# Helping Address Your GDPR Needs Using Oracle IT Infrastructure.

## Security: a legal and economic imperative.

The need to secure your company's data is nothing new. We all know that corporate data is at risk from loss, theft, and corruption, and that it's important to put processes and technologies in place to protect it. But the threats to your data are evolving, so data protection must evolve too.

New data protection legislation is being put in place to strengthen the existing data security process in addition to introducing new requirements. In May 2018, the EU General Data Protection Regulations (GDPR) will come into effect, and organisations based both inside and outside the EU subject to it will have no choice but to comply.

Oracle has a range of solutions that can help you implement a strategy to address the incoming EU GDPR, but no matter how effective your security solutions, if your infrastructure is open then you're still exposed and vulnerable. For that reason, this paper will focus on how Oracle IT infrastructure can be used to implement a robust security framework to help address these new regulations.

## What is EU GDPR?

The European Union (EU) introduced its data protection standard 20 years ago, via the Data Protection Directive 95/46/EC. Because EU Member States are allowed a certain degree of manoeuvrability when implementing such directives into national law, Europe ended up with a patchwork of different privacy laws. Additionally, two decades of increasing security breaches, rapid technological development, and globalization have brought new data protection challenges. The EU has developed the General Data Protection Regulation (GDPR) in an effort to address this situation.



ORACLE

## The objectives of EU GDPR.

The objectives and requirements of EU GDPR are comprehensive and far-reaching, but let's take a look at some of the most significant.

### To re-affirm that data protection is a fundamental right of the individual.

EU GDPR mandates that individuals have certain rights, such as the right to have their data 'rectified'—i.e., updated—and 'deleted' (the so-called "right to be forgotten") under certain circumstances, should they so wish. By the time it comes into effect, you'll need to have processes, technologies, and automation in place to effectively protect personal data.

### To clarify the responsibilities of EU data protection.

EU GDPR states that organizations should consider data security 'by design and by default'. This applies not just to EU businesses and organisations, but all those who host, handle, or access the data of EU data subjects.

### To define a baseline for data protection.

EU GDPR seeks to ensure a consistently high level of common information security across the European Union.

### To elaborate on the principles of data protection.

Under the tenets of EU GDPR, data protection can be broken down into three principal categories: evaluate, prevent, and detect. These three broad categories can help organisations like yours address threats from multiple angles, and secure data from unauthorised access.

### To increase enforcement powers.

EU GDPR has implemented new enforcement powers with which to punish organisations that fail to comply. These include fines of up to 20 million EUR, or four percent of a business' total worldwide annual turnover—whichever is greater.

## The consequences of noncompliance.

The potential penalties for noncompliance are significant. Not just in terms of a company's reputation—the consequences can be financial too. Companies could potentially face an individual administrative fine of up to 20 million EUR, or four percent of their total worldwide annual turnover—whichever is greater.

Failing to secure your data is a risk that no organisation should be willing to take.

### Noncompliance means:

A POTENTIAL FINE OF UP TO

€20

**MILLION** EUR

OR

4 PERCENT

OF YOUR WORLDWIDE ANNUAL TURNOVER

WHICHEVER IS GREATER



ORACLE

## How technology can help.

Data security is predominantly a people and process issue. Implementing security best practices—and ensuring that all employees are trained to follow them—will help to keep your data safe, but IT architecture still has a vital part to play in data protection. You need to build an information fortress with multiple layers of process and technology if you are to protect your data and remain compliant.

As individuals, we're only capable of delivering a single element of the data protection equation. Technology is another. Selecting and deploying the correct servers and operating systems to protect your data from attack will help you comply with some of the new GDPR requirements.

Security should be present throughout the IT stack—from servers and storage, to database and applications. This means embracing security:

- **At the software level,** using smaller, less sensitive sets of stored data protected by database security measures (unstructured data must also be protected). This implies data is protected at the application level, too.
- **At the hardware level,** because security implemented at the hardware level is inherited by all software. Remember: Oracle's cryptography benchmark measurements show Oracle SPARC provides greater encryption acceleration than any other general-purpose CPU, and protects data in memory with Silicon-Secured Memory.

