Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

Oracle Engineered Systems and GDPR: Ten Capabilities To Consider for Protecting your Oracle Database Environments

How Oracle's Solutions Help Address GDPR Data Challenges

By Christophe Bertrand, ESG Senior Analyst

October 2018

This ESG White Paper was commissioned by Oracle and is distributed under license from ESG.

Contents

GDPR Overview

Regulatory compliance has affected organizations around the world for decades, yet now IT is at the center of the effort. Compliance is no joke, nor is it easy: indeed, ESG has determined that 65% of organizations that have been subject to audits by a regulatory agency have failed part of one at least once in the past five years due to issues with data access or retention.[1] Typically, compliance initiatives around the world either (a) have been rooted in the need to improve security and reduce operational risk—HIPAA and Sarbanes-Oxley (SOX) in the U.S are good examples—or (b) have focused on minimizing and managing data breaches; the UK's Good Practice Guide 13 (GPG13), for instance, is a data protection regulation for business processes that is mandatory for organizations managing high-impact data. In recent years, however, the focus on how data is used and how it affects individuals' privacy has come to the forefront of compliance requirements. Such regulations still relate to how enterprise data is managed; they include requirements covering data access, classification, retention, deletion, and rapid recovery; and many have the common thread that punitive consequences, such as fines, loss of accreditation, legal exposure for executives, etc., may result from failing to comply.

The European Union General Data Protection Regulation (GDPR[2]) exemplifies the shift of emphasis towards increasing personal privacy and limiting the use of personal data to the legitimate business needs for which it was collected. GDPR Article 25 stipulates "*data protection by design and default,*" meaning that all data protection principles, including data security, must be integral to any data processing, storage, and backup solution. Since modern enterprises run on data, the impact of GDPR on how IT organizations use and protect personal data can have a "domino effect" that will ultimately affect virtually all IT systems and processes. GDPR came into effect in May 2018, and has global impact, since any organization, irrespective of location, that has EU residents as targeted customers or processes data from them must comply. Other regions are beginning to adopt similar regulations. For example, Japan recently passed a GDPR match-up regulation called the Act on Protection of Personal Information. Additional examples include the Personal Data Protection Act in Singapore, which can impose $1M fines, OCC regulations for banks with greater than $50B in assets in the U.S., and the Financial Supervisory regulation in Korea.

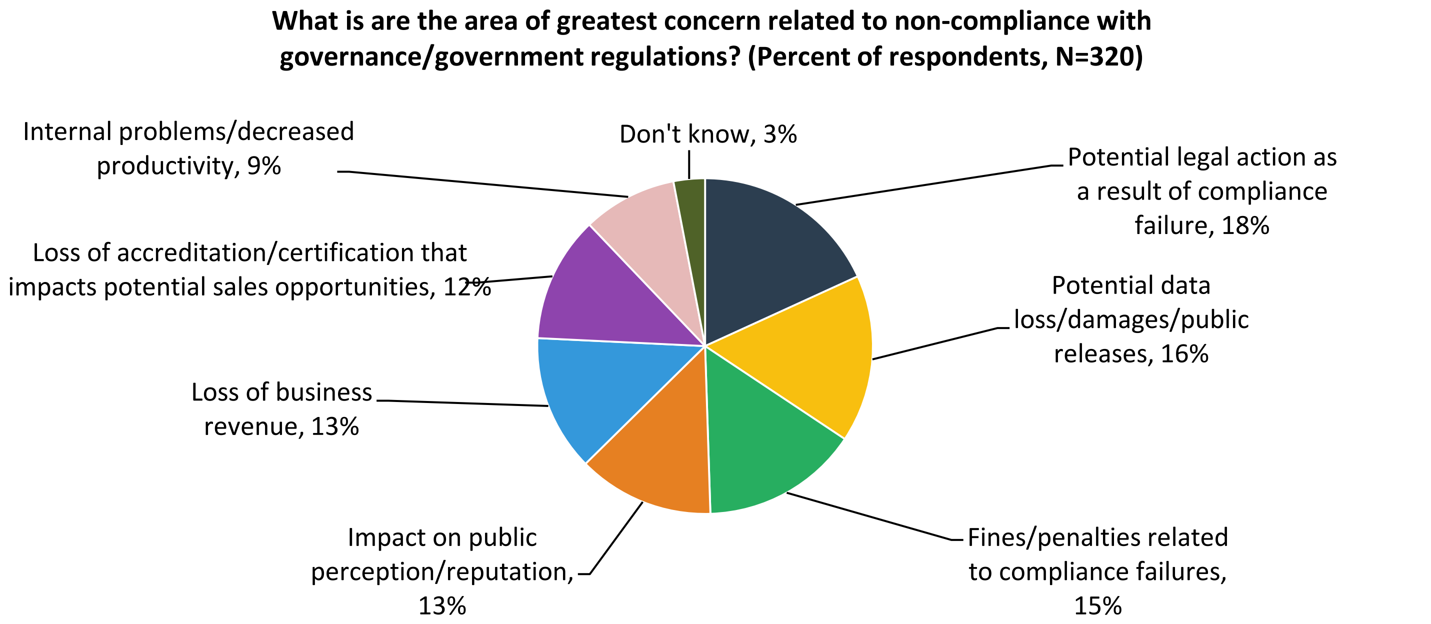
GDPR Is a Business Compliance Imperative

