MySQL Enterprise Edition
and EU General Data Protection Regulation (GDPR)
Table of Contents

Executive Summary ........................................................................................................................................3
Introduction to the General Data Protection Regulation (GDPR).................................................................3
Key Security Objectives of GDPR ...............................................................................................................4
Core Actors of the GDPR ..........................................................................................................................4
Key GDPR Data Security Requirements ......................................................................................................7
MySQL Enterprise Security and the GDPR ...............................................................................................11
Conclusion ..................................................................................................................................................19
References ..................................................................................................................................................19
Appendix: Mapping of MySQL Enterprise Edition Products to GDPR ....................................................20
Additional Resources ..................................................................................................................................24
Disclaimer: The purpose of this document is to help organisations understand how MySQL Enterprise Security technology can be utilized to help comply with certain EU General Data Protection Regulation requirements. Some of the MySQL Enterprise Security technologies may or may not be relevant based upon an organisation’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 organisations 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 organisations to consider how Oracle’s MySQL Enterprise Edition can help to accelerate adoption of the GDPR’s assessment, preventive, and detective controls.

This paper summarizes several key requirements of the GDPR and maps them to MySQL Enterprise Edition 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 MySQL Enterprise Edition 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

<table>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish data privacy as a fundamental right</td>
<td>The GDPR considers data protection as a fundamental human 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.</td>
</tr>
<tr>
<td>Clarify the responsibilities for EU data protection</td>
<td>To avoid fragmentation and ambiguity, GDPR has set a baseline for data protection by requiring anyone processing the personal data of an individual that is in the European Union to follow the requirements laid down in the GDPR.</td>
</tr>
<tr>
<td>Elaborate on the data protection principles</td>
<td>The GDPR considers encryption as only one of the components of a broad security strategy, and mandates that organisations need to consider assessment, preventive, and detective controls based upon the sensitivity of the personal data they have.</td>
</tr>
<tr>
<td>Increase enforcement powers</td>
<td>The EU aims to ensure compliance with the GDPR by enforcing huge fines of up to 4% of the global annual revenue upon non-compliance.</td>
</tr>
</tbody>
</table>

Core Actors of the GDPR

The GDPR defines various actors to explain the data protection concepts and their associated roles:
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 France. 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 individuals (“Data Subjects”). This EU-based company determines the purposes and the means of the processing of personal data (“Controller”). The development, testing, customer care & billing efforts are outsourced to external subcontractors in Brazil and India (“Processors”) where the employees often copy their customer's data (“Personal
Data”) to their local systems for development, testing, and processing, respectively. XYZ also partners with payment and delivery companies (“Third parties”) of different countries and provides them with individual’s data (“Personal Data”) for the processing of an order. An independent public authority monitors the application of the GDPR (“Supervisory Authority”).

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

![Figure 1: GDPR Actors with EU Enterprise and Controller](image)

GDPR can apply to 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 individuals who reside in the European Union.
- 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.
- A US-based hotel chain or an airline company that stores information of EU individuals travelling to the US.

The GDPR will also apply to businesses based outside of the EU that offer goods and services, or monitor the behavior of individuals that are in the Union. It does not exclusively apply to companies that are established in the EU.

In the following picture, the Controller is located outside of EU, but is still subject to the GDPR.
The key GDPR data security requirements can be broadly classified into three categories: Assessment, Prevention, and Monitoring/Detection. The GDPR also requires compliance with the data protection principles to enhance the quality and rigor of protection of the data. 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 organisation’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 refers to reducing the linkability of a data set with the original identity of a data subject. 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

On excluding personal data that is rendered anonymous from the scope:

... The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

-- Recital 26 of GDPR
Privileged User Access Control

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

… Processor and any person … who has access to personal data, shall not process those data except on instructions from the controller…

-- Article 29 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 Personal Data.

… 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

The 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 organisations minimize the risk of attack, they cannot eliminate the possibility that a data breach may occur. The GDPR recommends monitoring and alerting to detect such breaches through the following mechanisms:

Audit Data

The 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 organisations address threats from multiple angles and secure the data from unauthorized access.

