Accelerate Your Response to the EU General Data Protection Regulation (GDPR)

Using Oracle Database Security Products

ORACLE WHITE PAPER | JUNE 2016

AUTHOR: DINESH RAJASEKHARAN | SENIOR PRODUCT MANAGER | DATABASE SECURITY

Executive Summary 2

Introduction to the General Data Protection Regulation (GDPR) 2

Key Security Objectives of GDPR 2

Core Actors of the GDPR 3

- Hypothetical Example 4

Key GDPR Data Security Requirements 5

- Assess Security Risks 5
- Prevent Attacks 6
- Monitor to Detect Breaches 7
- Quality of Protection 8

Oracle Database Security and the GDPR 9

- Assess Security Risks 10
- Prevent Attacks 11
- Monitor to Detect Breaches 15
- Maximum Protection with Transparency, Accuracy, Performance, and Scale 16
- Hypothetical Example 17

Conclusion 18

References 18

Appendix: Mapping of Oracle Database Security Products to GDPR 19

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

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of any vendor's products or services.

Executive Summary

As organizations prepare for the new European Union (EU) General Data Protection Regulation (GDPR) by considering changes in processes, people, and technical controls, it is important for organizations to consider how Oracle's products can help to accelerate adoption of the GDPR's assessment, preventive, and detective controls. These easy-to-use tools provide transparent controls for implementing many of the data security principles mandated by the GDPR.

This paper summarizes several key requirements of the GDPR and maps them to Oracle Data Security features. While the GDPR mandates many different data protection and governance principles and requirements (such as cross border data transfers), this paper covers only those key GDPR data protection security principles that may be addressed by Oracle Data Security features.

Introduction to the General Data Protection Regulation (GDPR)

The European Union (EU) introduced its data protection standard 20 years ago through the Data Protection Directive 95/46/EC. Because a Directive allows Member States a certain margin of maneuverability when implementing it into national law, Europe ended up with a patchwork of different privacy laws. In addition, increasing security breaches, rapid technological developments, and globalization over the last 20 years has brought new challenges for the protection of personal data. In an effort to address this situation, EU developed the General Data Protection Regulation (GDPR).

Key Security Objectives of GDPR

The following are key GDPR security objectives.

Objective	Description
Establish data privacy as a fundamental right	The GDPR considers data privacy as a fundamental right of an individual, which includes a "right to the protection" of their personal data. Anyone based in the EU, or anyone handling or targeting the personal data of an EU-based individual must have processes, technology, and automation to effectively protect personal data.

Clarify the responsibilities for EU data protection	The GDPR applies to anyone based in the EU, or anyone handling the personal data of an EU-based individual or targeting him/her by offering goods or services from outside the EU borders ,
Define a baseline for data protection	To avoid fragmentation and ambiguity, GDPR has set a baseline for data protection by requiring anyone handling the personal data of an EU individual to follow the GDPR guidelines.
Elaborate on the data protection principles	The GDPR considers encryption as only one of the components of a broad security strategy, and mandates that organizations need to consider assessment, preventive, and detective controls based upon the sensitivity of the data they have.
Increase enforcement powers	EU aims to ensure the compliance with the GDPR by enforcing huge fines up to 4% of global annual revenue upon non-compliance.

Core Actors of the GDPR

The GDPR defines various actors to explain the data protection concepts and their associated roles:

Actor	Description
Data Subject	A person who can be identified directly or indirectly by means of an identifier. For example, an identifier can be a national identifier, credit card number, username, or web cookie.
Personal Data	Any information, including sensitive information, relating to a Data Subject. For example, address, date of birth, name, and nationality.
Controller	A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. For example, a controller can be an organization or CIO.
Data Protection Officer	An individual within the Controller with extensive knowledge on the data privacy laws and standards. Data Protection Officer (DPO) shall advice the controller or the processor of their obligations according to the GDPR and monitors its implementation. DPO acts as a liaison between the controller and the supervisory authority. A DPO for example can be a Chief Security Officer (CSO) or a Security Administrator.
Processor	A natural or legal person, agency or any other body which processes Personal Data on behalf of the Controller. For example, a developer, a tester, or an analyst. A Processor can also be an automated entity such as a server or a website, or a cloud service provider.
Recipient	A natural or legal person, agency or any other body to whom the personal data is disclosed. For example, a tax consultant, insurance agent, or agency. Unlike a Processor, a Recipient cannot process but can only see or read the information.
Enterprise	Any natural or legal person engaged in an economic activity. This essentially includes all organizations whether in public or private sector, whether in EU or outside of EU.

Third party	Any natural or legal person, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data. For example, partners.
Supervisory Authority	An independent public authority established by a Member State such as court or auditing agency.

Hypothetical Example

To understand the various actors and their roles and how they relate to one another, let us consider a hypothetical gadget manufacturing company XYZ based in Belgium ("Enterprise"). Customers of XYZ place online orders through the company's web portal. As part of its multi-national business model, XYZ stores and processes personal information about EU individuals ("Data Subjects"). This EU-based company has one of its main data centers ("Controller") in Europe which it stores the information of Data Subjects. The development ("Processor"), testing ("Processor"), customer care & billing ("Processor") efforts are outsourced to Brazil and India where the employees ("Processors") often copy their customer's data ("Personal Data") to their local systems for development, testing, and processing, respectively. XYZ also partners with the payment and delivery companies ("Third parties") of different countries and provides them an individual's data ("Personal Data") for processing an order. An auditing firm represented by an EU government body ("Supervising Authority") audits the security of XYZ periodically.

The following picture shows a sample geographical distribution of the above-mentioned actors.