ESG's research finds that regulatory compliance impacts businesses' DP initiatives (see Figure 1):[3]

- Reflecting their concerns about—and drivers of—compliance, 18% of organizations surveyed by ESG cited the potential of legal action, and 16% cited the risk of data loss/damages/public releases as areas of greatest concern.
- Some highlight the risk of financial penalties (15%) and reputational impact (13%) as concerns.
- Other organizations more directly tied compliance to the risk of lost revenue (13%) and sales opportunities (12%).

[1] Source: ESG Master Survey Results, *2018 Data Protection Landscape*, to be published.
[2] See appendix for the main articles and requirements of GDPR for data protection.
[3] Source: ESG Master Survey Results, *2018 Data Protection Landscape*, to be published.

Figure 1. Compliance Generates Concerns



Source: Enterprise Strategy Group

The concerns from these organizations are not at all abstract, but are based on their recent compliance audit experiences. Forty-three percent of organizations report having been audited by a regulatory agency in the past five years, and 33% have been audited six to ten times.[4] Organizations identify GDPR as the second most impactful corporate governance regulation related to their data protection policies (right behind Sarbanes-Oxley) and 68% report that GDPR has already had either some or a significant impact on their data protection strategy. And all of this translates directly into IT investment (some of it desired, some of it merely of necessity!)—73% of surveyed organizations told ESG they'll need to make some or a significant incremental IT investment to meet GDPR requirements.[5]

Clearly, non-compliance isn't an option. It is too risky and too potentially costly. Authorities *will* audit. That said, GDPR can actually be used to an organization's advantage.

The Role of IT

GDPR requires a company-wide effort, with initiatives across the organization invariably converging on IT. That's because the digital data and IT systems tied to GDPR are inevitably at the heart of compliance. No single "silver bullet" will address 100% of GDPR data rules. Many areas must be considered—such as storage, access, security, integrity, management, backup, recovery, and reporting.

"Doing" GDPR is not a trivial exercise: the IT organization can and should expect significant adjustments to its data management, storage, and backup and recovery activities, norms, and processes. Complying with GDPR requires adequate resources and skills—an effort best effected when it's driven from the top of the organization.

However, GDPR also offers opportunities to improve IT processes and strengthen security, backup/recovery, and even customer relationships. And it is with the maximizing of the gains from GDPR, while minimizing its pain, that Oracle Engineered Systems can provide impressive, differentiated capabilities.

[4] ibid.
[5] Source: ESG Brief, *Perspectives on Readiness for and Impact of GDPR*, January 2018.

How Oracle Engineered Systems Help

A Comprehensive Portfolio

Oracle Engineered Systems are architected to work as a unified whole, so organizations can hit the ground running after deployment. Organizations choose how they want to consume the infrastructure: on-premises, in a public cloud, or in a public cloud located inside the customer's data center and behind their firewall using Oracle's "Cloud at Customer" offering. Oracle Exadata and Zero Data Loss Recovery Appliance (Recovery Appliance) offer an attractive alternative to do-it-yourself deployments. Together, they provide an architecture designed for scalability, simplified management, improved cost of ownership, reduced downtime, zero-data loss, and an increased ability to keep software updated with security and patching.

Oracle **Exadata** Database Machine offers many compelling optimizations to run Oracle Database—invariably it costs less, scales better, and is more secure than DIY infrastructures. Organizations enjoy extreme performance and efficiency using custom Oracle-only features, and its three consumption models mentioned earlier—on-premises as a private cloud, in Oracle Public Cloud, and as public cloud in customers' data centers and behind their firewall—form a solution that puts them on a path to use cloud on their terms.

