An Oracle White Paper
April 2010

Oracle E-Business Suite HCM
Data Privacy – Challenges and Solutions

Table of Contents

What is Data Privacy and Who Should Be Concerned?

Simply put – data privacy/data protection is the ability of an individual to exercise appropriate control over their personally identifiable information. In many countries, those of the European Union for example, privacy is considered a fundamental right and the individual is provided with rights related to information collection, storage and use, including sharing and transfer of information.

Compliance with these requirements can be complex with variations of specific elements across countries. Compliance requires that companies understand these laws and develop the correct policies and practices to comply. This paper is not a manual of how a company should comply with law; only the company, its advisors and legal counsel can do that. This paper is intended to highlight some of the issues inherent in compliance and address the role that technology can play in facilitating compliance. While much of the information in this whitepaper regards data privacy in general, it is written specifically for customers utilizing the Oracle Human Capital Management applications.

What Constitutes Personally Identifiable Information (PII?)

Personally Identifiable Information (PII) refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The abbreviation (PII) is widely accepted, but the phrase it abbreviates has four common variants based on personal, personally, identifiable, and identifying.

Among the most common items which might be considered PII are a person's

- Full name
- National identification number
- Telephone number
- Street address
- E-mail address
- IP address
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Family details (emergency contacts, beneficiaries)

While some of these such as full name or unique national identifier will always be considered PII, others may be more context-dependent. Data must be considered in context to determine privacy requirements. A meal preference, for example, is innocuous enough, but it has been found to warrant protection as sensitive data if it may be used to make religious inferences. Thus vegetarian may not be sensitive, but Kosher or Halal may be.

OECD Guidelines

In 1980, the OECD[1] developed the OECD Guidelines on the Protection of Data and transborder Data Flows (Guidelines); still considered by many to be the best international statement of privacy principles.

A few years after the OECD Guidelines were issued the EU developed a regional interpretation of the OECD Guidelines embodied in Directive 95 (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) commonly referred to as the EU Directive. Both the OECD Guideline and the EU Directive are predicated on the protection of personal data and treat data protection as a fundamental right. Both were also among the first documents to consider data protection in the context of international data flows. The early and mid eighties saw the growth of electronic data interchange, mostly batch processing of data by specialist data processing companies supporting business needs of growing national and multinational companies.

These dual objectives are set forth in the Directive with a primary objective to "protect the fundamental rights and freedoms of natural persons and, in particular, their right to protection with respect to the processing of personal data." And a second objective to ensure the free flow of personal data – within specified guidelines. All of the countries of the EU are required to develop a national implementation of the Directive. Unfortunately, there is a variability of requirements across these national implementations, which creates greater complexity of compliance. The Directive was always meant to be a floor, not a ceiling, and specific wording is not required in the implementations. Thus variability may exist both in the strength and the phrasing of the national requirements..

Another significant variable, which occurs across national implementations, are requirements related to registration or notification of processing. In some cases these can be complex requiring significant detail for each processing activity, in others they are a simpler summary checklists and in some jurisdictions they are obviated by the appointment of a corporate data protection officer.

Adherence to data protection requirements has become critical to the global enterprise that uses Human Resources data for operating business functions – from payroll and benefits to global staffing and management development – because non-compliance with the requirements can subject the enterprise to financial penalties or even to data embargoes.

[1] Organization for Economic Cooperation and Development – an intergovernmental organization of the industrialized nations

One of the main differences between the Directive and many other privacy or data protection laws, is the formalized system of findings of adequacy as a basis for transfer of information. Like many laws sourced from the OECD Guidelines, the EU directive requires that:

- PII is collected pursuant to a prominent, understandable and comprehensive notice
- the collection of information is limited to that which is needed or relevant to the purpose for which the information was collected
- the data subject (individual whose information is collected) provide unambiguous consent to the collection and use of the information
- the data subject is provided with access to the information collected for review or correction
- the integrity and security of the information is maintained
- the information is maintained only for a period of time appropriate to accomplish the purpose for which it was collected

Most laws and the OECD Guidelines consider the need to assure these protections are maintained if the information is transferred. The Directive has developed a high-level requirement that, absent an applicable derogation, information should only be transferred to other jurisdictions whose privacy laws have been found to be "adequate" by the European Commission. While other countries have adequacy requirements, the EU Directive formalizes this requirement to include formal government recognition. To date only a handful of jurisdictions have received such adequacy findings.