Quality of Protection

For both large and small organisations, 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 stipulates the following to help ease the administrative overhead of the security controls and increase the quality of protection:

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 manner 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
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

Comprehensive Security

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

*In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

--- Article 32 of GDPR

MySQL Enterprise Security and the GDPR

Organisations typically have multiple layers of security surrounding the database through firewalls, intrusion detection systems, and proper networking segmentation, 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. Organisations 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.
MySQL Enterprise Edition has released many features over the years to help organisations address attacks from different threat vectors. Things such as Fine-grained Auditing, Transparent Data Encryption, user authentication, advanced encryption, and Database Firewall.

MySQL Enterprise Edition security features 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 MySQL Enterprise Security controls can help to synthesize GDPR’s requirements for security assessment, prevention, and detection.

<table>
<thead>
<tr>
<th>Assess</th>
<th>Prevent</th>
<th>Detect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes, Users, Data, Risks</td>
<td>Encryption, Access Controls, Separation of Duties, Pseudonymization, Anonymization</td>
<td>Auditing, Monitoring, Alerting, Reporting</td>
</tr>
</tbody>
</table>

**Assess Security Risks**

Article 35 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.

MySQL Enterprise has features that 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 personal data
Assess Sensitive Data Landscape using MySQL Workbench Tools

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. MySQL Workbench Data Modeling, Schema Inspector, and Table Inspector tools automate the discovery of columns holding Personal Data and the corresponding parent-child relationships defined in the database. Using MySQL Workbench tools, users can discover tables storing data 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.

Assess Least Privileged Access using by performing 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. The MySQL Workbench User Administration tool as well as MySQL Enterprise Monitor 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 to achieve a least privilege model.

Assess Database Configuration using MySQL Enterprise Monitor

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. Organisations need to scan databases for numerous security-related settings, including checks for default account passwords and account status. MySQL Enterprise Monitor can be used to run policy checks against MySQL Databases, identify trends, and monitor drift from the proper “golden” configuration.

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 control 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 organisations may hesitate deploying preventive security measure for the existing applications.

While some of these concerns may have been valid a decade ago, MySQL Enterprise Edition addresses such challenges through preventive controls that are transparent to most applications and with very minimal impact on performance and ongoing IT operations. MySQL provides an easy-to-implement suite of preventive controls that helps organisations implement the key preventive techniques mandated by GDPR including encryption, pseudonymization, anonymization, data hiding, fine grain access controls, and firewall rules.

![Figure 6: MySQL Enterprise Edition Security Controls](image)

**Encrypt Data-at-rest Using Transparent Data Encryption**

Article 32 and Recital 83 of the GDPR recommends encryption as one of the data protection techniques. One of the challenges to organisations while implementing data encryption is ensuring that not only is the Personal Data in tables encrypted, but also in backups. Locating and encrypting data from all these sources can be a resource-intensive task. MySQL Transparent Data Encryption (TDE) addresses this challenge by encrypting the data in innodb tablespaces, redo, and undo logs, as well as MySQL Enterprise Audit Logs directly in the source (database layer). TDE encrypts data automatically when written to storage including backups. 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. MySQL Enterprise Edition 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 as TDE leverages MySQL Database caching optimizations, and utilizes CPU-based hardware acceleration available on various chipsets.

**Centrally Manage Encryption Keys using Key Vaults**

Centralization helps controllers enforce same security controls everywhere and also be able to take immediate and quick actions in case of a breach. Key Managers such as Oracle Key Vault (OKV) or other Key Vaults supporting KMIP protocol provide 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 Key Vaults. Key Vaults provide the ability to suspend access to the master key and render the encrypted data unintelligible in the event of a data breach or suspicious activity. Smaller organisations with few servers may wish to also review use of the MySQL Encrypted Keyring file or other options for key protection.

Oracle’s OKV is a software appliance that enables users to quickly deploy encryption and other security solutions by centrally managing not only MySQL encryption keys, but much more - Oracle wallets, Java key stores, application keys, credential files, etc.

Encrypt Data-in-Transit

To meet the requirements of Article 32 of the GDPR for protecting Personal Data when transmitted, MySQL Enterprise Edition includes OpenSSL support for network data encryption and helps organisations and controllers encrypt data-in-transit and prevent data sniffing, data loss, replay, and man-in-the-middle attacks.

MySQL Enterprise provides OpenSSL Transport Layer Security (TLS) based network encryption and supports organisations with PKI infrastructure. Network Encryption is built-in to MySQL and can be installed on the fly.