## A closer look at EU GDPR.

Let's take a deeper dive into EU GDPR security, and what it might mean for your organisation. Different methodologies exist, but one methodology is to break down the regulation's key data security requirements into three simple principles: evaluation, prevention, and monitoring/detection. We'll now look at each of these in more detail.

### Evaluate.

EU GDPR mandates that controllers must perform data protection impact assessments when certain types of processing present a high risk. These must include an extensive, systematic evaluation of an organisation's security processes, its security profile, and the tools used to safeguard personal data.

Data protection impact assessments lay a foundation for the mitigation of data breaches, identifying gaps and evaluating any risks you need to address.

When completing your evaluation, consider both current risks and those you'll need to prepare for in future. And then there's compliance, incident response, and attack vector experience to consider, too.

**Your security reports must be:**

- relevant
- comprehensive
- flexible
- easy to understand.

Thorough data protection impact assessments are necessary to ensure continued compliance with all standards imposed on your organisation.

Auditors are not always familiar with businesses' operating systems, and may struggle to match security controls with security requirements. As such, tools that can do this on the auditors' behalf can reduce time wastage and minimise costs. The Oracle Solaris Compliance Tool can help with your compliance reporting. Simple report templates mean it's easy to use, and it also provides instructions on how to mitigate compliance test failures. Most Linux distributions employ OpenSCAP as such a mechanism.



ORACLE

For Solaris, Oracle has developed the Oracle Solaris Compliance Framework. The Compliance Framework allows you to set a security benchmark, and the tool will assess and report on the operation of your Oracle Solaris system for you. It delivers a standardised approach for maintaining the security of enterprise systems by:

- automatically verifying the presence of critical updates
- checking system security configuration settings
- ensuring the correct mechanism is used for checking security-relevant configurations
- complying with Security Content Automation Protocol (SCAP) standards.

For Linux, the OpenSource community developed the OpenSCAP ecosystem—based on the Security Content Automation Protocol (SCAP) maintained by the National Institute of Standards and Technology (NIST). This allows administrators to write their security content with a scripting language, and use the SCAP security guide package.

## Prevent.

There are numerous techniques that can help businesses like yours prevent an attack from succeeding.

### End-to-end encryption, near-zero performance impact.

The first of these is encryption. Put simply, encryption is the process of converting data into code in such a way that only authorised parties can access or understand it. EU GDPR considers encryption to be one of the core techniques organizations should look at to help prevent data from being viewed by those not authorised to access it.

It's important to remember that encryption won't prevent interference or data theft, however—it simply prevents cybercriminals from exploiting your data once they've taken it. Encryption helps render it useless to them.

Oracle provides data encryption at rest in the Oracle Database through Transparent Data Encryption, and in Oracle Solaris' ZFS file system—both of which can utilise Oracle SPARC hardware cryptographic acceleration, or EAS-NI (Advanced Encryption Standard New Instructions) available in x86 processors. The latter is an extension of the x86 instruction set architecture. The main difference between EAS-NI and SPARC encryption is that EAS-NI is an extension of the processor's instruction set, meant to accelerate cryptography. But the encryption operation must still be managed by the processor itself—unlike in SPARC, where this operation is processed by a separate crypto core.

The biggest challenge seems not to be encryption per se, but key storage and distribution. Encryption is only as secure and accessible as the keys themselves.

## Reduction of attack surface.

Your data is vulnerable to attack from a variety of directions. When we refer to the attack surface, we're talking about all the different attack vectors where a cybercriminal could extract data or gain entry. Every layer of the stack is at risk—from applications and middleware to virtualisation and operating environments.

Reducing the attack surface is a simple but effective strategy for enhancing data security—it's merely a case of minimising the amount of code you have running. Think about the functionality you really need. Use minimal installs—by avoiding installing unnecessary code, you'll avoid any potential security vulnerabilities, too.

We use this minimal install approach in our engineered systems, appliances, and cloud offerings.

### Oracle Solaris RBAC and SELinux.

With Oracle Solaris RBAC and SELinux, users are given specific access privileges based on their role. They're able to delegate within the parameters of their assigned permissions, and are subject to time-based controls—which limit access to specific days and times. RBAC may be further enhanced by requiring multi-factor authentication before the use of elevated privilege.