The US is the most unique of these adequate jurisdictions as the finding was not predicated on an omnibus national law or separate privacy authority, as neither exists in counterpart to EU institutions, but rather on the basis of the Safe Harbor Agreement. The Safe Harbor is a letter agreement between the US Department of Commerce[2] and the European Commission which sets out a number of principles which must be adhered to as well as the option of using private sector oversight agencies (Trustmarks – TRUSTe, BBB-Online or the AICPA) or being subject to a panel of data protection authorities. The Safe Harbor requires member companies to post privacy policies that embody the safe harbor principle. Those polices are enforceable in the first instance by the Trustmark, but also by the Federal Trade Commission under their Section 5 powers related to fraud and deception.

[2] The US Department of Transportations was also party of the agreement

In order to understand how to approach compliance obligations, companies must have some basic understanding of the types of the data they collect and, how those data are used, managed, stored and retired. This understanding should show both a general data flow and data lifecycle mapping of PII within your company. This will simplify many of the subsequent questions which will need to be answered. There are many steps and requirements to achieve compliance so each organization should research this area thoroughly. Below is a list of most commonly asked questions.

- Who has control and responsibility over personal data?
- Who has authority to access the data?
- Who can make changes to the data?
- How will the collected data be used?
- What are the applicable legal and regulatory requirements?
- What information technology systems are in place and how can they be best used to handle the requirements

Because the process of meeting legislative requirements can take a long time, we recommend that your organization begin complying with data protection requirements as soon as possible. Ongoing communication with your "in-country" legal staff is critical. Your legal team will be sensitive to the local cultures' views about the protection of data and can deal with the local agencies as needed. As a software provider and implementer, Oracle cannot provide any legal advice regarding data privacy compliance.

In order to address the notice requirements, many organizations draft a privacy policy setting forth the company practices related to the collection, use and management of information. In light of some of the contextual differences between workplace and business-to-customer interactions, some companies develop separate employee and customer privacy policies, but both are rooted in the requirements of the EU Directive. These policies typically state the rights of the employees, as the organization is responsible for informing its employees about their rights. Some points that are typically included are:

- Employees have the right to access information being transferred and to verify its accuracy
- Employees can rectify incorrect data and file a complaint
- Employees have the right to know when, how, and what data is being processed and to whom it is being sent
- Need for explicit employee consent before sensitive data—such as racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union memberships, and data concerning health—can be processed.

To comply with the Directive, organizations should review all collection, storage, and uses of personal information, in any format or vehicle—automated or manual—as well as all policies and practices relating to personal information.

In some countries, organizations also utilize contracts as part of their compliance solution. The Directive has provided a derogation that foresees the use of contractual clauses to meet the requirements of adequacy to transfer PII. Both the EU and the International Chamber of Commerce have issued model contract clauses that have been approved by the Commission to meet the requirements of adequacy as set forth in the Directive. http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm. Model contracts exist at present between Data Controllers as well as between Data Controllers and Data Processors. Wok is now being undertaken to consider how to contractually deal with Data Processor-to-Data Processor transactions. It is important to understand the distinction between data processor and data controller to better understand the legal obligations that are involved. Data Controllers are those persons or organizations that can exert control over information, where processors merely execute instructions over the information. Controllers have all obligations from notice to collection limitation to security to retention/deletion. Processors on the other hand often have no direct communication with data subjects and thus may have little role to play in notice and collection limitation for instance. This can, of course, change based on context.

Compliance Options – Country to Country

Transferring data within the EU requires legal basis for transfer, but all EU countries already meet data protection requirements, thus there is no need for an adequacy finding. It is when data is transferred from an "adequate" country to a country with no adequacy finding that special controls need to be put in place to find a way to address the adequacy requirement.