Anonymize and Minimize using MySQL Enterprise Masking and De-identification

Anonymization can be used to de-identify the Data Subject’s Personal Data and prevent exposing 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.

MySQL Enterprise Masking and De-identification addresses these challenges by providing a library of anonymization and masking formats, functions and dictionary transformations, and data blacklisting. Personal Data and other sensitive information, such as credit card numbers, national identifiers, and other personally identifiable information (PII) can easily be masked with an out-of-the-box library of masking, randomization, dictionary, and blacklisting capabilities.

Recital 26 also states that the principles of data protection do not apply to anonymous information when the personal data is rendered anonymous in such a manner that the data subject is no longer identifiable. Masking data in non-production environments can help to keep Development, Test and other environments out of scope of the GDPR where personal data is not really required.

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 organisations must maintain a record of its processing activities.
This can only be achieved by constantly monitoring and auditing activities on Personal Data. This data can then be used to timely notify authorities in case of a breach. In addition to mandating auditing and timely alerts, GDPR also requires that the organisations must keep the audit records under their control. Centralized control of audit records prevents attackers or malicious users to cover the tracks of their suspicious activity by deleting the local audit records.

MySQL Enterprise Edition Audit provides a comprehensive auditing collection and reporting mechanism to meet the monitoring requirements of GDPR. MySQL Enterprise Audit is certified to work with Oracle Audit Vault and Database Firewall (AVDF) which provides a next generation data-centric audit and protection (DCAP) platform that provides comprehensive and flexible monitoring through consolidation of audit data from many databases including MySQL, Oracle database, and non-Oracle databases, operating systems, file systems, and application specific audit data. At the same time, MySQL Enterprise Firewall provides an instance based firewall to provide a last line of defense or the 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 Audit Vault supports Oracle, Microsoft SQL Server, IBM DB2 for LUW, SAP Sybase ASE, and Oracle MySQL.

![Oracle's Database Security Diagram](image)

**Figure 7: Oracle’s Database Security**

**Maximum Protection with Transparency, Accuracy, Performance, and Scale**

The 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 organisations.

MySQL database Security addresses this challenge by pushing controls closer to the data and enforcing security within the databases. Many of the data protection controls offered by MySQL are built into MySQL Enterprise Edition. 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) used in conjunction with the Oracle Enterprise Manager for MySQL provides a unified web-based GUI for managing Oracle Database Security components.

The following picture represents a MySQL Enterprise Edition Security Architecture showing how different security features integrate with each other to secure Personal Data.
Hypothetical Example

Having described GDPR's objectives, actors, and key data protection principles, here is how the hypothetical French manufacturing company XYZ, introduced earlier in this paper, might leverage MySQL Enterprise Edition 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 MySQL Workbench and MySQL Enterprise Monitor.
- **Discover sensitive database columns** holding sensitive data of the Data Subjects using MySQL Workbench
- **Assess how sensitive data is being accessed** by scanning user privileges and roles using MySQL Workbench.

Prevent

- **Encrypt the database** holding Data Subject’s Personal Data using MySQL Transparent Data Encryption.
- **Manage the encryption keys centrally** in Oracle Key Vault (or other KMIP 1.1 compliant Service)
- **Pseudonymize** sensitive information in the customer care & billing application using MySQL Masking and De-identification
- **Anonymize** Personal Data before processing for development and testing using MySQL Masking and De-identification
- **Encrypt network traffic** of the database using MySQL network encryption (configure TLS/SSL).
- **Implement privileged user access control** and separation of duties using MySQL Access and Authentication controls and roles.

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 MySQL Enterprise Audit.
- **Centrally collect and manage the audit records** using Oracle Audit Vault (or a similar audit archiving technology).
- **Monitor, alert, report, and block suspicious behavior** using MySQL Enterprise Firewall and/or Oracle Database Firewall.
Conclusion

MySQL has been developing innovative data security products for several years to help organisations address attacks from different threat vectors. Organisations worldwide can accelerate their response to the GDPR requirements by leveraging MySQL Enterprise Security for assessment, preventive, and detective controls with minimal overhead, high degree of transparency, and low deployment complexity. Additionally MySQL Enterprise Security may fulfill other security requirements related to other regulations or security risks not specifically addressed in the scope of GDPR.

