Helping Address GDPR Compliance Using Oracle Security Solutions

ORACLE WHITE PAPER | SEPTEMBER 2017

Disclaimer

The purpose of this document is to help organizations understand how Oracle security solutions can be utilized to help comply with certain EU General Data Protection requirements. Some of the security solutions described in this document may or may not be relevant based upon an organization's specific environment and needs. Oracle always recommends testing security solutions within your specific environment to ensure that performance, availability and integrity are maintained.

Further, the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations and regulatory guidelines. Customers and prospective customers should seek their own legal counsel about the applicability of laws and regulations to their processing of personal data, including through the use of any vendor's products or services

Introduction

With all the activity around the new European Union General Data Protection Regulation (GDPR), some organizations are scrambling to understand the impact it will have, including but not limited to:

- Potential fines up to 4% of annual revenue turnover and legal costs and recourse
- Reviewing and modifying organizational processes, applications, and systems
- New and more stringent privacy and security requirements to be addressed

Addressing GDPR compliance requires a coordinated strategy involving different organizational entities including legal, human resources, marketing, security, IT and others. The subject matter may involve information collected from various entities (i.e. customers and employees), as well as coordinated communications and technology used.

Organizations should therefore have a clear strategy and action plan to address the GDPR requirements with an eye towards the May 25, 2018 due date.

Leveraging our experience built over the years and our technological capabilities, Oracle is committed to help customers implement a strategy designed to address GDPR security compliance. This whitepaper explains how Oracle Security solutions can be used to help implement a security framework that addresses GDPR.

Aligning a Security Strategy to Address Threats, Reduce Risk, and Maintain Continuous Compliance

GDPR is not likely the only privacy and security regulation your organization addresses. In fact, many enterprises must maintain compliance with multiple laws and regulations, as well as global industry standards. These laws and regulations are intended to protect citizens, the economy, government and industry to name a few. It is important to have an overall strategy that easily accommodates this ever-changing regulatory landscape.

The drive for more and more security regulations can, in part, be explained by the rise in data breaches and cyber security incidents. Whether involving espionage, organized crime, or insider-related, cyber criminals are gaining illicit benefit from ill-designed Information Technology (IT) systems. This ultimately jeopardizes the free flow of information which is one of the keys to a thriving economy and society.

To formulate an appropriate strategy to address compliance and mitigate risk, organizations require an overarching compliance framework that incorporates international industry best practices, such as ISO 27000 family of standards and others.

GDPR promotes the use of best practices and well established security concepts. GDPR requires “controllers” (such as a customer contracting for services) and “processors” (such as cloud services providers) to adopt appropriate security measures designed to ensure a level of security appropriate to the level of risk that might affect the rights and freedoms of the individuals whose data is being collected and used by the controller (“data subjects”). The law

then insists on risk analysis and implementing security measures (also known as security controls) to address those risks.

Overall, GDPR addresses the key security tenets of confidentiality, integrity and availability of systems and data. Oracle has a long history, and proven record, of securing data and systems. Oracle security includes a full set of hybrid cloud solutions, from the chip to applications, that help prevent, detect, respond to, and predict security threats; it can also help address regulations like the GDPR.

The benefits of strategically implementing the right technology, with effective security controls, can help:

- Address regulatory requirements
- Reduce risk (whether driven by regulatory compliance or other needs)
- Improve competitive advantage by enabling increased flexibility and quicker time to market
- Enable digital transformations

Ultimately, implementing effective security will offer organizations the opportunity to improve their IT security and IT security organization.

Key Articles that Impact IT Security

Containing 99 articles and 173 recitals, GDPR includes some key requirements that directly impact the way organizations implement IT security.

The protection of the individuals whose personal data is being collected and processed is a fundamental right that necessarily incorporates IT security. In modern society, IT systems are ubiquitous and GDPR requirements call for good IT security.

In particular, to protect and secure personal data it is, among other things, necessary to:

- Know where the data resides (data inventory)
- Understand risk exposure (risk awareness)
- Review and, where necessary, modify existing applications (application modification)
- Integrate security into IT architecture (architecture integration)

The following table highlights the most relevant GDPR articles that speak to IT security:

IT SECURITY CATEGORY AND GDPR ARTICLE

IT Security Category	GDPR Article Reference
Data inventory	» *Art. 30 Records of processing*
Risk awareness	» *Art. 35 Data protection impact assessment*
Application modification	» *Art. 15 Right of access by the data subject* » *Art. 16 Right to rectification* » *Art. 17 Right to erasure ('right to be forgotten')* » *Art. 18 Right to restriction of processing* » *Art. 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing* » *Art. 20 Right to data portability*
Architecture integration	» *Art. 32 Security of processing* » *Art. 5 Principles relating to processing of personal data* » *Art. 24 Responsibility of the controller* » *Art. 25 Data protection by design and by default*

	» *Art. 28 Processor* » *Art. 34 Communication of a personal data breach to the data subject*

Creating and maintaining a data inventory is a requirement under article 30 (records of processing) of the GDPR, and more generally, also the starting point of any activity related to personal data collection and handling.