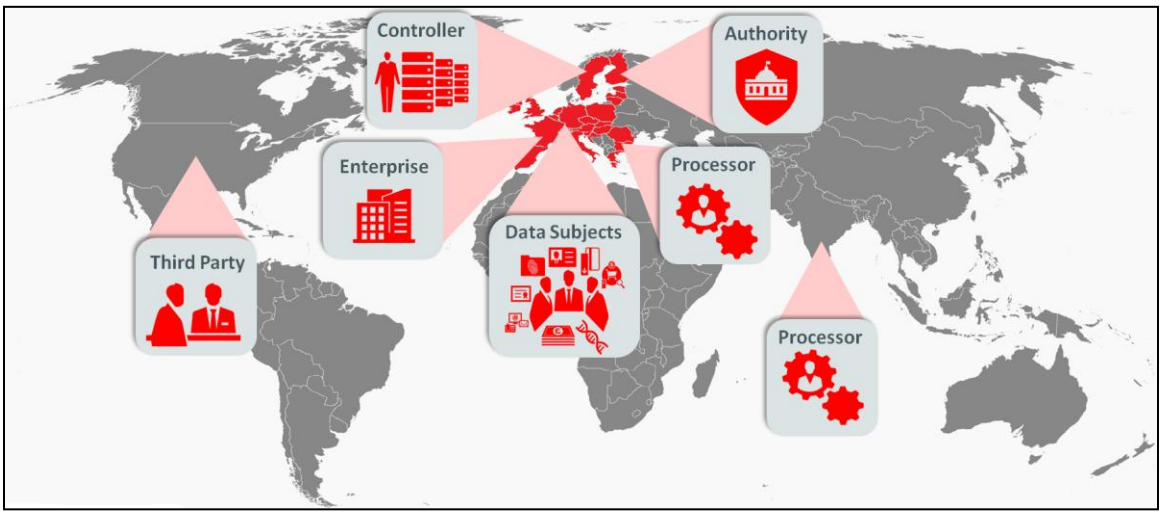

Figure 1: GDPR Actors with EU Enterprise and Controller

GDPR can apply to Enterprises, Controllers, Processors, and Third Parties located outside of EU but are handling EU Data Subject's information. For example:

- An Australian company offering goods and services to EU residents operating a global website from the US.
- An Indian company tracking profiles of EU residents (e.g., social networking site or non-EU websites).
- A supplier (internal or external) based in Canada with no "establishment" in the EU and none of its servers located in the EU, offering cloud computing services to EU citizens.
- A marketing campaign driven out of a Chinese-based company, targeting EU citizens (among others), offering various services.

» Non-EU based cloud providers who may directly or indirectly (through clients and partners) host personal data of EU individuals.

» US based hotel chain or an airline company that stores information of EU individuals travelling to US.

In the following picture, Enterprises and Controllers are located outside of EU, but are still subject to GDPR.

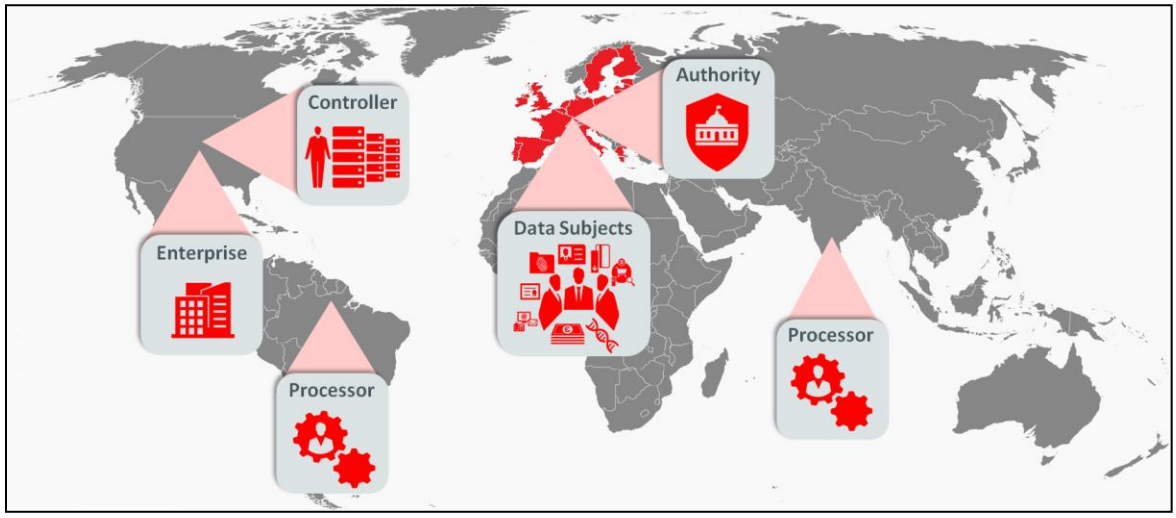

Figure 2: GDPR actors with Non-EU Enterprise and Controller

Key GDPR Data Security Requirements

The key GDPR data security requirements can be broadly classified into three categories: Assessment, Prevention, and Monitoring/Detection. The GDPR also recommends facilitation of the data privacy principles to enhance the quality of protection. This section summarizes key data security requirements discussed in the GDPR.

Assess Security Risks

The GDPR mandates that Controllers perform Data Protection Impact Assessments when certain types of processing of Personal Data are likely to present a "high risk" to the data subject. The assessment must include a systematic and extensive evaluation of organization's processes, profiles, and how these tools safeguard the Personal Data.

> *… The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks …* *-- Article 35 of GDPR*

Data protection impact assessments lay a foundation for preventing breaches by evaluating the gaps and risks.

Prevent Attacks

At various places in the regulation, the GDPR reiterates the importance of preventing security breaches. The GDPR recommends several techniques to prevent an attack from succeeding:

» **Encryption**

The GDPR considers encryption as one of the core techniques to render the data unintelligible to any person who is not authorized to access the personal data.

> *… 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;* -- *Article 32 of GDPR*

The GDPR provides that in the event of a data breach, the Controller need not to notify data subjects if data is encrypted and rendered unintelligible to any person accessing it, thereby removing notification costs to the organizations.

> *The communication to the data subject … shall not be required if... data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption …* -- *Article 34 of GDPR*

» **Anonymization and Pseudonymization**

Data anonymization is the technique of completely scrambling or obfuscating the data, and pseudonymization involves partially scrambling the data. The GDPR states that anonymization and pseudonymization techniques can reduce the risk of accidental or intentional data disclosure by making the information un-identifiable to an individual or entity.

> *... The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations …*
>
> -- *Recital 28 of GDPR*

» **Privileged User Access Control**

The GDPR implies controlling privileged users who have access to the sensitive Personal Data to prevent attacks from insiders and compromised user accounts.

