Data Privacy in Oracle PeopleSoft and Cloud Products

Higher Education User Group

January 2018

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Data privacy – or the masking, encryption, and scrambling of specific data points – is very important to protect the identity and assets of our constituents, and the penalties for a breach can be significant. Additionally, data privacy laws and regulations, as well as institutional initiatives, are very broad, vast, and always changing, thus requiring solutions to protect all kinds of data - deemed as relevant data points on a more institutional or local regulatory basis – be configurable and easy to implement. This white paper aims to highlight the most beneficial enhancements or new features in the area of data privacy. These recommended enhancements or new features would serve to allow easy configurability to protect institutions' data points and allow for their ability to become – or stay - compliant with any relevant regulations, laws, or institutional policies in an efficient manner.

During Higher Education User Group (HEUG) Summit 2016, advisory group and board members identified a need to discuss and advocate for functionality and standardization around built-in data encryption, masking, and scrambling within and amongst all three PeopleSoft systems (Campus Solutions, HCM, and Financials,) as well as any new, or existing, Oracle cloud ERP products used by HEUG institutions. Out of these discussions, the HEUG sponsored a working group to solicit and review recommendations for enhancements or new features related to data privacy from the HEUG communities. The goal of the group was to formulate and write up the recommendations in the form of this white paper. The working group consisted of members of the HEUG communities at large, the HEUG Board of Directors, and members of the following Advisory Groups (AG): Human Capital Management (HCM), Campus Community (CC), Contributor Relations (CR), Procurement to Pay (PTP), Reporting and Business Intelligence (RBI), Financial Aid (FA), and the Technical Advisory Group (TAG).

After the recommendations for enhancements or new features were collected from the HEUG communities, the working group evaluated and prioritized the items - with regard to their level of impact on the HEUG communities as a whole - as either first or second priorities. These priorities were agreed on using feedback from the AGs and HEUG community members, as well as our own experiences and knowledge. The approach was chosen in order to clearly communicate the main areas of interest, with a view to identifying the areas that we would like Oracle to consider as primary or secondary priority items.

While our recommended priorities were defined based on input from the HEUG community, we realize that regulations in this area are always changing and that regulatory obligations – such as those currently being constructed in the General Data Protection Regulation (GDPR) – may cause a need for Oracle to adjust or add priorities to this list as deemed appropriate.

Additionally, we find it prudent to note that, while at the time of our research, the HEUG community did not find the ability to purge sensitive data sets enough of an imminent priority to include in this paper, we are aware that GDPR regulations are currently being written for European Institutions to comply with a 'Right to Erasure' policy in the future and this, as well as

other regulatory items, may need to take precedence over items prioritized by the community. To-date, in the PeopleSoft products, this function can be addressed by using the Data Archive Manager and/or the delivered Employee Delete Process, however, these processes do have some limitations that may make complete compliance with the new GDPR regulations more difficult without customization. We have become aware that Oracle – at least in their PeopleSoft HCM product – have started to make some improvements in this area including, for the Employee Delete process, the ability to override the ID Delete Control Check, the ability to allow users to configure exclusion tables to retain certain types of data – such as audit data, and better logging.[i] While we have not prioritized this item in this paper, we recommend that any functionality that is delivered in a particular product to address the GDPR 'Right to Erasure' is replicated across all PeopleSoft products and their Oracle Cloud counterparts.

A detailed explanation of each priority item is contained within this white paper. For each priority item, we detail a summary of what the item is, list out any known bug or enhancement requests related to the existing functionality or desired functionality, describe the summary of need from our HEUG constituents using use cases where applicable, and suggest embodiments – or possible configurations – for the desired functionality. First priority items are: define a minimum field list to recommend delivered masking, encryption, and/or scrambling at the component/page level; and masking/encryption of fields for internal and external integrations. Second priority items are: multi-factor authentication within the applications themselves; and encrypting/scrambling of non-production data.

2. DEFINITIONS

Since many common terms related to data privacy can be used in varying ways throughout different industries and software products, please reference the following definitions of common terms used throughout this white paper.

Scrambling or obfuscation – consistently scramble identified fields in a legitimate format throughout the database so it is not usable to steal an identity. The process is irreversible so the original data cannot be derived from the scrambled data. This is good for non-prod data and not good for prod data.

Masking – hiding all or part of a field so users accessing a system cannot see it through the user interface.

Encryption – Convert information in a database so it is unreadable if accessed directly. If the information is accessed through the user interface, and the user has appropriate privileges, the data appears correctly. This function may be combined with masking.