Risk mitigation is an important part of good IT security. Organizations must mitigate the risks that can lead to a personal data breach and should consider executing a security and risk assessment. To learn more about how Oracle can help with the assessment, see your local Oracle representative.

For certain rights of the data subject (Art. 15 to 20) you may need to implement changes that enable these rights (e.g. “right to be forgotten”). Because the changes are implemented within specific applications that may hold data subject information, it is necessary to know the specific data model and business logic to execute the requested function.

Additional measures can be implemented within the architecture. For example, this is the case for network or database encryption. Measures that are possible to implement in the architecture are normally easier and less expensive than application modifications, and are generally more robust because they are not constrained by the need to know application data models and business logic. In large companies, where deep IT system stratification and lack of application knowledge often occur, this can be an easier approach to help protect personal data.

Oracle Solutions and GDPR

Oracle has an extensive value proposition to help address GDPR requirements that impact data inventory, risk awareness, application modification, and architecture integration. The following diagram provides a high-level representation of Oracle’s solutions framework, which includes a wide range of products and cloud services.

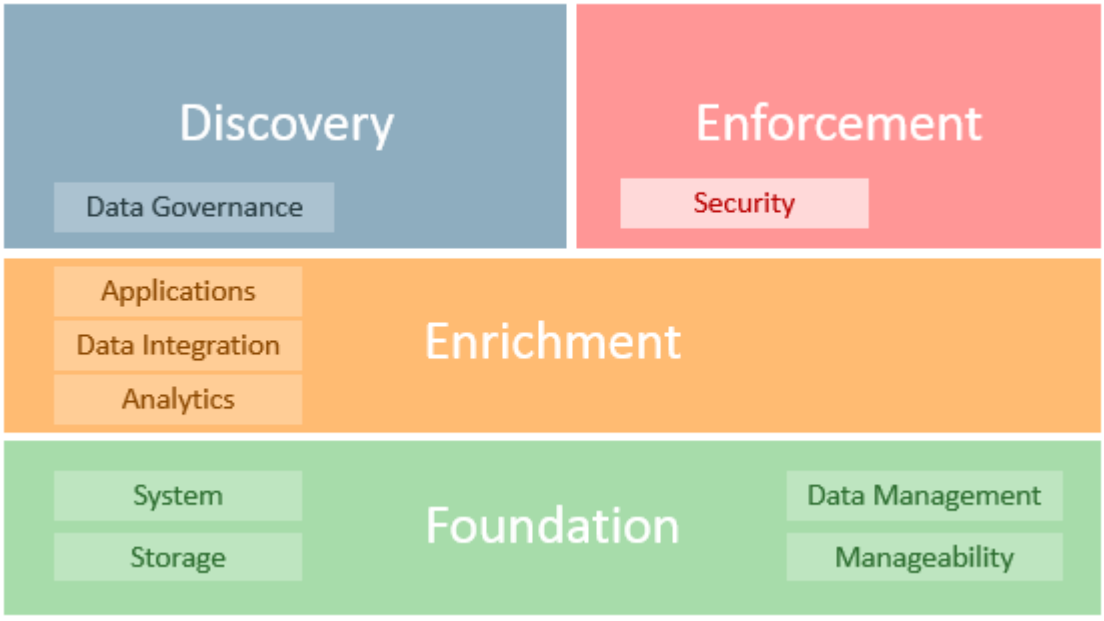

Figure 1. Oracle solutions framework for GDPR.

Discovery. On premises products and cloud services that can help discover personal data and map data flows. This technology includes the discipline of data governance and provides capabilities such as data lineage, asset inventory, and data discovery.

Enrichment. Enrichment includes application modifications that may be necessary to comply with rights of the data subject (Art. 15-20). As well, it may be necessary to consolidate customer data to get a single view of the data subjects across the organization.