> *… Processor and any person ... who has access to personal data shall not process them except on instructions from the controller…* -- *Article 32 of GDPR*

» **Fine-grained Access Control**

In addition to privileged user control, the GDPR recommends adopting a fine-grained access control methodology to ensure that the Personal Data is accessed selectively and only for a defined purpose. This kind of fine-grained access control can help organizations minimize unauthorized access to sensitive information.

… Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. *-- Article 25 of GDPR*

» **Data Minimization**

GDPR recommends minimizing the collection and retention of Personal Data as much as possible to reduce the compliance boundary. While collecting, processing, or sharing Person Data, Controllers and Processors must be frugal and limit the amount of information to the necessities of a specific activity.

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). *--Article 5 of GDPR*

Monitor to Detect Breaches

While preventive security measures help organizations minimize the risk of attack, they cannot eliminate the possibility that a data breach may occur. GDPR recommends monitoring and alerting to detect such breaches through the following mechanisms:

» **Audit data**

GDPR not only mandates recording or auditing of the activities on the Personal Data but also recommends that these records must be maintained centrally under the responsibility of the Controller. In other words, processors and third-parties must not be able to tamper or destroy the audit records. In addition to book-keeping, auditing also helps in forensic analysis in case of a data breach.

Each controller …. shall maintain a record of processing activities under its responsibility. *-- Article 30 of GDPR*

» **Monitor and timely alert**

Constant monitoring of the activities on Personal Data is critical for detecting anomalies. In addition to close monitoring, GDPR also mandates timely notifications in case of a breach.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority … *-- Article 33 of GDPR*

The three broad categories of security guidelines (assessment, prevention, and detection) help organizations address threats from multiple angles and secure the data from unauthorized access.

Quality of Protection

For both large and small organizations, implementing and administering data security without proper planning can obstruct day-to-day IT operations and result in a significant administrative overhead. While lack of proper planning and increased costs may have in the past given some enterprises a reason to not implement security, with regulations such as the GDPR, security is a requirement, not an option. To address some of these challenges, GDPR recommends the following guidelines to help ease the administrative overhead of the security controls and increase the quality of protection:

» **Centralization**

The GDPR recommends centralized administration when dealing with security of multiple applications and systems as they help take immediate actions in case of a breach. Centralized controls also enforce uniformity across multiple targets, reduce the chances of errors on individual targets, and leverage the best practices across the enterprise.

> *The main establishment of a controller in the Union should be the place of its central administration in the Union ...and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing...* *-- Recital 36 of GDPR*

» **Data Security by design and by default**

The GDPR mandates making data protection a core part of the system. Considering security during the initial design phase of a technology life cycle increases the security worthiness of the system and ensures that technical security controls will perform as expected

> ***Data protection by design and by default***
>
> *… … The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects* *-- Article 25 of GDPR*

» **Comprehensive Security**

Threats and attacks can come from multiple sources and organizations must be prepared from all directions. The GDPR mandates protection of Personal Data in all the stages of data lifecycle such as data at-rest and in-transit.

> *Appropriate level of security account shall be taken ... from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.* *-- Article 32 of GDPR*

Oracle Database Security and the GDPR

Organizations typically have multiple layers of security surrounding the database through firewalls, intrusion detection systems, and proper networking, hoping that attackers would not be able to reach the databases directly. However, as the traditional network perimeters are becoming blurry, and the number of people (administrators, test and development, and partners) who have direct access to the databases is growing; it is becoming very important to directly secure databases. In order to shrink the attack surface, and reduce the number of ways in which attackers can reach the databases, it is extremely important to enforce security as close to the data as possible.

One of the challenges while assessing the nature of risks is to determine what to evaluate, because database applications typically contain several entry points from networks, operating systems, databases, and the application itself. Malicious intruders can exploit the weaknesses in any of those entry points. In addition, the intruders can target employees and contractors that are responsible for using, managing, testing, and maintaining the system. Organizations also need to consider how their systems are deployed including it being on the cloud, use of legacy applications where they may not have their source code, and dependency on third party test and development teams whether within the EU or outside.

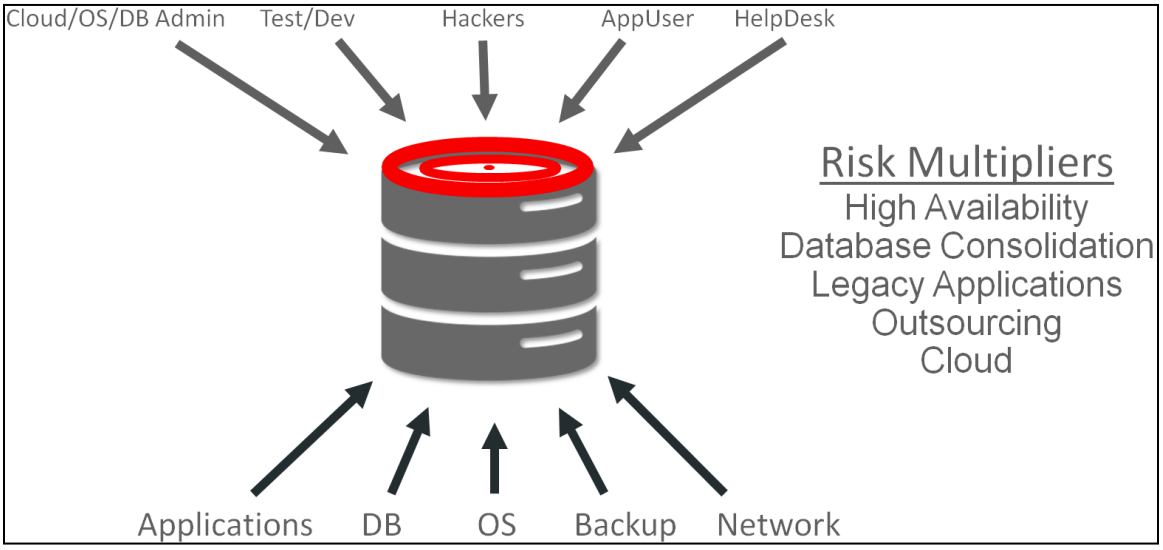

Figure 3: Attack Vectors and Targets for Databases

Oracle has been the undisputed leader in data security for decades and has been developing innovative data security products for several years to help organizations address attacks from different threat vectors. Oracle was the first one to introduce controls such as Row-level security, Fine-grained Auditing, Transparent Data Encryption, restricting privileged user access to sensitive information, Privilege Analysis, and Database Firewall.

