=253508236955&cm_mmca11=b&gclid=EAIaIQobChMIs7-R9P2I4gIVUjPTCh034g1jEAAYASAAEgI4rvD_BwE

[4] Gemalto : 2017 The Year of Internal Threats and Accidental Data Breaches https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/

[5] Regulation (eu) 2016/679 of the European parliament and of the council of 27 April 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

© 2019 IBM Corporation

- In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

IBM Z pervasive encryption

Integrated IBM Z hardware, firmware, and software solutions are engineered to provide pervasive encryption capabilities. Such integration can help simplify the implementation of data encryption and is designed to reduce the cost of protecting data and achieving compliance.

The IBM z14™ server includes several features that are specialized for cryptographic processing. They include the following:

- A cryptographic coprocessor chip (Central Processor Assist for Cryptographic Function - CPACF) that works synchronously with the central processors
- A Crypto Express card that is placed in the I/O drawer
- A Trusted Key Entry (TKE) workstation for key management
- An Integrated Cryptographic Service Facility (ICSF), a software component of the operating system, that provides the application programming interface to request cryptographic services

The heart of the operation is the coprocessor assist for cryptographic functions (CPACF). Since this coprocessor executes synchronously with the regular CPU, cryptographic processing will not compete for CPU resources with applications or system processes.

z/OS® data set encryption can be enabled through policies and profiles. Data can be encrypted in bulk with low overhead, while allowing for varying levels of encryption granularity. Operating system components and IBM Z hardware integrated cryptographic engines are designed to deliver industry leading solution using protected key encryption with high performance and high security.

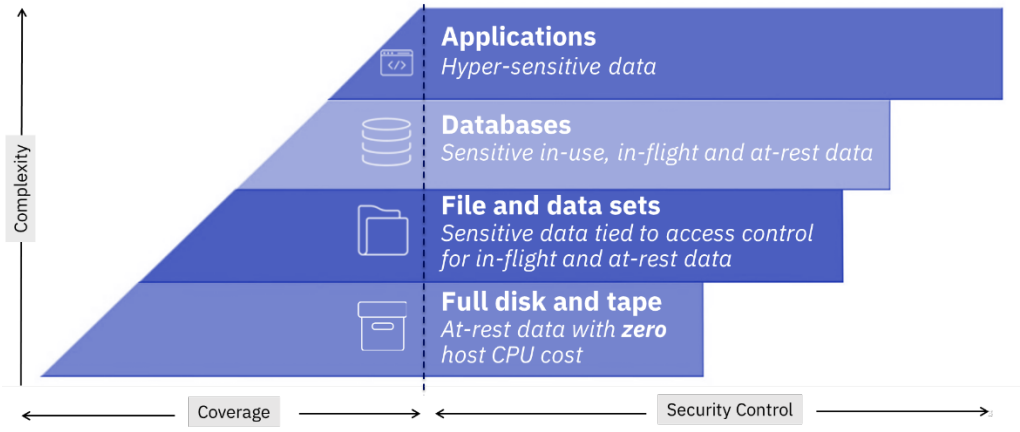
IBM Z pervasive encryption technology is intended to provide the comprehensive data protection your organization and your customers demand. By placing security controls on the data itself, the solution creates an envelope of protection around application and database data that resides on the IBM Z server.

IBM Z pervasive encryption implements comprehensive security with ongoing operations in mind. In other words, the solution doesn’t require users to make application changes, and it can be implemented using policy-based controls with low CPU overhead. These capabilities are engineered to help reduce costs associated with data encryption.

IBM Z provides more than hardware capabilities to help reduce security breaches. Encryption, pseudonymization and data masking help enterprises in their efforts to meet GDPR regulation. Additionally, IBM Z technologies can assist by providing centralized logging, auditing and software alerts, that are designed to help clients manage GDPR notification requirements.