Foundation. The comprehensive set of mature operational technologies that are a part of Oracle's DNA to enable good IT security with an emphasis on availability and performance of the services. This includes hybrid cloud solutions from maximum availability architecture and engineered systems to operating systems and processors. These solutions can help address *"availability and resilience of processing systems and services; and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident"* (Art. 32).

Enforcement. Oracle hybrid cloud technologies that enforce security policies and controls that protect people, software, and systems. This encompasses products and services that provide predictive, preventive, detective and responsive security controls across database security, identity and access management, monitoring, management, and user behavior analytics.

The next section of this whitepaper goes deeper into *enforcement*. Additional GDPR information can be found here: https://oracle.com/goto/gdpr.

Security Solutions (Enforcement)

Data controllers and processors must implement appropriate security measures designed to ensure the level of security is appropriate to the risks associated with the data that is being processed, as outlined in article 32 GDPR ("security of processing").

Article 32 references pseudonymisation and encryption as examples of possible appropriate security measures. **The GDPR ultimately leaves the decision and responsibility with the organizations responsible for implementing a security framework to choose the appropriate measures that guarantee confidentiality, integrity, availability, and resilience of data and systems.** A common misconception, often dispersed by security vendors, is that the GDPR lists out specific technologies to be applied. In reality, the GDPR holds the controller and the processor accountable and requires that they consider the risks associated with the data they handle and adopt appropriate security controls to mitigate these risks. Organizations do not necessarily address even the most basic security controls that include, for example:

- Encrypt sensitive data at rest and in transit
- Patch systems within a reasonable timeframe
- Collect system logs to find anomalous activity
- Maintain "least privilege" or "separation of duties" for privileged accounts
- Control access to, or distribution of, production user credentials
- Mask production data that is copied to development environments

The enforcement section of the Oracle solutions framework includes four groups that encompass basic security measures that organizations should consider implementing.

Protect the Data. Deploying encryption for data at rest and in motion is one of the most common first steps to data protection because it is relatively simple and effective. Encryption is often implemented because it is designed to

prevent unauthorized access, it is transparent to applications and users, it provides a strong preventive control, and modern solutions typically experience low performance impact. Additional data protection technologies include management of encryption keys, redaction of application layer data, and masking of sensitive production data for use in nonproduction environments for testing and development purposes.

Access Controls. Encryption of data without security controls that determine who has authorized access, is meaningless. Therefore, it is necessary to implement access and identity management technology for both application users and IT personnel, including system administrators.

Monitor, Block and Audit. With today's innovative security threats, it is critical to implement intelligent and automated monitoring of security and performance incidents. Software components and applications produce logs and audit trails. To mitigate data breaches, it is critical to collect and analyze internal and external threat feeds and logs to detect and mitigate threats.

Secure Configurations. For appropriate security hygiene, software should be updated, well configured, and regularly patched. Secure configuration management is increasingly required as part of international best practices because cyber criminals often take advantage of vulnerabilities in unpatched software to steal sensitive data.

These four security requirements are a part of many global regulatory requirements and well-known security best practices (i.e. ISO 27000 family of standards, NIST 800-53, PCI-DSS 3.2, OWASP and CIS Controls). To expand on Figure 1, we drill in deeper to the enforcement section of the Oracle solutions framework that help address the GDPR.

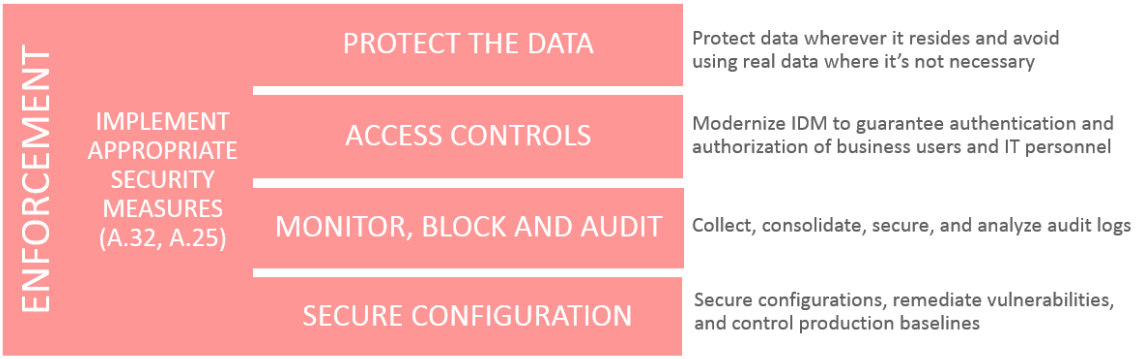

Figure 2. Detailed view of enforcement as part of the Oracle solutions framework.