## Consolidation.

Consolidation is tied to the idea of reducing the attack surface. If you have a lot of separate databases running on separate infrastructure, then you'll have a large attack surface—and that means greater vulnerability. Consolidating your databases not only helps reducing this footprint in line with GDPR articles 25 and 32, it also reduces operating costs and makes the environment more physically resilient to attack.

Virtual machines are used in consolidation programs, although immutable zones are a more sophisticated approach. Virtual machines imitate dedicated hardware and allow users to run multiple operating systems side-by-side, managed by a hypervisor. Immutable zones, meanwhile, provide process centralisation—applications can still run, but those parts of the system that shouldn't be altered are locked down. The case for immutable zones is particularly convincing, because although reducing the attack surface will help to minimise data breaches, it won't mitigate the amount of damage an attacker can inflict if and when they discover a vulnerability.

## Standardisation.

Standardisation can also be grouped with reducing the attack surface area as a means of protecting your data. It's a forward-looking approach, which aims to create a secure, reliable foundation both now and in the future. Standardisation means using the same platform, the same management tools, and the same systems to support as many services as possible. The end result from a data security perspective is that administrators will be able to develop a deeper knowledge of their systems, and spend more time architecting and building a secure environment. This process can help administrators comply with Principle 7 of EU GDPR: Accountability—ensuring "data protection by design and by default".

## Access control.

Access controls are extremely important in mitigating the risks of attacks. In the majority of cases, users do not 'own' the data they work on—it's either hosted or owned by the company they work for—and access is usually based on employee functions. Role-based access control (RBAC) policies limit access based on the functions any given user is allowed to perform, and EU GDPR stipulates that data should only be accessible by those who absolutely require access to it. This is a particular challenge for those companies that still have root users. These 'superuser' accounts can make unrestricted, system-wide changes, making it practically impossible to comply with the GDPR stipulations. But by making root a role rather than a user, you can easily track and control who has these elevated privileges.

Whether you still have root users or not, RBAC policies and a fine-grained privilege separation structure—which helps ensure personal data is accessed selectively, and only for a defined purpose—are now essential.

## Updating systems.

Keeping your systems up-to-date is considered best practice to achieve a secure environment. EU GDPR mandates that you frequently update your operating system with the latest security patches, updates, and drivers, and that you regularly update software for box fixes, new device drivers, up-to-date system support, and general software performance. All of these updates help to ensure system speed, security, and reliability.

## Configuration drift.

Configuration drift is a problem for many organisations—particularly those where multiple administrators are tasked with the management of multiple servers. IT infrastructure goes through numerous changes over time, resulting in bloated, cluttered, unwieldy configurations. Servers can easily drift out of configuration, with inconsistent patching, ad-hoc changes to hardware and software, and incomplete or non-existent records of such changes. Configuration drift is a common cause of disaster recovery system failure.

There are ways of combating configuration drift, and bringing your evaluative processes in line with the requirements of EU GDPR. With Oracle Solaris Unified Archives, administrators can archive multiple system instances in a single unified file format. They can duplicate or 'clone' system configurations, and install them on other machines.

Then there are immutable zones. As we mentioned earlier, immutable zones are an effective means of preventing data manipulation. They expand the runtime boundary, and prevent accidental or deliberate configuration changes.

### Do it yourself, or let us do it?

Let's suppose you've decided to implement DISA STIG (Defense Information Systems Agency, Security Technical Implementation Guide) ahead of EU GDPR. We all know that implementing STIGs takes a lot of time and manual effort. Do you have the resources to do it yourself?

With Oracle MiniCluster, it's simple. MiniCluster features 250+ integrated security controls—including DISA STIG—which can be preselected ahead of installation. Our engineers have proven that Solaris 11 STIG requires 60 hours per zone to check, fix, and verify—across 24 zones, two kernel zones, and two global zones, that equates to 1,680 hours or 42 weeks of work. With MiniCluster, you can be ready and secure out-of-the-box in just six hours.