Oracle Database Security technologies and products can help organizations accelerate GDPR compliance by addressing the challenges through its automated, transparent, and performant suite of technology and products. This section explains how Oracle Database Security controls can help to synthesize GDPR's requirements for security assessment, prevention, and detection.

ASSESS	PREVENT	DETECT
Processes, Profiles, Data Sensitivity, Risks	Encryption, Pseudonymisation, Anonymisation, Fined Grained Access Control, Privileged Access Control, Separation of Duties	Auditing, Activity Monitoring, Alerting, Reporting

Figure 4: GDPR Assessment, Preventive, and Detective Principles

Assess Security Risks

Article 35 of the GDPR mandates a data protection impact assessment for certain types of data processing. One of the challenges while assessing the nature of risks is to determine what to evaluate, because database applications typically contain several entry points, and have Personal Data spread across multiple columns and tables with loosely defined access control.

Oracle Database Security technology and products help address this challenge by providing tools to evaluate multiple aspects of application's data:

- Discovery of tables and columns containing "Personal Data"
- Configuration of the databases to determine the overall security profile
- Analysis of database roles and privileges to determine how controllers, processors, third parties, data subjects, and recipients can access sensitive data

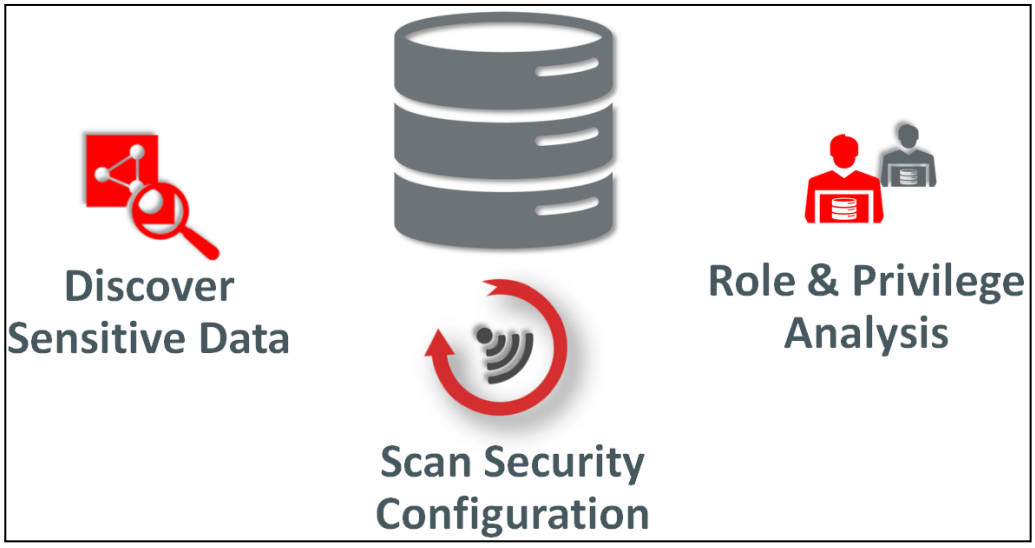

Figure 5: Assess Security Risks

» **Assess Sensitive Data Landscape using Oracle Application Data Modeling**

Finding Personal Data is a non-trivial task in today's complex applications as various identifying information could be embedded in multiple tables across multiple application schemas. Oracle Application Data Modeling automates the discovery of columns holding Personal Data and the corresponding parent-child relationships defined in the database. The discovery process uses built-in extensible patterns such as credit card numbers and national identifiers to sample data and identify the sensitive columns. Once the Personal Data is identified, it then becomes possible to apply the relevant controls whether preventive or detective. The resulting Application Data Model provides a complete set of sensitive columns along with their relationships ensuring that the application integrity is maintained by the data protection controls.

» **Assess Database Configuration using Oracle Database Lifecycle Management Pack**

All databases come with many tunable configuration parameters to suit wide-ranging security requirements. It is important to ensure that the configuration is still secure, has not drifted over time, and enforces the current set of best practices. Organizations need to scan databases for numerous security-related settings, including checks for default account passwords, account status, and account profiles. Oracle Enterprise Manager's Database Lifecycle Management Pack can be used to run more than 100 out-of-the-box policy checks against Oracle Databases, identify trends, and monitor drift from the golden configuration. Also, custom configuration checks can be defined to supplement checks provided by Oracle.

» **Assess Database Security Profile using Oracle Database Security Assessment Tool**

As per Article 36 of the GDPR, depending on the sensitivity of data, organizations may have to take the approval of a supervisory authority before processing sensitive information. The challenge is to quickly generate a presentable report of privacy and security assessment to submit to the supervisory authority. Oracle Database Security Assessment Tool analyzes not only the configuration but also how some of the security policies are implemented. It then presents its findings in a structured user readable format, which can then be presented to the Supervisory Authority. Organizations do not have to spend a lot of time and resources gathering and analyzing the findings of a data protection impact assessment on Oracle Databases.

» **Assess Least Privileged Access using Oracle Database Privilege Analysis**

Once the Personal Data has been identified, it becomes important to identify users (Data Subjects, Third Parties, Supervisory Authorities, and Recipients), including the privileged users and administrators (controllers, processors), who can not only access but also Process the Personal Data. During the application design and maintenance process, additional privileges may be granted inadvertently to the users. If such users are later compromised, significant damage can occur. Oracle Database Vault Privilege Analysis helps increase the security of applications by identifying the actual privileges used at run-time. Privileges identified as unused can be evaluated for potential revocation, helping reduce the attack surface and achieve a least privilege model.

Prevent Attacks

We discussed above the various preventive techniques recommended by the GDPR such as encryption, pseudonymization, anonymization, privileged user control, and others. One of the challenges with any preventive data protection technique is the possible overhead it creates on the applications and day-to-day IT operations. This overhead can come in terms of change of processes; changes required in the application source code, testing, performance overhead, and scalability concerns. Due to these challenges, some organizations may hesitate deploying preventive security measure for the existing applications.

While some of these concerns may have been valid a decade ago, Oracle Database Security addresses such challenges through preventive controls that are transparent to most applications and with very minimal impact on performance and ongoing IT operations. Oracle provides an easy-to-implement suite of preventive controls that

helps organizations implement the key preventive techniques mandated by GDPR including encryption, pseudonymization, anonymization, privileged user control, fine-grained access control, and data hiding.