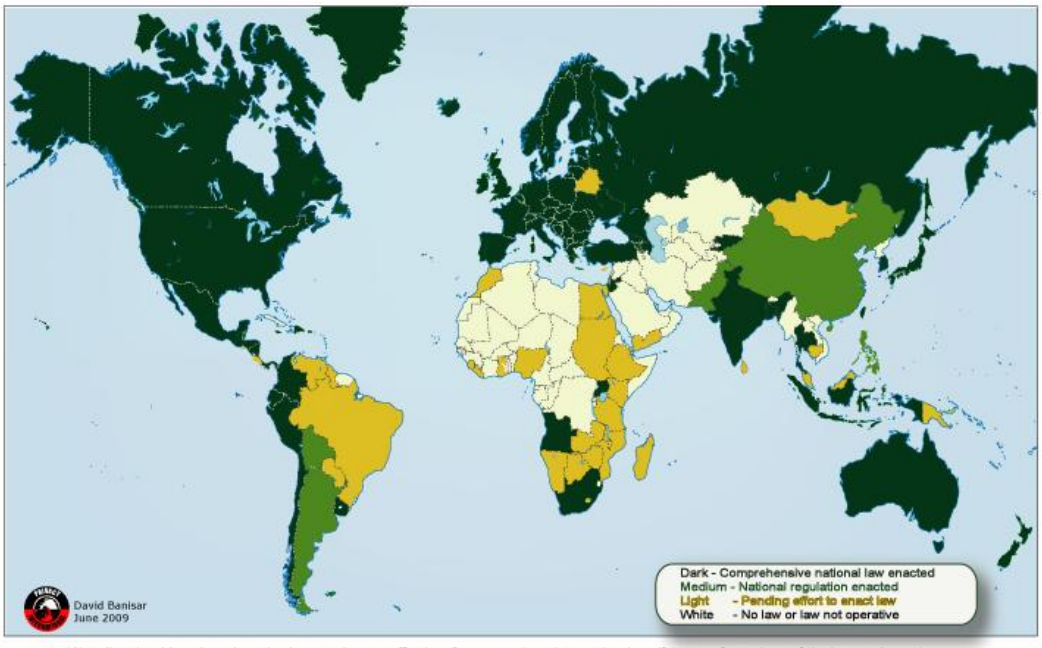
Where no adequacy finding exists between two jurisdictions there are only a few accepted methods to transfer information:

- With the explicit consent of the data subject
- Pursuant to a model contract
- In the case of the US via the Safe Harbor, or
- An emerging option is under Binding corporate rules

In addition to the stringent requirements surrounding data privacy in the EU, they also exist in many other parts of the world, including the Americas, the Asia Pacific region, and Africa. Organizations need to consider these continents and make themselves familiar with their requirements to guarantee free data flow on a global basis. A global organization may have to submit different information from one country to another because of differing requirements.

Many organizations may see the encryption of personal data before it is transferred to another country as a possible solution. Encryption is already regulated in some countries including: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Portugal, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States.

National Freedom of Information Laws, Regulations and Bills 2009



*Not all national laws have been implemented or are effective. See www.privacyinternational.org/foisurvey for reviews of the laws and practices

http://www.privacyinternational.org/

While every effort has been made to provide you with the most current information, it is constantly changing, so this document, in no way replaces the need for your legal counsel involvement.

Risks of Non-Compliance

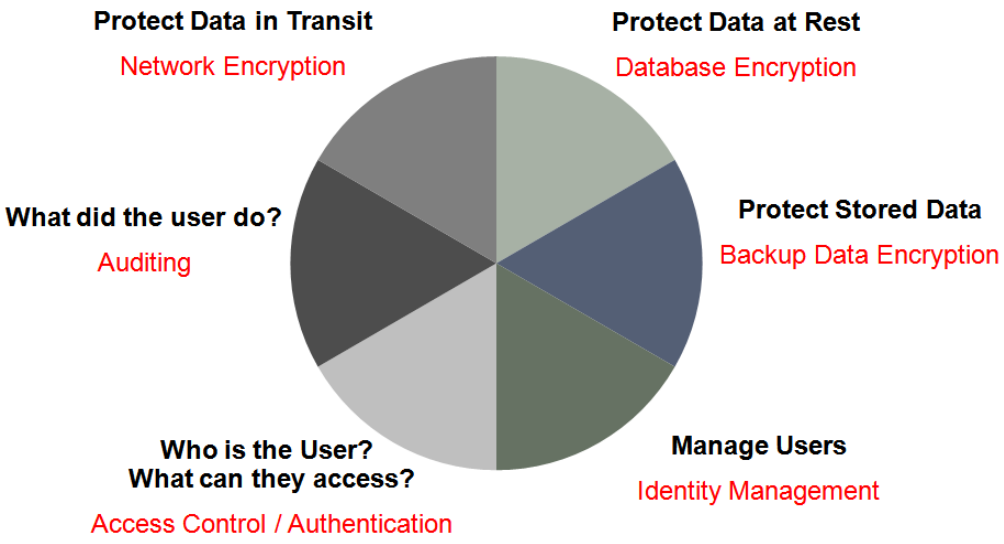
Implementing data privacy is complicated and can be costly. Because of this, it can be very tempting to simply try to avoid the issue and either hope that you don't get caught, or that any fines or penalties will outweigh the cost of actually implementing data privacy measures. However, there are a number of other factors that organizations must consider outside of simply being fined for not adequately protecting employee data.