Oracle Security Products that Can Help Address GDPR

Oracle provides on prem and cloud security products for hybrid cloud environments that are designed to help protect data, manage user identities, and monitor and audit IT environments. The following table provides a brief product description organized by the type of security measure. Each product provides more functionality than described, so be sure to ask your Oracle sales representative for more details.

ORACLE SECURITY SOLUTIONS THAT CAN HELP ADDRESS GDPR

Oracle Product	Security Measure	Cloud Service	Short Description
Advanced Security	Protect the data		Encrypt Oracle Databases transparently and redact sensitive application data
Key Vault	Protect the data		Securely manage encryption key lifecycle as well as passwords, certificates and more.
Data Masking and Subsetting	Protect the data		Anonymize production data for testing and development environments.

Database Vault	Access controls		Control privileged user access using least privilege and separation of duties enforcement.
Identity Cloud Service	Access controls	X	Manage identities from the cloud for hybrid access, authorization, authentication, provisioning, and SSO.
Identity Governance	Access controls		Manage the identity lifecycle: user administration, privileged account management, and identity intelligence.
Access Management	Access controls		IT asset protection and identity federation for multiple scenarios.
Directory Services	Access controls		Manage large, fast read-write user directories.
Label Security	Access controls		Allow individual data records to be labeled with metadata that describes the characteristics of the data, and then enforces access to those records based on the metadata.
Audit Vault and Database Firewall	Monitor, Block and Audit		Centralized auditing, monitoring, reporting and alerting of anomalous database activity management.
Security Monitoring and Analytics Cloud Service	Monitor, Block and Audit	X	Monitor security incidents across heterogeneous and hybrid cloud environments.
CASB Cloud Service	Monitor, Block and Audit	X	Discover unsanctioned cloud services and implement consistent security policies across sanctioned SaaS, PaaS, and IaaS environments.
Configuration and Compliance Cloud Service	Secure compliance	X	Implement and maintain continuous configuration and compliance for IT assets.
Enterprise Manager: Configuration Mgmt.	Secure compliance		Check that IT assets are properly installed and securely configured.

As a beginning step to enforcement, Oracle suggests implementing Oracle Advanced Security with transparent data encryption because of two important factors: encryption is considered a good practice and databases often contain important data that can benefit from strong encryption.

"Data Protection by Design"

An important concept embedded in GDPR is "Data protection by design and by default" (Art. 25) that states *"both at the time of the determination of the means for processing and at the time of the processing itself, it is necessary to implement appropriate technical and organizational measures"*. The concept of data protection by design is close to the similar "security by design", which Oracle technology supports very well by pushing policies and controls close to the data.

The benefits of deploying Oracle security solutions as part of architecture integration (referenced in table 1) include:

- Simplified security protection deployed as part of proven Oracle technologies
- Software updates and patches
- Eliminating the need for error-prone development, which can introduce programming and system errors that may expose personal data to a breach

A Use Case Example

The following business use case is intended to illustrate how Oracle products can be used to make IT systems more secure and help address the EU GDPR.

Business use case: Healthcare

This fictional organization is a large private hospital. The private healthcare market is consolidating and this organization recently acquired another company that provides medical diagnosis and short term hospitalization services in several cities. The acquired company has grown through acquisitions, but at a smaller scale.

They started a large project with the following business objectives:

- Consolidate customer databases to enable integrated and discreet marketing activities that market preventive diagnosis
- Improve customer experience related to reservations (online, mobile) and withdrawal of medical reports
- Guarantee compliance with national and regional laws, and including GDPR
- To be perceived as a secure and modern company, respectful of patient privacy

As well as the following IT objectives:

- Modernize dispersed IT systems (the result of multiple mergers) without disrupting the business.
- Manage employee identities (doctors, nurses, administration, etc.) and provide single sign-on capabilities to reduce the risk of fraud and administrative burden.

For technical reasons, they do not want to change all systems at once, some legacy will be addressed at a later time, others will be modified in stages. They also use some packaged applications from an ISV, and one of their three important applications was developed by a company that is no longer in business and they are no longer able to maintain and evolve the software code. Finally, they use outsourcing services in local data centers (must be maintained for the next two years at least) that include hardware, network, operating systems and Oracle Databases.