### Verified Boot.

Oracle Solaris has a further system to help prevent configuration drift: Verified Boot. When enabled, Verified Boot increases the security and robustness of Oracle Solaris by verifying kernel modules before execution. This defends against a variety of threats, including:

- corrupted and deliberately or accidentally modified kernel modules
- the insertion or substitution of malicious programs masquerading as legitimate kernel modules (such as Trojans, viruses, spyware, and root kits)
- the installation of unauthorized third-party kernel modules

## Cryptographically-secure installation and update.

Oracle Solaris provides a cryptographically-secure network installation and update mechanism. All initial software packages and updates are signed by Oracle release engineering, and Oracle Solaris can be configured to require a limited set of signed publishers for software installation and update. GDPR article 32 stipulates a level of security appropriate to the risk, and Oracle Solaris helps by defending against:

- replacement of potentially vulnerable older but valid programs, libraries, and configuration files
- installation of software from untrusted sources
- malicious or accidental tampering of software during download—for both initial install and update.

Oracle Solaris packaging metadata includes a list of fixed security vulnerabilities using the standard CVE numbering scheme, thus providing an easy mechanism to ensure that vendor-provided required security fixes are installed.

## Detect

While preventative security measures can help organisations like yours minimise the risk of attack, they can't eliminate the possibility of a successful data breach completely. As such, monitoring and alerting processes must be carried out to identify any breaches that weren't successfully prevented.

The reliable detection of potential security vulnerabilities is crucial for compliance with EU GDPR. While auditing can't prevent hackers from gaining unauthorised entry, it's become a fundamental element of system security and maintainability nonetheless. Auditing is the process of examining the history of any actions and events on a system, allowing us to determine what happened in the event of a data breach. Auditing can help to detect potential security breaches, misuse, and unauthorised activity, any attempt to bypass protection mechanisms, and extended use of privilege.

Successful auditing begins with two security processes: identification and authentication. Once a user has provided a user name and password at login, a unique audit session ID is generated. This ID is associated with that user's processes—even if that user changes identity during the session.

### Audit services.

With an audit service in place, you can:

- monitor any security-related events that take place on the host
- record the events in a network-wide audit trail
- detect misuse or unauthorised activity
- review access patterns and histories for both individuals and objects
- uncover any attempts to bypass the protection mechanisms
- discover extended use of privilege, suggesting a change of user identity.

Technology can play an important role in supporting and implementing your audit processes. Authentication is one such mechanism. Authentication identifies a user or service based on predefined criteria—from simple username/password pairs to more elaborate challenge/response systems. Strong authentication systems rely on users supplying information that is unique to them, or a verifiable item like a smart card or a fingerprint.

**Oracle Linux and Oracle Solaris have a variety of authentication features, including:**

- **Pluggable Authentication Module (PAM):** A framework enabling various authentication technologies to be plugged into a system entry service, without recompiling it. This provides multi-factor (or two-factor) authentication via one-time password (OTP) or local USB-accessible smartcards.
- **Simple Authentication and Security Layer (SASL):** A framework that provides authentication and security services to network protocols.
- **Secure Shell (SSH):** A secure remote login and transfer protocol that encrypts communications over an insecure network.
- **Kerberos service:** A client/server architecture that provides authentication with encryption.
- **Oracle Solaris BART:** A file integrity scanning and reporting tool to help administrators detect changes.
- **Oracle Solaris Compliance Tool:** Highlights the current state of the system and helps to reduce compliance reporting overheads. With Linux, we can use OpenSCAP.
- **Audit records:** Can be exported in real time through syslog or XML for use with an external network intrusion detection service.


Authentication with encryption is the basis of secure communication, helping to ensure that both the source and the destination are the intended parties. Encryption codes the communication at source, and decodes it again at destination, preventing intruders from making sense of any transmission they might intercept.

Operating environments should use fine-grained auditing, logging, and alerting, tracing actions back to an individual user—even across multiple uses, privileges, and role assumptions. This acts as a deterrent, as users who know that their activities are being audited are less likely to attempt any malicious activities.

## Conclusion

With EU GDPR coming into effect in May 2018, effective data protection is vital to ensure ongoing compliance. Organisations like yours can accelerate and enhance their response to EU GDPR security requirements by utilising Oracle's evaluative, preventative, and detective security controls.

The time to start planning and implementing an effective data protection strategy is now. Oracle infrastructure can help your organisation implement the controls you need, and assist you on your path towards GDPR compliance.

Oracle is committed to helping customers implement a strategy for GDPR compliance. To learn more about how we can help, contact your local sales representative or visit our GDPR Resource Centre.

**Further reading**

- Read the complete terms of EU GDPR.
- Find out more about Oracle Solaris.



ORACLE