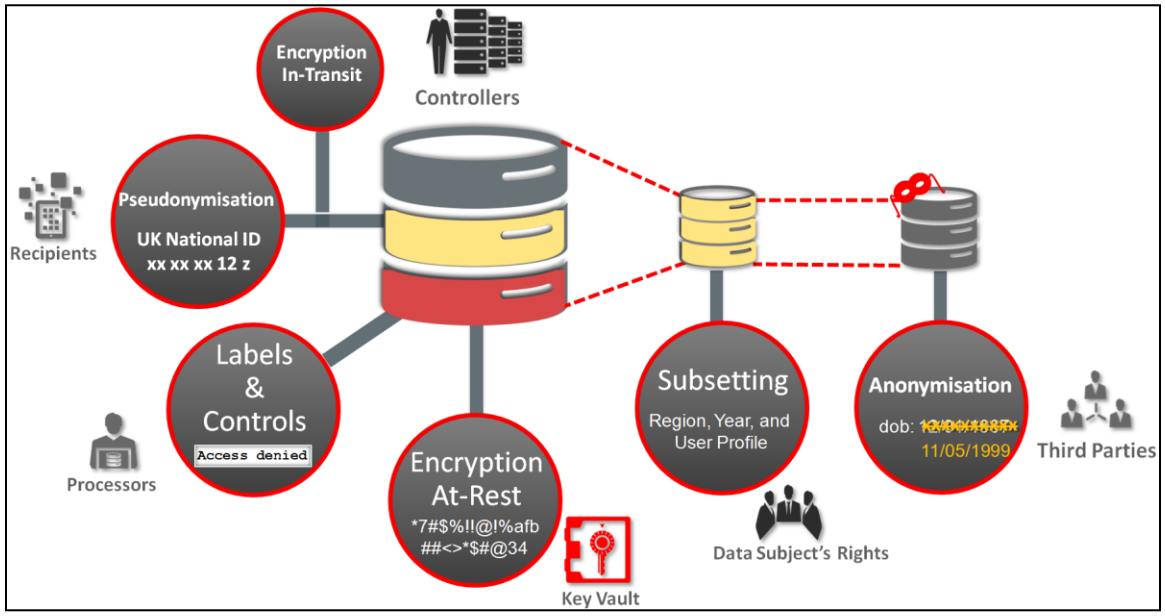

Figure 6: Oracle Database Security Preventive Controls

» Encrypt Data-at-rest Using Transparent Data Encryption

Article 32 of the GDPR strongly recommends encryption as one of the data protection techniques. One of the challenges to organizations while implementing data encryption is ensuring that not only is the Personal Data in tables encrypted, but also in backups, data dumps, and log files. Locating and encrypting data from all these sources can be a resource-intensive task. Oracle Advanced Security - Transparent Data Encryption (TDE) addresses this challenge by encrypting all the data directly in the source (database layer). TDE encrypts data automatically when written to storage including backups, data dumps, and logs. Encrypted data is correspondingly decrypted automatically when read from storage. This automatic encryption-decryption capability at the database layer makes the solution transparent to database applications. Access controls that are enforced at the database and application layers remain in effect. SQL queries are never altered, and hence no application code or configuration changes are required. Oracle Database comes pre-installed with TDE and can be enabled easily.

Another concern when encrypting data is the performance impact on database and application operations. The encryption and decryption process is extremely fast because TDE leverages Oracle Database caching optimizations, and utilizes CPU-based hardware acceleration available in Intel AES-NI and Oracle SPARC.

» Centrally Manage Encryption Keys using Oracle Key Vault

GDPR recommends centralization as it helps controllers enforce same security controls everywhere and also be able to take immediate actions in case of a breach. Oracle Key Vault (OKV) provides centralized control over data encrypted with Transparent Data Encryption (TDE). TDE provides two-tier encryption key management with data encryption keys and master encryption keys. The master encryption keys can be centrally controlled and managed using Oracle Key Vault (OKV). OKV provides an ability to block access to the master key and render the encrypted data unintelligible in the event of a data breach or suspicious activity.

Oracle Key Vault is a software appliance that enables customers to deploy quickly encryption and other security solutions by centrally managing encryption keys, Oracle wallets, Java key stores, and credential files.

» Encrypt Data-in-Transit using Oracle Network Encryption

To meet the requirements of Article 32 of the GDPR for protecting Personal Data when transmitted, Oracle Network Encryption helps organizations and controllers encrypt data-in-transit and prevent data sniffing, data loss, replay, and person-in-the-middle attacks.

Oracle provides both native network encryption and Transport Layer Security (TLS) based network encryption for organizations with PKI infrastructure. Network Encryption is built-in to the Oracle Database and is installed by default. Oracle provides support for global encryption algorithms such as AES.

» Pseudonymize Data using Data Redaction

Article 32 of the GDPR recommends pseudonymization. For example, a 16 digit credit card number can be pseudonymized to a partially redacted value such as xxxx-xxxx-xxxx-1245. Pseudonymization helps address attacks by preventing accidental or intentional exposure to sensitive data in application screens. Such screens could be used by the Processors and Third Parties for supporting the application or for call center which may be outside the boundaries of the European Union. One of the challenges while implementing pseudonymization is how to intercept application queries to the database and transform the data without affecting the application or backend database.

Oracle Advanced Security - Data Redaction can help address this concern by providing selective, on-the-fly redaction or pseudonymization of Personal Data in SQL query results before returning to the applications so that unauthorized users cannot view the data. It enables consistent redaction of database columns across application modules accessing the same database information. Oracle Data Redaction minimizes changes to applications because it does not alter actual data in internal database buffers, caches, or storage, while preserving the original data type and formatting when transformed data is returned to the application. Oracle Data Redaction has no impact on database operational activities such as backup and restore, upgrade and patch, and high availability clusters as no persistent data is changed. Unlike historical approaches that require making changes to applications or intercepting access to the database through a proxy, Oracle Data Redaction policies are enforced directly in the database kernel, resulting in tighter security and better performance. Oracle Data Redaction also allows the Controller to specify the conditions under which real data should be returned to the authorized Recipients. Oracle Database comes pre-installed with Data Redaction and can be easily enabled.