PII - Personally Identifiable Information (PII) - PII field(s), while varying in definition based on the state or region, is loosely defined as any data that could be used to identify a person.

3. Data Privacy – Summary and Priority List

Summary

Easily configurable and standardized data privacy functionality, for all institutions, is core to reducing the chances, as well as the impact, of a data breach within and amongst all PeopleSoft products and other Oracle products used in Higher-Ed, such as Oracle's line of Cloud SaaS products for Student, HCM, and Finance. Furthermore, data privacy regulations, laws, and internal institutional policies vary extensively and are always changing and adapting, therefore, having robust and configurable delivered methods to protect data at the application level, will provide a lower barrier to institutions that want – or need – to protect their constituents data and assets. To this end, we have identified, from the user community, areas where we believe that delivered modifications or new functionality would bring the most benefit to the community and we have organized them by priority to reflect the items that we understand to be first priority and second priority to the community. While these recommended priorities were defined based on input from the HEUG community, we realize that regulations in this area are always changing and that regulatory obligations – such as those currently being constructed in the GDPR – may cause a need for Oracle to adjust or add priorities to this list as deemed appropriate.

Priority List

Data Privacy First Priority Items

1. Define a minimum field list to recommend delivered masking, encryption, and/or scrambling at the component/page level
2. Masking/encryption of fields for internal and external integrations

Data Privacy Second Priority Items

3. Multi-factor authentication within the applications themselves
4. Encrypting/scrambling of non-production data

4. Data Privacy – First Priority Items – Detail

1. Define a minimum field list to recommend delivered masking, encryption, and/or scrambling at the component/page level

Summary of current functionality

Existing Functionality in the PeopleSoft pillars:

Limited functionality, known as Demographic Data Access Security (DDA security) exists in PeopleSoft Campus Solutions. DDA security is limited to only two display fields - National ID and Birth Date - and allows for masking the display of these fields in search records, prompt records, and on the Bio/Demo Data and the Relationships pages. Additionally, you can mask entire fields, the first five characters of the national ID field, or the year of the birth date field. This functionality is implemented through the use of PeopleSoft security and permission lists and requires that both the user and the page have display-only security.[ii]

The above referenced delivered functionality is only available for the PeopleSoft Campus Solutions product. No other functionality to mask, scramble, or encrypt data fields at the component or page level is known to exist for any of the PeopleSoft pillars.

Existing Functionality in the Fusion framework for Oracle Cloud products:

This functionality, as delivered by Oracle, is not known to currently exist, in any form, within any of the fusion cloud products.

Known Oracle bugs or enhancement requests related to functionality

Enhancement #: 20271006
Enhancement #: 18677690
Enhancement #: 20271006
Oracle Doc ID #: 1961214.1

Summary of need

The masking, encryption, and scrambling of data points, deemed as sensitive by an institution or regulator, is very important to protect the identity and assets of our constituents. In most institutions, a large number of people have access directly into software products that contain sensitive data. Often, staff members do not actually need to see all - or part - of these sensitive data fields to do their jobs, but they do need to have access to the components/pages that contain this data. Thus, providing the option for institutions to limit access to data deemed by them as sensitive, institutions would be able to easily take steps to largely reduce the potential of a data breach being

caused due to access to data that was not pertinent to a staff members job responsibilities.

Additionally, because data privacy laws and regulations, as well as institutional initiatives, are very broad, vast, and always changing, there is a need for more - or all - fields to have the ability to be either masked, scrambled, or encrypted among all of the PeopleSoft products. A full survey of regional requirements has not been undertaken, however, as global products, the software should provide for configurable masking of required fields in order to ensure the legislative compliance required by individual nations/jurisdictions. Our survey responses focused on fields such as SSN and DOB, which may hint at North American-focused requirements (the majority of the survey respondents reside in North America). For other regions, such as Europe, SSNs are less prominent as person identifiers, and fields such as National_ID, names, addresses, and phone number would require equal priority in terms of masking. Due to the global reach of these products, using the National_ID field to store and secure the SSN – and other national identification numbers - rather than the SSN field is recommended. Furthermore, regional legislation within Europe currently requires enhanced protection around personal data fields such as those relating to sexuality, ethnicity/nationality, trade union/political affiliations, physical/mental health, criminal record and religion.

