Accelerate Your Response to the EU General Data Protection Regulation (GDPR) with Oracle Cloud Applications

ORACLE WHITE PAPER

Disclaimer

The purpose of this document is to help organizations understand how Oracle Cloud Applications can be utilized to help them comply with certain EU General Data Protection Regulation requirements. Some of the Oracle Cloud Applications features described herein may or may not be available based upon an organization's specific environment and Oracle Cloud Applications services acquired.

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 Oracle's products or services.

Table of Contents

Introduction

As organizations prepare for the new European Union (EU) General Data Protection Regulation (GDPR), Oracle Cloud Applications customers are challenged with implementing changes in the way they manage processes, people, and technical controls in order to comply with the new legislation. Oracle is committed to helping our Cloud Applications customers address GDPR requirements that may apply to their use of Oracle products and services.

To learn how Oracle Cloud Applications can help you accelerate your response to GDPR, this paper will look at some of the GDPR requirements that may be particularly relevant to Cloud Applications customers, and will discuss some of the privacy and security features available for Oracle Cloud Applications that can help you address these requirements.

What is GDPR and why it matters

The European Union (EU) introduced its data protection standard over 20 years ago through the Data Protection Directive 95/46/EC. Because the EU requires each EU Member State to implement Directives into national law, Europe ended up with a patchwork of different national privacy laws. And over time, the increasing number security incidents, rapid technological developments and globalization brought new challenges to the protection of personal data. In an effort to address this situation, the EU developed the General Data Protection Regulation (GDPR), which is directly applicable as law across all member states.

Once effective in May 2018, the GDPR will apply broadly to any company, whether based both inside or outside the EU, that collects and handles personal data from EU-based individuals. Personal data, also known as personal information or personally identifiable information in other parts of the world, is defined by the GDPR as any information relating to an individual that can be directly or indirectly identified, for example by reference to identifiers such as names, identification numbers, location data, online identifiers (including pseudonymous identifiers) or to one or more factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. With new and strengthened rights for individuals, accountability requirements for companies, and increased scrutiny by regulators, companies collecting and handling personal data in the EU, both offline and online (for example, involving e-commerce or online advertising activities), will need to consider and manage their data handling practices and use cases more carefully than ever before.

How the GDPR is expected to impact Cloud Applications

GDPR mandates many different personal data protection principles and requirements that apply to organizations that handle personal data of EU citizens. In this white paper, we will take a closer look at some of the requirements that may be of particular relevance to organizations that rely on Cloud computing applications. For ease of reference, we have broken these down into two key themes to consider: Managing Personal Data in the Cloud and Protecting Personal Data in the Cloud.

Managing Personal Data

In addition to considering applicable notice, consent and other requirements under GDPR related to your data collection and processing activities in the Cloud, GDPR places a great deal of importance on data subjects rights. For example, GDPR consolidates and strengthens existing rights for individuals such as the ability to have their personal data rectified and erased upon request, or the right to receive a copy of their personal data. It also introduces new rights for individuals such as the much-debated "right to data portability".

Organizations are therefore expected to carefully review their current practices with regard to the management of their data records in the Cloud, whether those relate to their employees, their end-customers, their suppliers or their website users.

Rectifying and Erasing Personal Data

GDPR gives individuals the right to rectify personal data that is inaccurate or to have incomplete personal data completed.

> *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed… - Article 16 of GDPR*

In addition to the ability to rectify or update personal data, Article 17 gives data subjects the right to erase personal data on request in specific situations. This right is also commonly referred to as "the right to be forgotten".

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay ...- Article 17 of GDPR

Data Portability

Article 20 GDPR provides individuals with the right to receive personal data on request as well as to have it transmitted directly to another controller under specific circumstances and where technically feasible.

Below, we will describe in greater detail some of the features offered by Oracle Cloud Applications designed to help you respond to data portability and right to be forgotten requests. However, as there are many considerations surrounding both the right to be forgotten and the right to data portability (such as data deletion standards and the use of commonly used file formats or transmission protocols), you should consult legal counsel to determine the implications Articles 17 and 20 might have on your organization.

Protecting Personal Data

Under GDPR, implementing good IT and information security are more important than ever when handling personal data. Organizations that collect and process personal data in the Cloud share a duty to protect and secure that data by implementing appropriate technical and organizational measures.

Security of Processing

Article 32 GDPR requires organizations that handle personal data to implement technical and organizational measures to ensure an appropriate level of security considering the costs of implementation, scope, purpose of processing, as well as the actual risk and likelihood of a potential breach.

> *… The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk...- Article 32 of GDPR*

GDPR is technology-neutral and does not mandate organizations to implement specific security controls, technologies or methodologies. However, Article 32 does provide guidance on certain security measures that organizations may consider implementing to help secure the data they are handling and, by extension, help mitigate the potential risk of a personal data breach. Examples of security controls and processes specified in Article 32 include:

» Pseudonymization and Encryption of Personal Data

» Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems.

» Control who may access the personal data.

» Restore the availability and access to personal data in the event of a physical or technical incident.