© 2019 IBM Corporation

Multi-layered encryption is essential for data at-rest



Protect enterprise workloads with Secure Service Container

The IBM Secure Service Container for IBM Cloud Private is a software solution that hosts container-based applications for hybrid and private cloud workloads on IBM LinuxONE™ and IBM Z servers. This secured computing environment for microservices-based applications can be deployed without requiring code changes to exploit the security capabilities provides:

- Tamper protection during installation time
- Restricted administrator access to help prevent the misuse of privileged user credentials
- Automatic encryption of data both in flight and at rest

More security solutions on IBM Z to assist with GDPR compliance

IBM security offers one of the most advanced and integrated portfolios of enterprise security products and services. From protecting cloud, mobile and big-data applications to simplifying provisioning, governance and authorization, the IBM Security zSecure suite helps detect threats, comply with policies and regulations, and reduce costs. This portfolio of security solutions can be deployed with IBM Z pervasive encryption to deliver a high-level, security-rich environment, enable rapid creation of new services, which can even help increase top-line revenue.

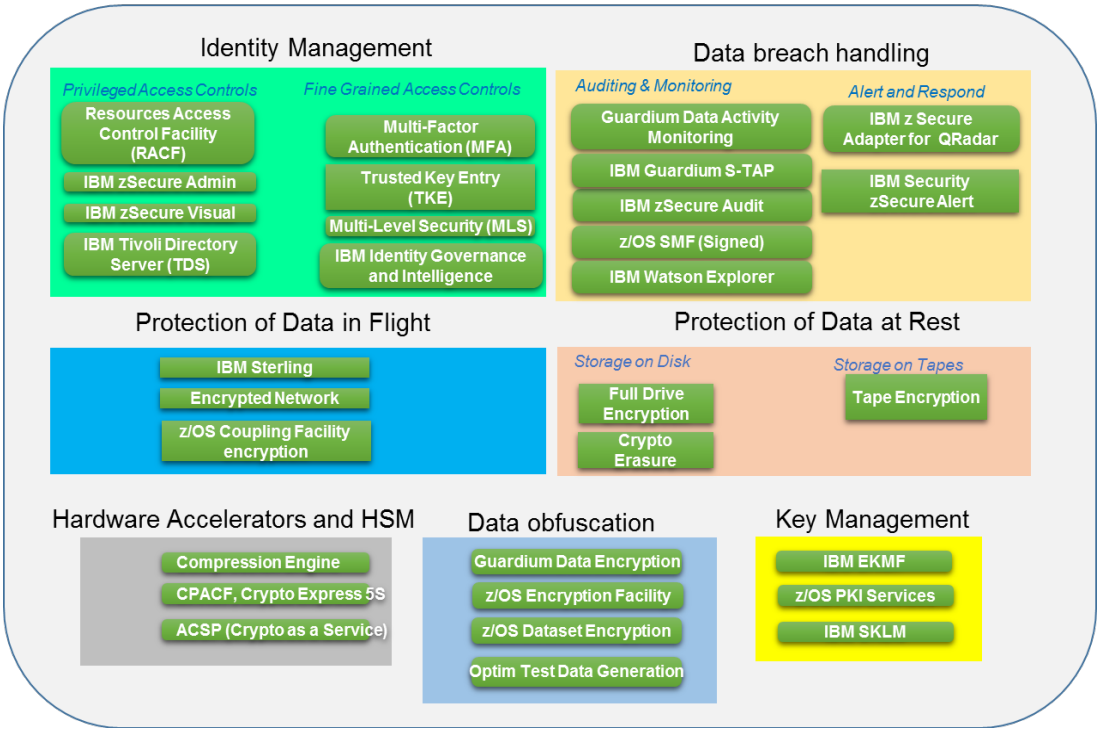
These solutions are designed to provide:

- Privileged identity management
  - IBM Resource Access Control Facility (RACF®), IBM Multi-Factor Authentication for z/OS, and IBM Security Identity Governance and Intelligence allow users to govern, protect and audit users with elevated privileges.
  - This privileged identity management solution helps prevent unauthorized access to sensitive data by rogue insiders or external attackers using compromised administrator credentials.
- Sensitive data protection
  - IBM Security Guardium® and IBM Security Key Lifecycle Manager, along with IBM Z pervasive encryption, can help defend and protect critical assets with unrivaled encryption and intelligent data monitoring, without compromising transactional throughput or response times.
- Integrated security intelligence
  - IBM Security QRadar® and the IBM Security zSecure™ Suite correlate huge amounts of security data to help uncover patterns of unusual activity.
  - This solution uses real-time alerts to call attention to critical security threats.

© 2019 IBM Corporation

Security solutions on IBM Z assist with GDPR compliance
IBM Z traditionally collects information from various subsystems and products that can be used for reporting, monitoring, and analysis. In a GDPR context, enterprises can leverage IBM Z software solutions to help identify, monitor and report data breaches.

IBM Z solutions to assist with GDPR regulations



IT Platforms challenges with encryption technologies
According to Compuware's white paper titled, "The New World of Mainframes' CIO Survey: Mapping the Platform's Future in a Mobile, Big Data World", non- mainframe platforms often disappoint CIOs when it comes to achieving security within projected budgets[6]. The report indicates that 70% of the respondents "have been surprised by the additional work and money required to ensure new platforms and applications will match the security provided by the mainframe."

Compared to several encryption technologies often provided on alternative platforms, pervasive encryption implementation on IBM Z offers attractive benefits to support encryption, including no application changes, simple maintenance and reduced cost:

- The IBM Systems article "IBM z14 Pervasive Encryption Protects All Data"[7] indicates that the z14 pervasive encryption solution offers more than 18x faster encryption at 5 percent of the cost of alternative solutions.

[6] Compuware CIO Survey «The new world of mainframes », https://resources.compuware.com/hubfs/Collateral/White_Papers/The_New_World_of_Mainframes_CIO_Survey.pdf

[7] IBM Systems article : http://ibmsystemsmag.com/mainframe/trends/security/enterprise-encryption/

© 2019 IBM Corporation

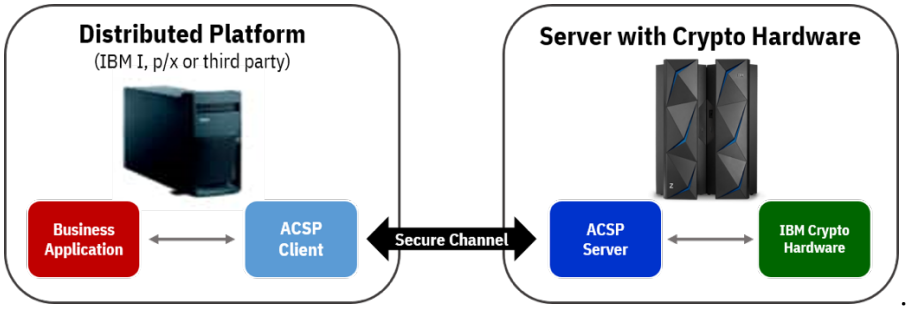
- According to a report done by Solitaire Interglobal Ltd. and sponsored by IBM, “Pervasive Encryption, A New Paradigm for Protection”[8], IBM pervasive encryption solution requires less overhead than other systems. Organizations that deploy pervasive encryption on IBM Z can reduce overall processing overhead by as much as 91.7 percent, according to the report. The report also found a lower total cost of ownership for IBM Z security implementations, by as much as 83.7 percent than that of other platforms.
- Although several alternative platforms can offer encryption technologies, others can require additional equipment for encryption implementation that can increase costs such as Hardware Security Modules (HSM), Trusted Platform Modules (TPM) and dedicated servers.