While Exadata is focused on database *execution*, the Recovery Appliance delivers thorough *protection* for Oracle Database. It may eliminate nearly all exposure to data loss while also signifiicantly reducing the overhead for protection efforts on production servers. This scalable solution enables full data lifecycle protection through disk backup, tape backup, remote replication, and accelerated and automated database recovery.

When combined, Exadata and the Recovery Appliance are better than do-it-yourself deployments or generic data protection solutions, because they are:

- Faster together:
  - Oracle Exadata is the fastest way to run an Oracle database.
  - Recovery Appliance helps further accelerate databases running on Exadata by dramatically reducing backup windows and validation overhead from the Exadata database servers, freeing them for more production work.
- More secure together:
  - Oracle Exadata and Recovery Appliance combine to create an end-to-end solution that reduces surface area of attack and offers tight role-based security that may not be available with DIY solutions.
  - They allow for full data encryption from creation through data protection and deletion to reduce the threat of unauthorized access, end-to-end data verification to ensure that backups are—and remain—valid, and single-vendor solution-level patching that speeds resolution of any potential security issues.
- More agile together:
  - Oracle Exadata and Recovery Appliance enable enhanced levels of database execution and protection consolidation, making it easy to rapidly reallocate resources within the systems so enterprises can deploy new applications and scale existing ones in less time and with less effort.
  - Oracle Exadata makes it easy to move the cloud on a user's terms by supporting three cloud consumption models with complete compatibility—on-premises private cloud, Oracle Public Cloud, and Oracle Public Cloud in customer data centers and behind their firewalls.

- **More resilient together:**
  - Oracle Exadata and Recovery Appliance use a field-proven, high-availability architecture with no single point of failure, one that can be upgraded and expanded without service interruption.
  - They create a strong defense against technology failures, natural disasters and malicious attacks by securely protecting data with consistent backup and retention policies that cannot be locally overridden.
  - They help mitigate potential data loss assocated with ransomware, malware, and the activities of disgruntled employees by protecting it on separate systems that are not actively linked to the Exadata. They effectively create an "air gap" to a system with different access restrictions that may make it more difficult to compromise the enterprise's data.

- **Greater value together:**
  - The combined Oracle Exadata and Recovery Appliance can improve the business return derived from improved customer experiences and employee productivity, because they enable applications to run faster than on DIY solutions.
  - They require substantially fewer system and licenses resources, and are generally less costly to operate than DIY solutions because their unique architectures are co-engineered with Oracle Database to offload substantial parts of the workload from database servers.
  - They consume far less data center space and resources than DIY solutions due to the high level of consolidation they enable.
  - They also significantly mitigate the financial impacts and potential data loss associated with outages by making data more recoverable and hastening the recovery process.

Ten Ways Oracle Engineered Systems May Help Organizations Meet Specific GDPR Requirements

While a significant portion of GDPR compliance involves business processes and a broad participation across an organization, the data-centric nature of GDPR makes it imperative to look at mission-critical databases because many of them hold personal data. Oracle Engineered Systems provide many capabilities based on built-in security, redundancy, and self-healing to support compliance efforts that are both streamlined and optimized. Here are ten ways that Oracle Engineered Systems may help.

1. Data Discovery

One of the key challenges of GDPR is locating where sensitive personal data resides so that organizations can comply with many aspects of the regulations. In particular, Articles 15 and 17[6] give the "data subjects" a right of access to their personal data, as well as a right (under certain conditions) to be "forgotten" or have the personal data deleted. If organizations don't know where personal data is, how can they comply? This makes data discovery and classification essential to embark on GDPR compliance. If an organization uses Oracle Database and Exadata, it can leverage the Application Data Model (ADM) which stores a list of applications, tables, and relationships between table columns that are either declared in the data dictionary, imported from application metadata, or specified by a user.

2. Data Minimization

GDPR requires data minimization (Article 5), which means that organizations keep only the minimum amount of personal data required for valid business purposes, to retain minimum numbers of copies of it, and also keep it only for as long as necessary. Data minimization has consequences tied to how customer databases should be managed and groomed. The

[6] The pertinent GDPR articles referenced in this paper are summarized and explained further in the Appendix

databases should follow specific backup retention rules, which Oracle's Recovery Appliance is architected to deliver and may help them adhere to.