It is critical to start planning now for how you will respond to the GDPR’s requirements. By using MySQL Enterprise Edition, organisations 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.

## Appendix: Mapping of MySQL Enterprise Edition Security Products to GDPR

<table>
<thead>
<tr>
<th>Reference</th>
<th>GDPR Guideline</th>
<th>MySQL Database Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assess</strong></td>
<td>Article 35</td>
<td>Data protection impact assessment: &quot;... 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.&quot;</td>
</tr>
<tr>
<td></td>
<td>Recital 84</td>
<td>&quot;... 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 that risk ...&quot;</td>
</tr>
<tr>
<td><strong>Prevent</strong></td>
<td>Article 6</td>
<td>&quot;... 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 pseudonymisation...&quot;</td>
</tr>
<tr>
<td></td>
<td>Article 32</td>
<td>&quot;... the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk,</td>
</tr>
</tbody>
</table>

- Use MySQL Workbench Data Modeling to assess the sensitive data landscape by scanning database columns for sensitive information.
- Use MySQL Workbench to assess how sensitive information is being accessed by scanning MySQL user privileges.
- Use MySQL Enterprise Monitor for evaluating database security configuration, deployed security policies, state of users, roles, and privilege grants.
- Use MySQL Enterprise Transparent Data Encryption to encrypt the data.
- Use MySQL functions, store procedures, views and other SQL expressions to perform data masking.
<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
</table>
| Recital 28 | "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 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."
| 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."
| 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');" |

- Use MySQL functions, store procedures, views and other SQL expressions to perform data masking to mask or anonymise data in non-production environments.
- Use MySQL functions, store procedures, views and other SQL expressions to perform data masking to subset the data by deleting the data or by extracting the data to a different location.
| Article 29 | “The processor and any person acting under the authority of the controller or of the processor who has access to personal data, shall not process those data except on instructions from the controller…” |
| Article 32 | “… 4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller…” |
| 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 MySQL grants and permissions in combination with MySQL functions, stored procedures, views and other SQL expressions to perform data masking for Fine Grained Access Control.

- Use strong authentication techniques such as SSL or MySQL Enterprise Authentication with Linux PAMs, LDAP or Active Directory to verify the identity of the database and application users accessing sensitive information.
<table>
<thead>
<tr>
<th>Detect</th>
<th>Article 30</th>
<th>“Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 30</td>
<td>• Use MySQL Enterprise Audit to enable and maintain records (audit records) of processing.</td>
<td></td>
</tr>
<tr>
<td>Article 33</td>
<td>“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...”</td>
<td></td>
</tr>
<tr>
<td>Article 33</td>
<td>• Use MySQL Enterprise Audit to record or audit specific activities of users such as SELECT on sensitive data</td>
<td></td>
</tr>
<tr>
<td>Article 33</td>
<td>• Use MySQL Enterprise Firewall along with Oracle Audit Vault or other secure Audit Storage methods to centrally store and manage the records of processing.</td>
<td></td>
</tr>
<tr>
<td>Article 33</td>
<td>• Use MySQL Enterprise Firewall, MySQL Enterprise Manager (this could include integration with Oracle Audit Vault and Database Firewall) to monitor and send timely alerts on suspicious behavior.</td>
<td></td>
</tr>
<tr>
<td>Article 34</td>
<td>“When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.”</td>
<td></td>
</tr>
</tbody>
</table>
### Maximum Protection

<table>
<thead>
<tr>
<th>Article 25</th>
<th>“… 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.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 32</td>
<td>“In assessing the appropriate level of security account shall be taken ... from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.”</td>
</tr>
<tr>
<td>•</td>
<td>Use MySQL Enterprise to maximum your security architecture to protect the data inside-out by deploying assessment, preventive, and detective controls.</td>
</tr>
</tbody>
</table>

## Additional Resources

**MySQL Enterprise Edition: Product Information**
http://www.mysql.com/products/enterprise

**MySQL Enterprise Edition: Documentation**
https://dev.mysql.com/doc/index-enterprise.html

**MySQL Enterprise Edition: Download (30 Day Trial)**
https://www.mysql.com/trials/

**MySQL Customers and Case Studies**
http://www.mysql.com/customers