Advanced Crypto Service Provider - A remote crypto services solution

The Advanced Crypto Service Provider (ACSP), offered by the IBM Crypto Competence Center Copenhagen in Denmark, is a remote crypto services solution that enables applications in distributed environments to access cryptographic hardware over the network.[9]

ACSP is designed for cost effective use of available cryptographic capacity, easy deployment of cryptographic services, and easier key management because the cryptographic key material is centralized, which should simplify management. It also positions users for a much better utilization of the cryptographic hardware, which is particularly true on IBM Z. Multiple decentral HSMs can often be replaced by a single crypto card in IBM Z which helps reduce cryptography management and costs.

ACSP’s secure channel for data between distributed servers and IBM Z



IBM Z assistance for GDPR Readiness

IBM Z offers robust services such as cryptographic hardware, system integrity and more to facilitate GDPR readiness. All IBM z14 models are designed for Common Criteria Evaluation Assurance Level 5+ (EAL5+) certification for the security of logical partitions using the IBM Z Processor Resource/System Manager. This certification means that IBM z14 is designed to prevent an application running on one operating system image on one LPAR from accessing application data running on a different operating system image on another LPAR on the server.

[8] Solitaire Interglobal Ltd :https://www.ibm.com/downloads/cas/R95QY5AV

[9] IBM Crypto Competence Center Copenhagen - https://www.ibm.com/security/key-management[8]
http://ibmsystemsmag.com/mainframe/trends/security/enterprise-encryption/

© 2019 IBM Corporation

IBM Z's ecosystem of security solutions extend protection across many data sources, applications, users and transactions. These solutions can help organizations reduce the business risks of a security breach while helping to minimize the costs of security readiness. Much of IBM Z security is inherent by design, and its features can simplify detection and notification tasks for GDPR.

IBM can help your organization secure and protect personal data with a holistic GDPR-focused framework that includes software, services and GDPR-focused tools. With deep industry expertise, established delivery models and key insights gained from helping organizations navigate complex regulatory environments, IBM is well positioned to help you assess your needs and identify challenges as you implement GDPR standards. Contact the IBM IT Economics Team for additional information.

About the author

Luc Colleville, an IBM IT Economics Consultant[10], works with clients in Europe to identify efficiencies in their IT environments. He has more than 30 years of experience architecting and implementing complex enterprise IT solutions across a broad range of industries and platforms.

During his tenure at IBM Luc has held a number of technical and management positions, working in IBM's industrial sector, IBM Systems and Hybrid Cloud organizations. His main domains of expertise are IBM Z infrastructure, system management and SAP/Oracle environments on IBM servers.

Luc Colleville holds a Master of Engineering (ESTP Paris) and a Master of Business Management from the University of Paris, France.

[10] Learn more about IT Economics at: www.ibm.com/iteconomics

© 2019 IBM Corporation

(C) Copyright IBM Corporation 2019
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

06/19

IBM, the IBM logo, IBM Z, Guardium, LinuxONE, QRadar, RACF, z14, z/OS and zSecure are trademarks or registered trademarks of the International Business Machines Corporation.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

InfiniBand and InfiniBand Trade Association are registered trademarks of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the OpenStack website.

TEALEAF is a registered trademark of Tealeaf, an IBM Company.

Temenos, T24, are trademarks of Temenos AG

UNIX is a registered trademark of The Open Group in the United States and other countries.

Worklight is a trademark or registered trademark of Worklight, an IBM Company.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

No other publication, distribution or use is permitted without the prior written consent of IBM. Customers who want a "deep drill down" on CPO Competitive Case Studies should be directed to the IBM Competitive Project Office under NDA. An NDA is required to explain CPO's methodologies, processes and competitive comparison. You can contact IBM Competitive Project Office by sending an email to ibmcpo@us.ibm.com

References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors and are not intended to be a commitment to future product or feature availability in any way.

IBM GDPR Legal Disclaimer
Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation.

Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability.

IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation. Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey at www.ibm.com/gdpr.

85025985-USEN-00

© 2019 IBM Corporation