As an example of the need for configurability, at the moment, the United States of America (U.S.A.) Data Privacy regulations and protections are limited unless your data is transferred overseas or falls into a certain sector, such as Health or Financials - and is regulated by a specific act or statute pertinent to that type of sector - however, the Federal Trade Commission (FTC) and the U.S. Congress have been discussing regulatory changes to enforce data privacy at a more broad level in the future. Additionally, in May 2018, the 1995 European Union (EU) Directive (and regional Data Protection legislation) will be repealed and replaced by the EU General Data Protection Act (GPDR) across all member states - including the United Kingdom (UK). This regulation will bring significant changes to Data Privacy and Protection regulatory standards and its impact will be felt globally - it will mandate stringent 'data minimization' requirements (i.e. 'privacy by design' and 'privacy by default') and will bring increased fines and penalties; it will also impose restrictions on the processing of EU citizen data inside and outside of the European Economic Area (EEA,) and will enhance individuals rights. In the UK, the Information Commissioners Office has indicated that the GDPR will be active before BREXIT, and is likely to remain the legislative model post-BREXIT. As countries, and Institutions themselves, are creating more strict regulations and policies around what data fields to protect, it will be more important for institutions to have the ability to adapt quickly to these requirements.

RECOMMENDED EMBODIMENTS FOR A SOLUTION

Our survey respondents showed interest in the ability to mask, encrypt, and/or scramble many different types of fields. Consistently, respondents indicated that they would not like to be confined by only having the ability to mask, encrypt, or scramble only a limited number of defined fields. However, due to the varying and constantly changing internal and external policies and regulations around data privacy and breach, respondents showed extreme interest in consistent and delivered functionality amongst all of the PeopleSoft pillars – at the time of the survey, not many HEUG institutions used Oracle cloud products - that allowed for easy configuration to mask, encrypt, or, scramble any data point as they see fit, at any given time, based on their individual requirements at that time. Additionally, as a consequence of the EU GDPR – and potentially regulations from other countries to follow, Higher Education Institutions will have a greater need for configurable data minimization functionality within the product. Greater control will become more important at the application layer to restrict visibility and update access to PII and other data fields deemed sensitive.

While configuration to mask, encrypt, or scramble any data point is the preferred embodiment by the working group, at a minimum, we feel that it is important to offer this ability for all data fields considered - by most data privacy regulations - to be either PII data or other sensitive data - such as banking data, salary, data, or health data - that if acquired by unauthorized parties would constitute a data breach by the majority of regulations internationally. If this embodiment were to be chosen, we realize that not all data privacy and breach laws - in the U.S, Europe, and other countries - are consistent in what data they feel is sensitive enough to constitute a breach. For example, some regulations only constitute certain data points - such as driver's license number or email address - as causing a breach if other PII data is included in the unauthorized acquisition of data. Furthermore, many of these regulations also differ on how much of certain data points need to have been acquired - for example, some regulations require that the whole last name be acquired and others only require that part of the last name be acquired. For this embodiment, we suggest that as many data privacy and data breach regulations - from all U.S. states and other relevant countries and jurisdictions - be reviewed, and that a list of common data points considered sensitive - either alone or in combination with any other piece of data - be compromised and used as a base number of fields to be delivered with the ability to be either masked, scrambled, or encrypted. Since the GDPR requirements are likely to be the strictest regulatory requirements in the near future, using those requirements as a minimum might make the most sense.

For both of the embodiments above, we suggest that this ability be secured and implemented in a manner that is consistent with how the current masking functionality for National ID and Birth Date currently work in PeopleSoft Campus Solutions. Thus, we would recommend that this functionality be implemented through the use of PeopleSoft security and permission lists – or their equivalent in the cloud products - and require

that both the user and the page have display-only security. However, conversely to the limitations of the current functionality to only mask all or certain parts of these fields, we would recommend that the user be able to define how much of a data point they want to be either masked, scrambled, or encrypted.

2. MASKING/ENCRYPTION OF FIELDS FOR INTERNAL AND EXTERNAL INTEGRATIONS

SUMMARY OF CURRENT FUNCTIONALITY

Existing Functionality in the PeopleSoft pillars:

Oracle introduced database level redaction in Oracle database 12c as part of the Advanced Security Option (ASO). ASO is an add-on option and is not included in the base version of the database. Database level redaction allows partial or full redaction, with masking, of data returned by a query. ASO redaction has also been backported to Oracle database 11g in version 11.2.0.4.[iii]

Database level redaction is a good solution for read-only applications such as reporting. However, since the data is redacted by the database at the time of query, this is not a recommended solution for applications that write back to the database, since the redacted data will be stored in the database, possibly replacing the actual value.

Additionally, PeopleSoft HCM and Campus Solutions offer masking functionality at the application layer for internal and external Search/Match, in order to mask a defined list of personal data fields, configurable using user security. The external searches are conducted using web-services, and can search within the HCM and Campus Solutions databases and external databases; the results are masked on the Integrated Search Results page.