» Anonymize and Minimize using Oracle Data Masking and Sub-setting

Anonymization can be used to de-identify the Data Subject's Personal Data and prevent exposing sensitive Personal Data in less protected environments such as test and development. For example, a 16 digit credit card number can be anonymized to a fake 16 digit credit card number such as 5678-0987-4512-1111. One of the challenges with anonymization is that if it is not done properly, the de-identified or scrambled data may not be usable for testers and developers. Moreover, it could break the data integrity of the applications and databases.

Oracle Data Masking and Subsetting addresses these challenges by providing a comprehensive and extensible library of anonymization and masking formats, functions/transformations, and application templates. Sensitive Personal Data such as credit card numbers, national identifiers, and other personally identifiable information (PII) can be easily masked with an out-of-the-box library of masking and anonymization formats.

Article 5 of the GDPR mandates Data Minimization to reduce the amount of Personal Data collected, processed, shared and retained. However, most global companies combine the data from multiple countries or regions in one table, thus making it difficult to apply different policies on different parts of the table. This becomes particularly challenging when organizations have to provide a copy of the data (including Personal Data) to Third Parties and Processors such as partners in a specific country outside the EU. If all the requirements of the GDPR cannot be met, it might be best to remove the EU specific data from the set while keeping the rest for specific business purposes. Oracle Data Masking and Sub-setting addresses this challenge through its easy-to-define goal or

condition based sub-setting such as sub-setting based upon the country identifiers. Data Sub-setting provides an automated ability to identify, delete or extract a subset of data from a large dataset. Data Sub-setting can automatically process the data relationships and dependencies during deletion or extraction, preserving the integrity of the data set.

Oracle Data Masking and Sub-setting extracts entire copies or subsets of application data from the database, anonymizes, and minimises Personal Data so that the data can be safely shared with the Processors and Third Parties such as test, development, and partners. The integrity of the database is preserved assuring the continuity of the applications.

Oracle Data Masking and Sub-setting is pre-installed in Oracle Enterprise Manager. It provides a unified web-based GUI to mask and subset databases on-premise and in the Oracle Cloud.

» Control Privileged Users and Enforce Separation of Duties using Oracle Database Vault

GDPR Article 32 recommends limiting a Processor's access as privileged accounts is one of the most commonly used pathways for gaining access to sensitive applications data in the database. While their broad and unrestricted access facilitates database maintenance, the same access also creates a point of attack for gaining access to large amounts of data.

Traditionally it has been difficult to restrict privileged users (e.g. DBAs) from accessing the Personal Data. Such restrictions might affect day-to-day operations, such as patching and maintenance. Oracle Database Vault embeds privileged user access control within the Oracle Database to limit access to Personal Data by privileged users, while allowing the DBAs to perform their regular operational activities such as patching, import, export, and backup without accessing the Personal Data. Oracle Database Vault is used to define the realm of Personal Data that needs to be protected not just from the privileged users, but also through the use of database commands. It controls the mechanisms and the factors that can be used by the controllers, processors, and third parties (authorized users) to access Personal Data.

» Selectively Hide Data using Oracle Virtual Private Database

The GDPR introduces temporary preventive techniques to handle intermittent issues such as temporarily making the selected Personal Data unavailable to users. But the challenge is to easily filter and hide a subset of values from a large set. For example, an organization may have a need to temporarily hide all the data for individuals that belong to France due to suspicious activity. Filtering and hiding only France national identifiers from a large column containing national identifiers of different countries typically requires a lot of programming effort.

Oracle Virtual Private Database (VPD) addresses this concern with its easy-to-declare row level security (RLS) policies. It computes a predicate or "where" clause that is automatically appended to incoming SQL statements, restricting access to rows and columns within the table. VPD is installed with Oracle Database by default, and can protect the database from unauthorized access not only for handling intermittent issues, but also for regular operations. This minimizes the attack surface in case there is a programming error that makes it possible for the users to not just see their own data, but the data for other users also.

» Control Access with Oracle Label Security

The GDPR recommends that organizations and controllers ensure that the Personal Data is accessed selectively by Processors and for a defined purpose. Oracle Label Security (OLS) helps organizations to classify Personal Data elements by assigning labels based on confidentiality (such as public, sensitive, or highly confidential) or regions (such as North America, Europe, or Asia Pacific). OLS provides easy-to-declare access controls based on data classification. For example, rows containing sensitive data elements such as credit card numbers can be classified

as European highly sensitive data and only select processors or users can be given access to this highly Personal Data.

With its easy-to-declare access controls, OLS simplifies the multi-level security (MLS) model, which typically is a mandatory requirement for many government and defense organizations. Oracle Database comes pre-installed with Oracle Label Security and can be enabled easily.

» Facilitate End-to-End Access Control with Oracle Real Application Security

Per recital 64 of the GDPR , the controller should verify the identity of a requesting data subject in the context of online services, before giving access to the personal data. In modern 3-tier applications, verifying the online context of a user's identity is a challenge because typically the applications and application servers connect to the database as a single database user making it hard to track the originating user.

Oracle Real Application Security (RAS) addresses this concern by providing a policy-based authorization model that recognizes application-level users, privileges, and roles within the database. With built-in support for securely propagating application users' sessions to the database, RAS allows security policies on data to be expressed directly in terms of the application users, their roles and security contexts. Oracle Database comes pre-installed with Real Application Security.

Whether it is encryption or pseudonymization or privileged access control, Oracle Database Security can minimize the effort to implement and maintain GDPR's mandated data protection principles with its extensive portfolio of preventive controls.

Monitor to Detect Breaches

Traditional perimeter firewalls play an important role in protecting data centers from unauthorized, external access, but attacks have grown increasingly sophisticated bypassing perimeter security, taking advantage of trusted middle tiers, and even masquerading as privileged insiders. Surveys of numerous security incidents have shown that timely examination of audit data could have helped detect unauthorized activity early and reduce the resulting financial impact. GDPR Articles 30 and 33 mandate that organizations must constantly monitor activities on Personal Data and timely notify authorities in case of a breach. In addition to mandating auditing and timely alerts, GDPR also requires that the organizations must keep the audit records under their control. A centralized control of audit records prevents attackers or malicious users to cover the tracks of their suspicious activity by deleting the local audit records.