These risks include:

- Complaints and dissatisfied customers
- Loss of business/customers
- Enforcement action and fines
- Adverse criminal/civil action against the organization's legal entities, executive management and individual staff members
- Adverse publicity
- Reputation and brand damage
- Loss of trust and confidence
- Adverse impact on shareholder value

Leveraging Technology for Data Privacy

At both the database level and application level, there are a number of key features tied to security that can help with privacy compliance.



Network Encryption – Protecting Data in Transit

Network encryption (sometimes called network layer or network level encryption) is a network security process that applies crypto services at the network transfer layer - above the data link level, but below the application level. Network encryption can protect data in transit through use of options such as:

- Advanced Security Option (if using an Oracle database)
- SSL (Secured Socket Layer): Oracle takes advantage of HTTPS, SSL, and digital certificates to secure the transmission of data from the web server to an end user's web browser and also to secure the transmission of data between Oracle servers and third-party servers (for business-to-business processing) over the Internet.

Database Encryption – Protecting Data at Rest

Oracle provides several techniques for database encryption. Some techniques that are commonly used are discussed below

Transparent Data Encryption (TDE)

TDE allows convenient encryption of sensitive data within the database and protection of the keys that are used to encrypt the data. Using TDE, when users insert data, the database transparently encrypts and stores it, whilst at the same time storing the encryption keys in a separate location. Similarly, when users access data to view, the database automatically decrypts it. This prevents anyone from using the data without the encryption keys. Since all this is done transparently, and without any change to the application code, the feature has an appropriate name: Transparent Data Encryption. By transparent we mean that as far as the user is concerned the process is seamless; they are unaware that encryption and decryption is occurring and they cannot control the process. TDE provides outstanding data security in the event of theft of data storage devices. With proper setup, it will ensure that sensitive data is unable to decrypted from a data disk, if that falls into unauthorized hands. However, since encryption and decryption consume CPU cycles, you must consider the effect on performance and you may wish to encrypt data selectively. Also, insider/super-user access cannot be controlled using TDE.

Database Vault (DB Vault)

At the database level, Oracle's Database Vault secures data from the System Administrators, reducing the insider/super-user threat. Database vault stops access to potential rogue programs that may try to hack the system. Oracle Database Vault addresses common regulatory compliance requirements and reduces the risk of insider threats by -

- Preventing highly privileged users (e.g. DBA's) from accessing application data
- Enforcing separation of duties
- Providing controls over who, when, where and how applications, data and databases can be accessed.

FND/DBMS_CRYPTO

Encryption using a built-in package DBMS_CRYPTO (or Oracle Applications supported FND_CRYPTO) offers another solution that can be explored. This technique will encrypt the data and store it in the database in the encrypted format. When you query from the database no matter what tools you use, the data is always returned in the encrypted format, unlike TDE. This technique may be applied to all rows and columns selected for encryption with certain caveats. To implement successfully, you must carefully choose the hooking point on which to peg the additional code that will be executing the encryption. This is important especially where validation is involved, since encrypted data will fail all validation unless decrypted values are passed to the validation routines. For example, if we decide to encrypt blood group held by a form item or page field item on which we have following validation rules implemented - blood_group in ('A', 'B', 'O', 'AB') - then validation will fail since the encrypted equivalent values will be very different from 'A', 'B', 'AB' or 'O'. The solution is to encrypt these values just before storing in the database using a database trigger or similar technique, and decrypt it before any validation starts.