3. Data Deletion

GDPR dictates that personal data be forgotten or deleted from production environments when it no longer has a purpose, or when individuals, after meeting certain requirements, exercise their right to be forgotten or have data deleted from a database (Article 17). Deletion of data within a database can be easily achieved with Exadata and Oracle Database. However, maintaining point-in-time recoverability to the instant after that deletion can be more problematic. Some traditional approaches to data protection may open potential data loss windows of up to 24 hours, which means that deletions that occurred within that time frame may also be lost. The Recovery Appliance enables continuous protection of Oracle database transactions, including deletions, at the System Control Number (SCN) level, which means that it is specifically designed to recover databases to their last known good state—including any deletions that took place.

GDPR *also* states that data should be protected against accidental deletion (Articles 25 and 32); organizations must therefore have reliable backup and recovery—a perfect fit for the Recovery Appliance. Backing up data is one thing, but when it comes to GDPR, the ability to recover personal data in a short time period using the Virtual Full Backup capability of the Recovery Appliance may help organizations meet GDPR's stringent requirements.

4. Data Masking/Anonymization

Anonymization is one of the most difficult goals to achieve under GDPR. Data masking and subsetting let IT anonymize production data for testing and development use or to accelerate compliance. In Article 32, the pseudonymization and encryption of personal data are outlined as key safeguards and measures for data processors and data contollers. Oracle Database easily handles anonymization with Oracle Data Masking, which may enable organizations to keep augmenting and testing their Oracle environment without risking a compliance breach by exposing data to unauthorized users. However, risks of identification evolve over time as data sets change and new factors are added that can enable indirect identification of an individual's personal data. It is imperative that enterprises don't think they can simply press a button once and they will forever meet this requirement. Oracle software can help enterprises meet anonymization goals, but they must remain vigilant and continually reassess the risks that personal information can be directly or indirectly exposed.

5. Encryption/Security

GDPR addresses the need for encryption and security in multiple parts of the regulation. Of note are Articles 25 and 32. Oracle Engineered Systems support end-to-end encryption at the Oracle Database level on Exadata, including backup to—and recovery from—the Recovery Appliance. Encryption support also covers archives stored in the Oracle Cloud. Data can be created, backed up, moved, recovered, and deleted without ever being unencrypted. It is even possible for administrators to use Oracle Key Vault to manage encryption key lifecycles, passwords, and certificates to secure an Oracle Database transparently and redact sensitive application data located on Oracle Exadata, which may help organizations meet GDPR encryption and security requirements.

6. Access Control

Access control is vital to meeting most compliance requirements and is extremely visible in GDPR requirements. For example, with regard to access control, Article 25 states: *"In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*." With Oracle Engineered Systems, many access control capabilities are available to help IT secure database access. Oracle Database Vault controls access privileges using "least privilege" methodologies and "separation of duties" enforcement. For instance, Recovery Appliance retention policies supercede locally defined RMAN policies so individual DBAs can't retain data for longer than intended or delete it prematurely. IT can also use Label Security to imbue individual records with metadata describing their characteristics, and then enforce access controls based on that metadata. Additional Oracle capabilities—Identity Governance, Identity Cloud Service, Directory Services, and Access Management—may also be usable to enable and enhance GDPR compliance.

7. Monitoring/Reporting

With Exadata, Recovery Appliance, and Oracle Enterprise Manager, administrators gain an environment that provides a full view of the data protection lifecycle. Backups are visibly tracked in the catalog and a real-time recovery status dashboard provides alerts to make sure that recoverability meets required recovery point objectives. Audit Vault and Database Firewall provide centralized auditing, monitoring, reporting, and alerting of anomalous activity. Oracle's Security Monitoring and Analytics Cloud Service monitors incidents across heterogeneous and hybrid cloud environments. Multiple articles in GDPR cover the vast topic of reporting and demonstrability of actions, such as articles 30, 32, 33 and 34. Article 39—which establishes the role of the Data Protection Officer—highlights his/her responsibility as the monitor of compliance for the regulation amongst other advisory and auditing tasks. Unified monitoring and reporting of backup recoverability may help enterprises meet GDPR demonstrability requirements.

8. Continuous Protection

Database administrators can recover an Oracle Database to a specified point in time by leveraging an integrated Exadata, Recovery Appliance, and Enterprise Manager solution. Real-time Redo Transport from an Exadata to a Recovery Appliance provides continuous data protection with less than one second of potential data loss, allowing a database to be recovered to the very last transaction. In most organizations, and for myriad business and regulatory reasons, data loss is simply not an option; for this, the near-zero RPO provided by Recovery Appliance may help organizations meet GDPR requirements with its mandate of "Data Protection by Design and by Default" (Article 25).