Oracle Database Security provides a comprehensive auditing collection and reporting mechanism to meet the monitoring requirements of GDPR. Oracle Audit Vault and Database Firewall (AVDF) provides a next generation data-centric audit and protection platform that provides comprehensive and flexible monitoring through consolidation of audit data from Oracle and non-Oracle databases, operating systems, file systems, and application specific audit data. At the same time, Oracle Database Firewall can act as the first line of defense on the network, enforcing expected application behavior, helping prevent SQL injection, application bypass, and other malicious activity from reaching the database. Oracle Audit Vault and Database Firewall can consolidate audit data from multiple databases and monitor SQL traffic looking for, alerting on, and preventing unauthorized or out-of-policy SQL statements. Data Protection Officers and Controllers can specify the conditions under which alerts can be raised in real time, attempting to catch the intruders with the abnormal activities. Dozens of out of the box reports combined with a custom reporting interface provide a comprehensive view of database activity across the enterprise whether observed through the network or through the audit logs. Oracle AVDF supports Oracle, Microsoft SQL Server, IBM DB2 for LUW, SAP Sybase ASE, and Oracle MySQL databases.

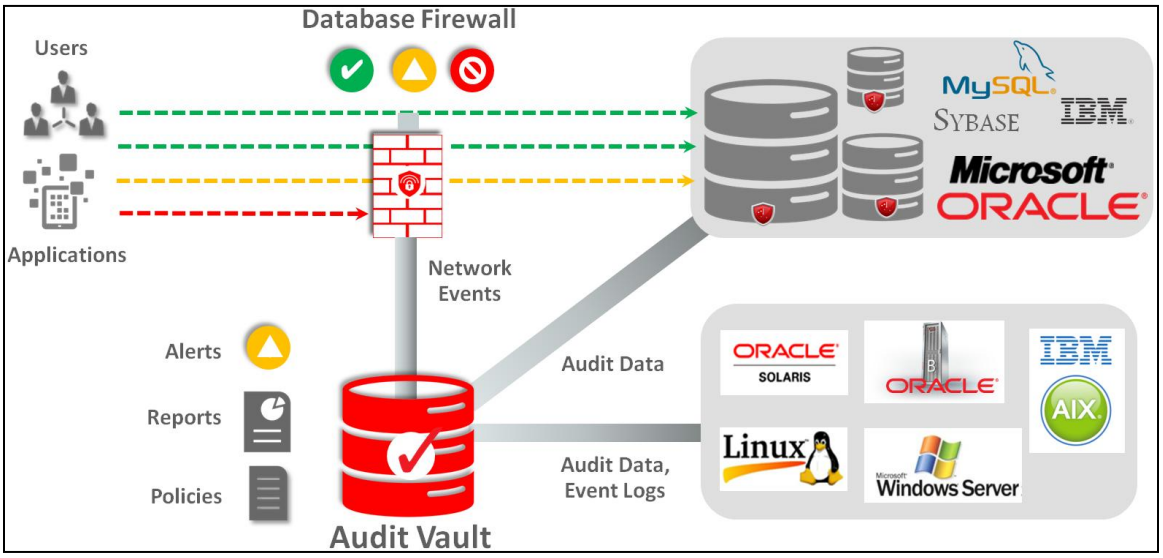

Figure 7: Oracle Database Security Monitoring Controls

Maximum Protection with Transparency, Accuracy, Performance, and Scale

GDPR Article 25 introduces the concept of data protection by design and by default. Modern applications contain multiple underlying components such as web gateways, web proxies, web servers, application servers, and database servers. Defining and implementing all the security controls in a multi-layered environment is a challenging task. Assembling all these different security controls and technologies from different vendors is an integration and administration challenge for organizations.

Oracle Database Security addresses this challenge by pushing controls closer to the data and enforcing security within the databases. Most of the data protection controls offered by Oracle are built into the Oracle Database. Securing data at the source not only simplifies the design and deployment but also improves the accuracy of protection, and minimizes the attack surface.

Oracle Key Vault and Oracle Audit Vault and Database Firewall complement the data protection at the source by centralizing the control and administration. Whether it is thousands of encryption keys, millions of audit records, or different types of security policies, these components can be managed centrally, greatly simplifying the administration related tasks. Oracle Enterprise Manager (EM) provides a unified web-based GUI for managing Oracle Database Security components.

Most importantly, all Oracle Database Security controls are well integrated to protect Personal Data inside-out. The following picture represents Oracle's Maximum Data Security Architecture showing how different Oracle Database Security products integrate with each other to secure Personal Data.

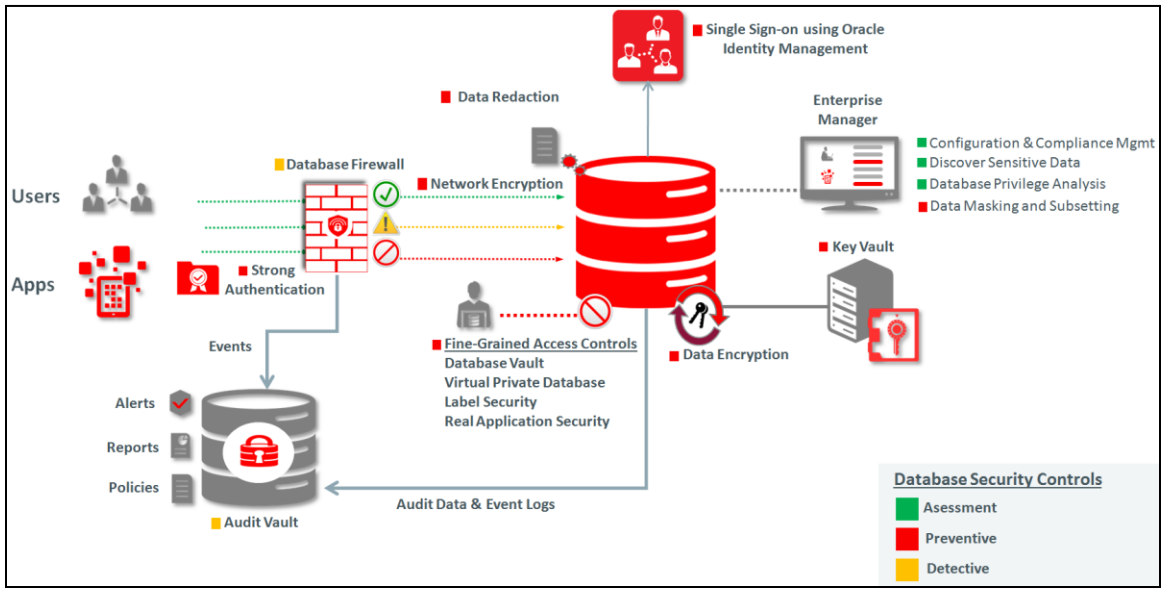

Figure 8: Oracle Maximum Data Security Architecture

Hypothetical Example

Having described GDPR's objectives, actors, and key data protection principles, here is how the hypothetical Belgium manufacturing company XYZ, introduced earlier in this paper, might leverage Oracle Database Security controls to help XYZ meet the GDPR's key data protection principles.