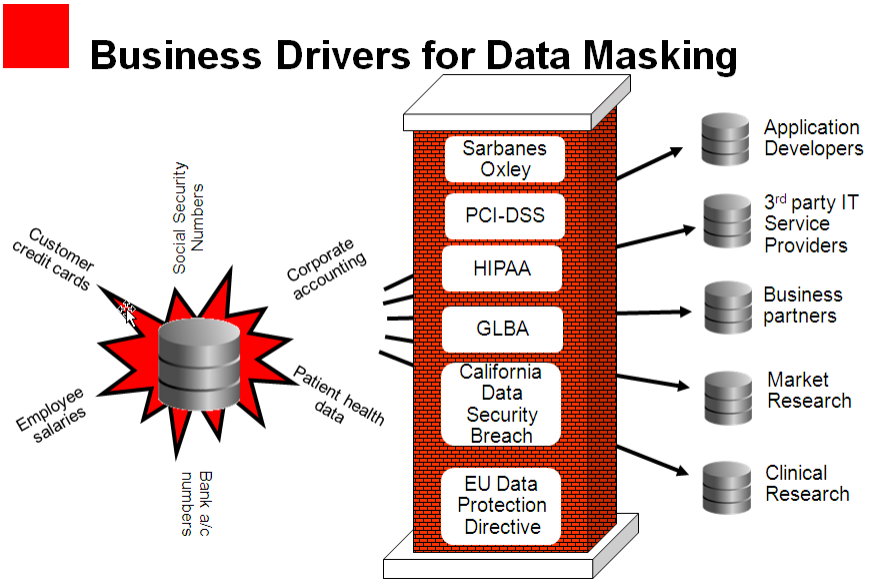
Data Masking at the UI layer

Oracle also provides for Data Masking techniques at both the database and the UI layers. From the UI perspective, a customer can use either OAF personalization at 'responsibility' level or Forms personalization. The Item property 'Conceal Data' can be used to mask data. This property is available for use in personalization. This is typically used for fields such as SSN, Citizen Identification Number etc. where there is a requirement to see the last 4 digits only.

Backup Data Encryption – Protecting Stored Data

Whilst a great deal of effort is expended in ensuring that sensitive data that is collected and stored onsite is secure, security issues involved in sending backup media to offsite storage for safekeeping often do not receive the same level of attention. Offsite media can be lost or stolen while in transit, exposing sensitive information to potential misuse. By using encryption on backup data, sensitive information will remain safe and secure, even if the backup tapes are lost or stolen.

Data Scrambling and Masking – Protection during Cloning of Instances



Cloning databases during regular maintenance, implementation and testing activities is normal. A customer might need to clone instances for testing purposes, upgrade activity, performance testing, adding new functionality etc. This is because the closer the test systems is to production, the more relevant and valid the tests are and hence mitigate the risk of the project itself. However this might result in sensitive and identity data being exposed to different audiences which is inappropriate and also can result in legal liability (HIPAA : the Health Insurance Portability and Accountability Act in the US and Data Protection Directive in the European Union). It can also result in identity theft. Hence we need to offer a comprehensive Data Scrambling technique that can achieve the twin requirements:

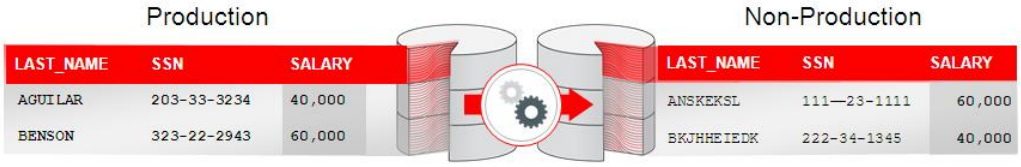
1. Prevent unauthorized access to personal, identity and security data (Personal Data, Job Data, Lifestyle Data, Hierarchy Data etc.)
2. Keep the Scrambled Data as realistic as possible to simulate real world scenarios

Oracle offers the Oracle Data Masking Pack that achieves the desired data scrambling results.

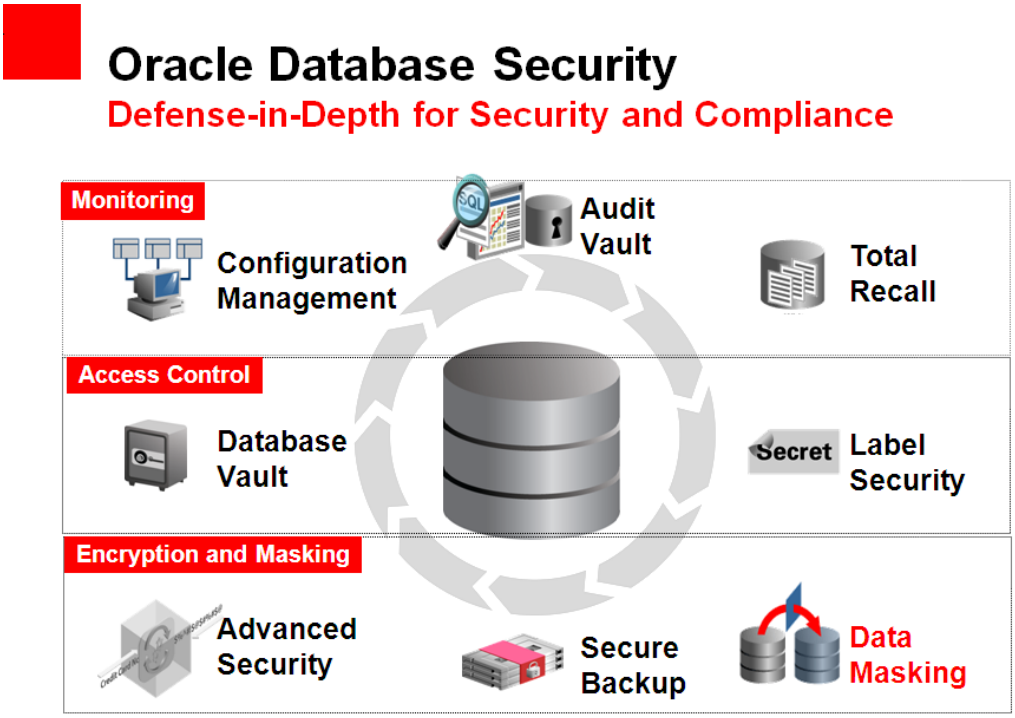
- Remove sensitive data from non-production databases
- Referential integrity preserved so applications continue to work
- Sensitive data never leaves the database
- Extensible template library and policies for automation