Building a plan

Initially they considered GDPR as an obstacle to their business objectives, but their CEO realized that business objectives aligned with the need to implement good IT systems and good security. With enough insight, the organization began deploying security within the architecture and gradually achieved both business and IT objectives.

Supporting technology

The first challenge was related to finding where sensitive personal data was stored. For the Oracle databases, they integrated the information with Application Data Model (ADM). The ADM stores the list of applications, tables, and relationships between table columns that are either declared in the data dictionary, imported from application metadata, or specified by a user.

The second challenge was to assess the organizations security posture. Using Oracle Consulting Services to review the security of Oracle databases, the organization interviewed IT personnel and outsourcers, implemented assessment tools (Database Security Assessment Tool and a beta program of Configuration and Compliance Cloud Service), they produced a report that was used to plan remediation projects and technology adoption—all within a week. This report has been stored as a key component of the GDPR adjustment project to demonstrate company accountability (as per GDPR Art. 24) and was presented to the Board of Directors by the Data Protection Officer.

The following was highlighted among the most important remediation actions:

- **Migrate to Oracle Database 12*c* from unsupported versions 10 and 9**. They had to ask their applications vendors to certify the new version but in one case (the bankrupted one) that was not possible. The DB was not migrated but as a compensating measure was implemented using the Oracle database firewall technology present in Oracle Audit Vault and Database Firewall.

- **Deploy encryption and access controls**. The healthcare organization determined they must encrypt database data with Oracle Advanced Security (suggested in Art. 32). Using Oracle Database Vault, they ran privilege analysis to check all account privileges, and created personal accounts with restricted access using the "need to know" principle. They found that system administrator passwords had not been changed for many years.
- **Centralize database user accounts**. The organization centralized all database user accounts into a directory using a feature of the database called Enterprise User Security and an existing instance of an Oracle directory.
- **Mask data in nonproduction environments**. The organization found the need to eliminate the use of real data that was being copied from production environments to development and test. That was achieved in two ways: providing empty systems to developers, and applying anonymization technology provided by Oracle Data Masking and Subsetting.
- **Re-activate logging mechanisms that had not been used for years.** Log production and analysis lays at the base of any security strategy. The organization chose to collect database logs with Oracle Audit Vault, and systems logs with Oracle Log Analytics Cloud Service. Oracle Storage Cloud Services was then used to reduce the on premises footprint of Audit Vault and applications log storage. Some applications have been modified to pass application user data to the database and is being used to provide accountability and an improved logging analysis.

In parallel, the healthcare organization integrated the current portal with Oracle Identity Cloud Service (IDCS) to manage a seamless user experience for their customers and provide a sense of security (SSO, strong authentication, adaptive access). They used the same technology (IDCS) to provide authentication and SSO for internal users. The identities have been synchronized with an existing on premises Active Directory. Finally, a project to reduce and centralize on premises identities has been started.

The healthcare organization uses Oracle CASB (Cloud Access Security Broker) Cloud Service to monitor the use of unsanctioned cloud services being used from the company network. They can be used to avoid the loss of personal data in the cloud and to monitor Microsoft email services. The deployment took one week to get up and running in production. They decided to adopt the Identity SOC technology (combination of Identity, CASB, Security Monitoring and Analytics, and Configuration and Compliance Cloud Services) provided by Oracle and substitute an outsourcing contract that is currently limited to the Network Operation Center. Moving forward, Oracle suggests the healthcare organization use the same company to provide the analysis, however, implementing Identity SOC for a more modern and extended solution that includes close loop remediation.

Conclusion

Non-compliance with GDPR can result in heavy fines and increased regulatory actions. More importantly, however, significant breaches can damage an organization's brand, value, and reputation. Protecting the brand requires that an organization that collects personal data must be able to prove it consistently and reliably complies with the GDPR privacy and security principles.

The path towards GDPR compliance includes a coordinated strategy involving different organizational entities including legal, human resources, marketing, security, IT and others. Organizations should therefore have a clear strategy and action plan to address the GDPR requirements with an eye towards the 25 May, 2018 deadline.

Based on our experience and technological capabilities, Oracle is committed to help customers with a strategy designed to achieve GDPR security compliance. To learn more about how Oracle help, please contact your local sales representative and visit https://oracle.com/goto/gdpr.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oraclesecurity
facebook.com/oraclesecurity
twitter.com/oraclesecurity
oracle.com/security

Integrated Cloud Applications & Platform Services

Helping Address GDPR Compliance Using Oracle Security Solutions
September 2017
Author: Alessandro Vallega, Troy Kitch
Contributing Authors: Angelo Bosis