» Assess

As the first step, XYZ's Chief Security Officer (CSO) guides the application (APP) and database (DB) groups to assess the current state of data security as summarized below:

- Assess the security profile of the databases by scanning the configuration using Oracle Database Lifecycle Management Pack or Database Security Assessment Tool.
- Discover sensitive database columns holding sensitive data of the Data Subjects using Oracle Application Data Modeling.
- Assess how sensitive data is being accessed by scanning user privileges and roles using Oracle Privilege Analysis.
- Generate a detailed assessment report to present the findings to the Auditors and Supervising Authority.

» Prevent

Based on the assessment findings, the CSO guides the DB and APP teams to implement preventive techniques to help insulate the applications from outsider and insider attacks as summarized below:

- Encrypt the database holding EU individual's personal data using Oracle Advanced Security - Transparent Data Encryption.
- Manage the encryption keys centrally in Oracle Key Vault.
- Pseudonymize sensitive information in the customer care & billing application using Oracle Advanced Security - Data Redaction.
- Encrypt network traffic of the database using Oracle Database Network Encryption.

- Anonymize Personal Data before processing for development and testing using Oracle Data Masking and Sub-setting.
- Implement privileged user access control and separation of duties using Oracle Database Vault.
- Implement fine-grained access controls on APP using Oracle Virtual Private Database, Oracle Label Security, and Oracle Real Application Security.

» **Detect**

Finally, the CSO guides the DB and APP teams to implement detective techniques to monitor the applications and database for suspicious activity as summarized below:

- Audit activity on the Data Subject's information using Oracle Database Auditing.
- Centrally collect and manage the audit records using Oracle Audit Vault.
- Monitor, alert, report, and block suspicious behavior using Oracle Database Firewall.

Conclusion

Oracle has been the undisputed leader in data security for decades. Oracle has been developing innovative data security products for several years to help organizations address attacks from different threat vectors. Organizations worldwide can accelerate their response to the GDPR requirements by leveraging Oracle Database Security assessment, preventive, and detective controls with minimal overhead, high degree of transparency, and low deployment complexity.

It is critical to start planning now for how you will respond to the GDPR's requirements. By using Oracle Database Security products, organizations can start implementing the controls in the fastest way for not just to accelerate your response but also for achieving strong security for their sensitive Personal Data and business data.

References

The following websites provide further information on Oracle Database Security products and the EU GDPR.

» EU GDPR: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

» Oracle Technology Network for data sheets, whitepapers, FAQ, documentation, references, blogs, forums, and demonstrations for Oracle Database Security products:
http://www.oracle.com/technetwork/database/security/index.html

» Oracle Database Lifecycle Management Pack: http://www.oracle.com/technetwork/oem/lifecycle-mgmt/index.html

Appendix: Mapping of Oracle Database Security Products to GDPR

	Reference	GDPR Guideline	Oracle Database Recommendations
Assess	Article 35	Data protection impact assessment: The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks ...	» Use Oracle Enterprise Manager's Database Lifecycle Management Pack to assess the security profile of Oracle Databases by scanning the configuration. » Use Oracle Enterprise Manager's Application Data Modeling to assess the sensitive data landscape by scanning database columns for sensitive information. » Use Oracle Database Vault Privilege Analysis to assess how sensitive information is being accessed by scanning Oracle Database roles and privileges. » Use Oracle Database Security Assessment Tool for evaluating database security configuration, deployed security policies, state of users, roles, and privilege grants.
	Recital 90	... Where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk …	
	Recital 91	A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale …	
Prevent	Article 32	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: the pseudonymization and encryption of personal data …	» Use Oracle Advanced Security - Transparent Data Encryption to encrypt the data. » Use Oracle Advanced Security - Data Redaction to pseudonymize the data in production applications. » Use Oracle Data Masking and Subsetting to anonymize the data in non-production applications.
	Recital 83	In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks, such as encryption.	
	Article 6	4.) Where the processing for another purpose than the one for which the data have been collected is not based on the data subject's consent...the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the data are initially collected, take into account, inter alia: 4.e.) the existence of appropriate safeguards, which may include encryption or pseudonymization.	

	Recital 26	The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.	» Use Oracle Data Masking and Subsetting to mask or anonymize data in non-production environments.
	Article 20	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine readable format and have the right to transmit those data to another controller …	» Use Oracle Data Masking and Subsetting to subset the data by deleting the data or by extracting the data to a different location.
	Article 5	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');	
	Recital 64	The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers.	» Use strong authentication techniques such as SSL or Kerberos with Real Application Security (RAS) to verify the identity of the database and application users accessing sensitive information.
Detect	Article 30	Each controller and, if any, the controller's representative, shall maintain a record of processing activities under its responsibility.	» Use Oracle Database Auditing to enable and maintain records (audit records) of processing. » Use Oracle Fine Grained Auditing to record or audit specific activities of users such as SELECT on sensitive data » Use Oracle Audit Vault and Database Firewall to centrally store and manage the records of processing. » Use Oracle Audit Vault and Database Firewall to monitor and send timely alerts on suspicious behavior.
	Recital 82	In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility.	
	Article 33	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority ...	

Maximum Protection	Article 25	… The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	» Use Oracle Database Security maximum security architecture to protect the data inside-out by deploying assessment, preventive, and detective controls.

ORACLE

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/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Hardware and Software, Engineered to Work Together

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0616


Oracle is committed to developing practices and products that help protect the environment