Oracle E-Business Suite HCM has already pre seeded all the desired data elements that need to be masked across the HCM family. This includes personnel, organizational and lifestyle

information. Customers can use this as-is or use the pre seeded data elements as a starting point to decide what they want masked or scrambled. This would vary on the business processes that they envision being tested.



To summarize, Oracle's database security techniques provide for end-end data security and privacy.



Identity Management – Managing User Access

When it comes to identity management, there are actions that can be taken at the database and application level. At the database level, E-Business Suite customers may want to consider utilizing two options for identity management:

- Oracle Internet Directory (OID) – Oracle Internet Directory serves as the central user repository for Oracle Identity Management, simplifying user administration in the Oracle environment and providing a standards-based application directory for the heterogeneous enterprise
- Lightweight Directory Access Protocol (LDAP) – LDAP is an Internet protocol used to access a directory listing. Organizations typically store user profiles in a central repository, or directory server, that serves user information for all of the programs that require it. If your existing computer network uses an LDAP V3 compliant directory server, Oracle supports that use case as well.

At the application level, you will always want to maintain roles and responsibilities using the Oracle E-Business Suite Security Model. However, you can maintain user profiles in Oracle or reuse user profiles and roles that are already defined within an LDAP directory server, if you are using LDAP. A directory server enables you to maintain a single, centralized user profile that you can use across all of your Oracle and non-Oracle applications. This approach reduces redundant maintenance of user information stored separately throughout your enterprise, and reduces the possibility of user information becoming unsynchronized.

Oracle E-Business Suite provides the following capabilities:

Roles limit the scope of access

- Each user is assigned to one or more roles
- Roles are named sets of privileges that determine a user's functional access
- Users only see the menus, screens and data that their role permits

Built-in user account management

- Users maintain their own passwords
- Self-service account and role requests make it easier to provision access
- Powerful password policies (e.g., expiration rules, requirements, account disabling)

External user account management

- Provided with Oracle Internet Directory (Other LDAP directories can also be used)
- Delegated administration features allow external organizations to create and manage their own accounts

Please refer to Steven Chan's blogs for more details and tips on EBS Security Techniques - (http://blogs.oracle.com/schan)

Please refer to the Oracle® E-Business Suite System Administrator's Guide – Security Release 12.1 Part No. E12843-04

Application Security – What Can the User Access?

Please refer to the following documents for a detailed technical write-up and explanation on access control and security.

1. Understanding and Using HRMS Security in Oracle HRMS - White Paper
2. Oracle® Human Resources Management Systems Configuring, Reporting, and System Administration Guide Release 12.1 Part No. E13509-03. (This document has a whole section on Security Rules.)

A simplified version is detailed below.

Overview

All Oracle HCM users access the system through a responsibility that is linked to a security profile.

The responsibility is the primary means of defining security. Business groups, menu structures, task flows, and information types are linked to a responsibility. The security profile determines which records (related to organizations, positions and payrolls) the user can access within the business group. This restriction enables secure, reliable data access and ensures that only people with the correct permissions can access personal data.

Depending on which security model is used, the deployment of responsibilities and security profiles to users requiring access to more than one business group can be managed using security groups.

Oracle HCM provides two different security models which enable you to set up security specifically for your enterprise: Standard HCM security and Security Groups Enabled security. Security groups enable responsibilities to be reused by linking them to many security profiles in different business groups if required.