» Regular testing, assessments and evaluation of technical and organizational security measure

Ultimately, each organization is responsible for determining the most appropriate level of security required for its specific data processing operations, depending on the particular risks associated with the personal data being processed.

How Oracle Cloud Applications can help

As part of our commitment to help customers address their GDPR needs, Oracle Cloud Applications come packaged with a set of built-in privacy and security features that put Cloud Applications customers in control of the personal data they handle. We are also actively engaged in product reviews to further assess which additional features and functionalities can be embedded into our Cloud Applications or made available to Cloud Applications customers.

Managing Personal Data in our Cloud Applications

As today's businesses typically capture and handle vast amounts of personal data, whether for HR, CRM, Marketing or other organizational and business purposes, Cloud customers require powerful tools that enable them to manage data at scale. Oracle Cloud provides a comprehensive portfolio of features that can be leveraged to help Cloud Applications customers manage personal data.

Efficiently Managing Personal Data

Oracle Cloud Applications provide a range of capabilities designed to help enable Cloud Applications customers to update personal data records on an ad hoc basis, e.g., following a subject access and rectification request, or through automated means designed to enable customers to make any changes directly to their data as they see fit. Depending on your businesses requirements and your use of Oracle Cloud Applications offerings, you may choose to leverage a combination of intuitive wizards, preference centres and other native features to manage personal data at scale.

Exporting and Transmitting Personal Data

Oracle Cloud Applications have made significant investments over the years to develop open platforms that can help enable Cloud customers to export personal data at scale. Depending on the Cloud services you have ordered, you may have access to a comprehensive suite of extensibility features covering modern API's and robust SFTP mechanisms to help facilitate and secure scalable personal data transmissions. Oracle Cloud Applications also provide intuitive tools designed to make it easy for Cloud Applications customers to export personal data on request.

Storage and Transfer of Personal Data

Cloud Applications customers may choose the data center region in which their Cloud Applications services environment will be hosted[1]. Available Cloud Applications data center regions include European Union (EU), North America (NA), Latin America (LAD) and Asia Pacific (APAC). To provide Cloud Applications customers the best possible service, Oracle operates a 24/7 global delivery model for Cloud Applications, including for Cloud Applications support or for incident management and security purposes. Oracle offers customers multiple safeguards and security options designed to protect and secure customer data wherever it resides.

[1] Limited exceptions may apply for selected service offerings.

Securing Personal Data in Our Cloud Applications

Native to Oracle Cloud Applications, we provide state of the art data security mechanisms and controls derived from generally accepted ‘privacy by design and privacy by default’ principles.

Security Controls

Oracle Cloud Applications have made significant investments in a wide range of data security measures and optional features across our products and data centers. These may include features such as encryption, data masking and hashing, and many more designed to help secure personal data in the Cloud Applications. Oracle Cloud Applications have deployed Oracle’s standard Transparent Data Encryption (TDE) across key areas of our infrastructure designed to secure personal data, with encryption keys stored in password-protected containers in accordance with accepted industry security standards. Customers may also choose to hash identifiers in order to pseudonymize personal data, as well as to encrypt data in transit between a user’s browser and a web server leveraging TLS.

Security Standards and Certifications

Oracle’s corporate security policies are aligned with the ISO2700x family of standards, including in the following key areas of information security: organizational security; organizational security infrastructure; asset classification and control; personnel security; physical and environmental security; communications and operations management; access control; systems development and maintenance; business continuity management; and compliance.

Many of our Cloud Applications offerings currently also hold an ISO 27001 certification for the Global Nerve Centers, Data Centers and relevant compliance and security processes. Additionally, Oracle makes available SOC 1 and SOC 2 type II reports for many applications within its Cloud Applications portfolio. Those reports reflect an independent assessment of many processes and controls complementary to the ISO 27002 standard controls.

Granular Access Controls

To help enforce authorized access to personal data, Oracle Cloud Applications provide the ability for organizations to implement and configure granular access controls. This enables organizations to distinguish which individuals or groups should have access to personal data. Advanced User Management can be used to define specific user roles and groups which can be assigned to pre-defined permissions across Oracle Cloud Applications. SSO, Secured User Access, and IP Whitelisting mechanisms may also be used as an additional layer of protection to prevent unauthorized access to personal data based on your business and legal needs.

Conclusion

At Oracle, we are committed to helping our Cloud Applications customers address their GDPR needs and to provide easy-to-use tools and transparent controls that can be leveraged by customers towards this goal. As you are challenged with operating in an ever-changing regulatory landscape, you can count on Oracle to help you accelerate your response to the EU General Data Protection Regulation.

If you have further questions about this white paper or about Oracle's privacy & security policies or service options that can help address your GDPR needs, please consult your Oracle sales representative or Customer Success Manager.

For more information, please visit: GDPR oracle.com/applications/gdpr

References

The following websites provide further information about the EU GDPR:

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

» UK ICO: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

ACCELERATE YOUR RESPONSE TO THE EU GENERAL DATA REGULATION | ORACLE CLOUD APPLICATIONS