9. Integrity Checking

Backups received by a Recovery Appliance (or replicated to other Recovery Appliances) are validated, compressed, and indexed during ingest, and then they are revalidated on a periodic basis as defined by the organziation. Backup validation is a requirement to guarantee recoverability and may assist organizations develop IT processes that comply with GDPR's Article 32 requirement to "*ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.*" It's stretching things to imagine any vendor other than Oracle could protect Oracle Database better.

10. Recoverability

Rapid recoverability is clearly called out in GDPR. Article 32 states that organizations must be able to "*restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*." The Recovery Appliance can help meet these requirements using its Virtual Full Backups, which eliminate the majority of the manual steps DBAs typically have to perform during a backup, thereby shortening recovery windows and reducing the number of people that have to access the data.

Summary Table

Table 1 summarizes the GDPR requirements that Oracle Engineered Systems—in conjunction with Oracle Database—support. This summary focuses on GDPR, but other data protection regulations have similar requirements.

Table 1. GDPR-related Capabilities/Solutions

GDPR Requirement	Oracle Engineered Systems	Key Capability/Functionality Provided by Oracle Database with Oracle Engineered Systems
Data Discovery	Exadata	Application Data Model
Data Minimization	Exadata and Recovery Appliance	Database Management Enterprise Manager Tool
Data Deletion	Exadata and Recovery Appliance	Database Management Enterprise Manager Tool
Data Masking/Anonymization	Exadata	Data Masking and Subsetting
Access Control	Exadata and Recovery Appliance	Database Vault Identity Cloud Service Identity Governance Access Management Directory Services Label Security
Security/Encryption	Exadata and Recovery Appliance	Advanced Security Key Vault End-to-end Encryption
Monitoring and Reporting	Exadata and Recovery Appliance	Full View of Data Lifecycle
Continuous Protection	Recovery Appliance	Redo Transport
Backup Integrity Checking	Exadata and Recovery Appliance	Integrity Checking Offload from Database Data Validation and Compression
Recoverability/Timely Restoration	Recovery Appliance	RMAN Redo Transport

The Bigger Truth

Data regulations are here to stay and will probably only become more complex. They are placing additional burdens on people, processes, and systems and are often thought to increase costs and risk. But in reality, simplifying and standardizing one’s approach to compliance is “business-future-proofing” that can boost organizational adaptability.

Oracle Engineered Systems complement Oracle Database, offering integrated capabilities to assist organizations in meeting their GDPR compliance requirements. These systems are designed to work as a whole, delivering efficiency and flexibility to production and data protection environments alike. *They place data at the heart of the compliance effort*.

Embracing GDPR can also be great for business. It forces a company to learn and understand what types of data it has stored, where it resides, who owns it, and how it is—or isn’t—being used. And, by providing a consistent framework and set of processes to protect data across an organization, GDPR helps IT organizations improve the resilience of their businesses and make it easier to meet other regulatory requirements.

That is, of course, as long as the right tools are available and have been properly integrated technically, functionally, and organizationally. Oracle Exadata, Recovery Appliance, and Oracle Database are designed and developed together to maximize performance, security and recoverability. They provide advanced capabilities that may be used by any organization attempting to comply with GDPR.

Appendix: Major Roles within the EU General Data Protection Regulation

Data Subject:

- A data subject is a natural person who can be identified, directly or indirectly via any means through the use of the data. They can be any individual located within the borders of the EU: a citizen, resident, or just someone passing through.
- Data subjects have specific rights regarding the collection, retention, processing, access to, and deletion of personally identifieable information (PII). These rights include but are not limited to the right to be informed about data collection and use, the right to be forgotten, the right to access and rectify personal information, the right to restrict and object to the processing, and the right to withdraw consent that was previously granted to use personal information.

Data Controller:

- A controller is any natural or legal person, public authority, agency or other body, which, along or jointly with others, determines the purposes and means of processing personal data.

Data Processor

- Any organization that processes data on behalf of a data controller. It might be, for instance, a cloud service or perhaps a marketing company that works with data.

Data Protection Officer:

- The employee or outsourced service officer tasked with reviewing GDPR compliance activities, ensuring employees are informed about all aspects of GDPR, and cooperating with supervisory authorities whenever requested or required.
- It is not an honorary title! This person or team must possess expertise in data protection law and practices.

Large organizations might already have put longstanding compliance officer functions into place.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.