Security processes are run to grant maintain the lists of organizations, positions, payrolls, employees and applicants that security profile holders can access and to set up and update the Security Groups Enabled security model.

Security Profile

The Security profile is the means by which you determine what users of the system have access to what data. It determines which type of person records are available. For instance, Applicants, Employees, Contingent Workers or Contacts. You then determine which work structures or other criteria you want to use to restrict access. For example, a particular HR Adminstrator may

only be given access to employees in organizations within a specific region, and only a senior Payroll clerk would be allowed access to employees in the Director's payroll.

Security Models

Oracle HCM provides two different security models which enable you to set up security specifically for your enterprise: Standard HCM security and Security Groups Enabled security (formerly called Cross Business Group Responsibility Security).

Standard HCM security restricts access to your enterprise's records and data. To set up Standard HCM Security, you first create responsibilities and then define the windows, menus items, workflows, data and records the user can access. The System Administrator then assigns users to as many of these responsibilities as is required to complete their business tasks. If you are using Standard HCM Security, you must ensure that the Enable Multiple Security Groups profile option is set to the default value No. You must then create a security profile for each distinct security grouping of employees your enterprise requires. You then create a responsibility for each user type you require, for example HR Manager, Branch Manager and Salesperson, and link the security profile and responsibility to a business group. These three elements create a security grouping to which you assign employees. By assigning users to the security grouping, you grant them access to the records, menus and data defined in the security profile and responsibility. You can add further users to this security component, but you cannot re-use the security profile and responsibility within another business group.

Security Groups Enabled allows you to assign a single responsibility to more than one business group, and hence enable users to access records from numerous business groups, although users cannot view information from different business groups simultaneously. To set up Security Groups Enabled security, you set the Enable Security Groups Profile option to Yes, and run the Enable Multiple Security Groups process. These steps in combination create a Security Group which has the same name as the business group from which it was created. Like Standard HCM Security, your enterprise must create Security Profiles for each distinct security grouping within your enterprise. Security Profiles function slightly differently in the Security Groups Enabled model than they do in Standard HCM security. Rather than one security profile being assigned to one responsibility, Security Groups Enabled security enables your enterprise to assign numerous security profiles to a responsibility. For example, an HR Manager and an Assistant HR Manager may be able to access the same menus and windows, but may be able to view different data. The functionality of responsibilities is also enhanced in the Security Groups Enabled security model. Increasingly, users require access to the records in more than one business group. To accomplish this, you can assign a responsibility to multiple business groups when you use Security Groups Enabled. The records, forms and type of data a user can access will be the same in each of the business groups to which they have access.

Security List Maintenance

Oracle HCM enforces security rules by using secure views which call a security function that works out access based on whether the security profile is dynamic or uses static lists. The static lists of people, organizations, payrolls, and positions are indexed against each security profile. They are maintained by a concurrent process called Security List Maintenance which is usually run overnight to ensure that any changes during the day that would affect the availability of a person's record i.e. organization, is reflected in all secure responsibilities the following day. If security profile is dynamic and not static, Security List Maintenance need not be run. Dynamic or user-based profiles are Supervisor, user-based Organization and Position security, custom security using the 'Restrict the people visible to each user using this profile' option, or Assignment Level Security.

Reporting Users

Your enterprise can also set up request groups to restrict user access to reports and processes. The request group is associated with a security profile which defines the data a user can view, and is then assigned to a responsibility. It is also possible to set up reporting only request groups for users who access the database, but who are not permitted to change any of the records within the system.

Self-Service Users

Oracle's security around self-service is two-fold. If the user is an employee, the system can match the user ID to the employee's ID and enables the employee to access only his or her own records. For manager self-service transactions, you can define the data permissions per transaction by matching the users' IDs with the reporting information on employees' job records. The system allows users to access the records of only the employees that report to them based on the employees' IDs or manager's ID driven by the "supervisor ID," the "report to" field, or the department manager ID.

Oracle User Management

Oracle User Management is a secure and scalable system that enables organizations to define administrative functions and manage users based on specific requirements such as job role or geographic location. With Oracle User Management, instead of exclusively relying on a centralized administrator to manage all its users, an organization can create local administrators and grant them sufficient privileges to manage a specific subset of the organization's users. This provides the organization with a more granular level of security, and the ability to make the most effective use of its administrative capabilities.

You can use the regulatory region functionality for country and region-specific transaction processing driven by regulatory requirements or local customs – such as ethnicity, diversity,

religion, disability, health, and safety data. This functionality filters country and region-specific data that is specifically addressed in the data protection requirements.

