# Table of Contents

What is Data Privacy and Who Should Be Concerned?.................... 3  
What Constitutes Personally Identifiable Information (PII?) ............ 3  
OECD Guidelines........................................................................ 4  
Compliance Options – Country to Country.................................... 7  
Risks of Non-Compliance ............................................................... 8  
Leveraging Technology for Data Privacy ........................................ 9  
Data Privacy for PeopleSoft HCM Solutions ................................. 12  
What Is Oracle Doing to Help Customers with Data Privacy Issues? 16  
Conclusion .................................................................................... 17
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 PeopleSoft 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\textsuperscript{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.

\textsuperscript{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 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](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. Work 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.

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)**
- **Hardware based encryption**

Database Encryption – Protecting Data at Rest

At the database level you can use products such as [Transparent Data Encryption](#) (TDE) to encrypt data stored in the database. TDE allows you to encrypt sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. This prevents anyone without the keys from using the data.

You can also use Pluggable Encryption Technology (PET) in PeopleTools to encrypt sensitive data at the application level to provide additional protection for PII. PeopleSoft pluggable encryption technology (PET) provides a way for you to use hashes and digital signatures to secure critical PeopleSoft data and communicate securely with other businesses. It enables you to extend and improve cryptographic support for your data in PeopleTools, giving you strong cryptography with the flexibility to change and grow, by incrementally acquiring stronger and more diverse algorithms for encrypting data.

And finally, in the PeopleSoft environment, we use Verity as the delivered search engine but it can be configured to limit information returned based on security permissions.

Backup Data Encryption – Protecting Stored Data

Although there is a lot of effort to protect data that is collected and stored onsite, often security issues involved when sending backup media to offsite storage for safekeeping is not considered. 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.

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, PeopleSoft customers may want to consider utilizing LDAP for identity management. [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, PeopleSoft supports the use of that server for managing user profiles and authenticating users. PeopleSoft enables you to integrate your authentication scheme for PeopleSoft with your existing infrastructure. PeopleSoft delivers pre-built configurations for Oracle Internet Directory, Novell eDirectory, Microsoft Active Directory and Sun Directory Server. A generic template is also delivered for custom LDAP configurations.

At the application level, you will always want to maintain permission lists and roles using PeopleSoft security. However, you can maintain user profiles in PeopleSoft security 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 PeopleSoft and non-PeopleSoft applications. This approach reduces redundant maintenance of user information stored separately throughout your enterprise, and reduces the possibility of user information getting out of synchronization.

You can also configure and extend your sign-on PeopleCode to work with any schema implemented in your directory server. You can assign roles to users manually or assign them dynamically. When assigning roles dynamically, you use PeopleCode, LDAP, and PeopleSoft Query rules to assign user profiles to roles programmatically.

Access Control / Authentication – What Can the User Access?

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 might 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 (DBA) from accessing application data
- Enforcing separation of duty
- Providing controls over who, when, where and how applications, data and databases can be accessed

At the application level, PeopleSoft delivers the most common authentication solutions and packages them with the PeopleSoft application. These prepackaged solutions include PeopleCode that supports basic sign-in through secure sockets layer (SSL), LDAP authentication, and single sign-on. PeopleSoft 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 PeopleSoft servers and third-party servers (for business-to-business processing) over the Internet.
Additionally, PeopleSoft employs the use of row-level security, navigation security, and role security. Row-level security allows you to design special types of SQL views -security views- to control access to individual rows of data stored within your application database tables. Navigation security defines the specific navigation allowed for each user or group of users. And role security defines the specific permissions a user can access such as pages, environments, time periods, administrative tools, personalizations, and so on.

**Auditing – What Did the Application User Do?**

At the application level, PeopleTools auditing can be turned on at the record/field level to track the data each user has added/updated/deleted. Oracle Audit Vault provides more comprehensive and enterprise wide auditing capability. PeopleTools provides features to audit record/field definition changes. These definition changes (create/update/delete) are recorded and the information is immutable (unchanging and unchangeable). Oracle Audit Vault provides consolidated auditing across the enterprise, including SELECT or view access with the Oracle database.

**Data Privacy for PeopleSoft HCM Solutions**

Whether you send personal information from one country to another or not, protecting the confidentiality and integrity of your human resources data is one of an organization’s highest priorities. PeopleSoft provides several tools to help enable data protection:

- Architectural tools
- Portals and self-service options
- Auditing tools

**Architecture**

Using permission lists and roles gives your security setup scalability and enables you to distribute the maintenance of your security system. Managers can give their employees the security access they need simply by assigning them to the appropriate role.

Data permission security enables you to grant and restrict access to employee-level data using security trees and data permission lists. The system enforces data permission security using security search views to access employee data.
View of Row Level Security in Tree Manager

PeopleSoft’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.

PeopleSoft’s global security limits user access to the global panels throughout the system depending on your enterprise’s business needs, policies, and procedures. This functionality also limits any single user’s or group’s access to specific country security. With panel/page level security, a global system will be able to ensure that access to sensitive, confidential, and personal information is controlled by limiting the number of users who have access to that information.

Using business units and SetIDs, you’re able to associate a business unit with employees in your enterprise. The flexibility to share TableSets among business units enables you to centralize redundant information while you keep other information – such as department and job codes – decentralized. This functionality enables you to limit the setup data available in a given transaction.

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.

Within the PeopleSoft HCM architecture, we offer customers the option to encrypt data as it traverses the network. We also support options to encrypt the browser to web server connections through the use of Secure Sockets Layer (SSL). SSL support also provides for securing the HTTP-based integration technologies such as PeopleSoft Application Messaging and Business Interlinks. For the application server to database server connection, you can secure encryption from the database. For example, Oracle offers SQL*NET Secure, which provides for data encryption. In addition authentication mechanisms include the use of digital certificates, Lightweight Directory Access Protocol (LDAP), and integration with third-party single sign-on solutions.

CONTROLLING ACCESS TO DATA IN THE PEOPLESOFT ENVIRONMENT

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, the “waive data protection” button keeps track of whether or not an employee gave permission for records to be collected or passed between countries.
Audits

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 PeopleSoft HCM database you can define the level of audit 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.

If an employee wants to know where data is sent as part of an automatic process then you can use the Workflow diagrams to produce a document that will provide this information. When an employee changes dependent data you could setup a workflow to automatically send a notification to the dependent listing the data that has been added to the database. There may be occasions when an employee decides to change the level of permissions they have agreed with the company on data protection. For example the employee may have agreed to their data being used for marketing when they were hired but later decided to restrict the use of their data. You could define company specific contract clauses to cover these eventualities; any changes to contracts are effective dated.

PeopleSoft 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.

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 with an option in the PeopleSoft HCM system.
- 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 PeopleSoft 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, PeopleSoft 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 to help our customers solve their issues around protecting an employee’s personal information.