The Internet poses challenges and opportunities for organizations trying to abide by the Data Protection rules. Employee Portals can help deliver the organization's policy statements on data privacy to all employees. Employees who have access and take ownership of their own data are less likely to have to ask – "what data is held on my record?"

In addition, on the personal information page, a customer can use special information type to keep track of whether or not an employee gave permission for records to be collected or passed between countries.

Auditing, Logging and Governance – What Did The User Do?

In some countries, employees can ask to see data held on them at any time. They can also ask for information on who else can view and change the data and what the data is used for. Within the Oracle HCM database you can define the level of audit and logging you require. Although the system allows for auditing at the data field level most organizations setup audits at the table level. For example - audit when the personal data table has been changed, the user login of the person making the change, the time and date of the change and the before and after value.

Oracle Audit Vault provides more comprehensive and enterprise wide auditing capability. These definition changes (create/update/delete) are recorded and the information is immutable (unchanging and unchangeable). Oracle E-Business Suite also supports transaction level logging and auditing at a functional layer

Oracle applications also provide detailed audit trails that indicate who has accessed or changed what information at what location and at what time. Data protection directives have challenged all multinational organizations to comply with its requirements when accessing, collecting, and transferring personnel data. For example, European ministers recognized the considerable potential of global information networks to foster economic growth. Ministers representing the 15 member countries and other interested entities – such as Japan and the United States – agreed to work together toward global principles on the free flow of information, while protecting the fundamental right to privacy of personal and business data. Data protection officials have welcomed the development of powerful services and software tools that enable information search, retrieval, and delivery directly to the user of specifically requested information.

Oracle also provides a comprehensive GRC Suite that helps with the governance aspects of using EBS applications and segregation of duties. Details on the Oracle GRC Suite can be found at http://www.oracle.com/us/solutions/corporate-governance/index.htm.

Real-Time Enforcement of Segregation of Duties and Access Policies

The ability to fine-tune user access—and to track that access—is key to complying with regulatory requirements and ensuring corporate security. Oracle Application Access Controls Governor provides real-time monitoring and proactive enforcement of crucial access policies, such as those that support segregation of duties (SOD). The system anticipates potential SOD conflicts before they arise, and even prevents any assignment of roles or responsibilities within an application that would compromise proper segregation of duties. Application Access Controls Governor also extends key access controls to "super-users" and temporary or contract workers.

What Is Oracle Doing to Help Customers with Data Privacy Issues?

- Continue to maintain Oracle's Safe Harbor designation.
- Stay on top of changing requirements and incorporate relevant product enhancements.
- Provide a variety of global implementation methods such as centralized, decentralized, or repository/data warehouse approaches.
- Offer a variety of configurable levels and approaches for database security, user security, and object security as well as audit trails that are well documented and broadly implemented.
- Filter country-and region-specific data by using regulatory region functionality used for transaction processing driven by regulatory requirements or local customs, such as ethnicity, diversity, religion, disability, health, and safety data.
- Control default fields and values throughout the system by using the operator preference feature.
- Track whether the employee gave permission for records to be tracked and passed between countries
- Provide employee self-service for employees to access their personal information at any time for accuracy and update.
- Offer customers the option to encrypt data as it traverses the network.

While Oracle Human Capital Management applications provide many capabilities to help customers meet the requirements of data privacy organizations worldwide, we can only provide the tools – we cannot guarantee compliance. Data privacy is primarily a business policy/process issue. Software can help support these policies/processes but can't define the policy/process. Compliance comes when an organization works with their local data privacy organization and with their employee works councils to fairly interpret requirements particular to them. Each

organization may interpret these requirements differently depending on their location, industry and individual situations.

Conclusion

Data Privacy, Data Protection and Trans-border Data Flow are critical issues for Human Resources organizations operating in a Global Environment. Because of the large number of global customers using our HCM Applications, Oracle is committed to providing both functional and technical solutions to help support companies' compliance with Data Protection legislation. It is no longer a luxury to manage a global employee organization to compete effectively - it is a necessity. The risks of non-compliance not only have financial and criminal action consequences, the misuse of employee information can affect the reputation and brand image of an organization. Our goal is to help provide solutions – both on and off-premise to help our customers solve their issues around protecting an employee's personal information.

Oracle E-Business Suite HCM
Data Privacy – Challenges and Solutions
March 2010
Author: Row Henson
Contributing Authors: Anand Subbaraman, Stephen Hughes

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

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

0109