Existing Functionality in the Fusion framework for Oracle Cloud products:

Similar to the ASO option for Oracle databases, a data masking service is available in the Fusion databases for certain Oracle Cloud products built on the Fusion framework. However, the data masking service is only available as an add-on product to customers with a paid subscription to the data masking services. Note that only certain specified PII data points are covered by this masking product and each data point has its own masking techniques that are available based on the type of data. [iv]

Just as in the case of the ASO product, this level of redaction on the fusion database is a good solution for read-only applications such as reporting. However, since the data is redacted by the database at the time of query, this is not a recommended solution for applications that write back to the database since the redacted data will be stored in the database, possibly replacing the actual value.

KNOWN ORACLE BUGS OR ENHANCEMENT REQUESTS RELATED TO FUNCTIONALITY

BUG #: 21949557

SUMMARY OF NEED

The survey asked about current and desired practices for encryption/masking of internal/external transfers and integrations, and responses showed a varied combinations of practice. A strong proportion of survey responses (42%) felt that masking/encryption of fields for internal and external integration should be the first priority. All responses said that they need to test external files in non-production environments, therefore incoming and outgoing data should be protected in all environments - not just production.

For the following example areas related to internal/external file transfers/integrations, the survey showed that data protection is required by a particular regulation or institutional initiative that is applicable to their institution.

a. Outgoing Data examples:
    i. Send ACH/EFT payments with supplier banking information
    ii. Send 1099 file(s) to IRS with supplier TIN information
    iii. Send 1098-T file(s) to IRS with supplier TIN information
    iv. Download any privacy data through PS Query
b. Incoming Data examples:
    i. Receive Student Vendor information through Integration Broker
    ii. Receive HR Person information through Integration Broker
    iii. Import Bank file for bank reconciliation

RECOMMENDED EMBODIMENTS FOR A SOLUTION

In terms of data masking and encryption for data in transit, Higher Education Institutions operate within varied and complex enterprise architectures, however, it would be useful if current industry/technology standards and best practice (across the products) could be defined and standardized (e.g. Secure File Transfer Protocol (SFTP) for any data transmission; encryption of incoming and outgoing files; advice on security model for incoming/outgoing document management).

Oracle data redaction and masking products can be executed at the database level using the Advanced Security Option in an Oracle Database – or the masking service for fusion products, but this is a significant technical project to implement and is an expensive Database add-on option. The HEUG Data Privacy working group's consensus was that data protection should be part of the baseline product, and Oracle deliver greater control by offering a flexible, configurable data masking tool that offers differentiated/field-level masking for internal/external integrations. To support different organizational contexts and enterprise architecture, we recommend a deliverable

through database management tools, in addition to a provision to manage this via security configuration at application layer.

The limited masking configuration available via internal/external Search/Match is indicative of a configurable application layer masking function, which could be extended to mask/encrypt the output of reports and internal/external data transfer processes. We believe that it is important that the design and concept be consistently applied across all applications including Oracle PeopleSoft and cloud products. Suggested solutions include:

i. Option to configure formula to alter the data
ii. Option to turn on/off the masking/encryption features as part of the configuration
iii. Options to setup masking/encryption configuration (eg via Reporting tools or Process Scheduler)
iv. Option to determine masking at the Record/Field or Role/Permission level
v. Oracle to deliver default values
vi. Option to group fields by type or by priority. For example:
    1. Group 1 – TIN, SSN,
    2. Group 2 – Driver License, Birth date
    3. Group 3 – Address

    However, this should be configurable to allow HEIs to determine their own groups.

5. Data Privacy– Second Priority Items – Detail

1. Multi-factor authentication within applications themselves

Summary of current functionality

Existing Functionality in the PeopleSoft pillars:

This functionality, as delivered by Oracle, does not currently exist within any of the PeopleSoft pillars.

Existing Functionality in the Fusion framework for Oracle Cloud products:

This functionality, as delivered by Oracle, is not known to currently exist, in any form, within any of the Fusion cloud products.

Known Oracle bugs or enhancement requests related to functionality

N/A

SUMMARY OF NEED

Access to systems has become increasingly jeopardized in instances where the only factor utilized to access said system is a password. Through social engineering, phishing, and other tactics, hackers are able to obtain these passwords and access the very sensitive data that is stored in HR, Finance, and student record systems. Many real world cases of this have occurred over the past few years resulting in the stealing of direct deposit funds, user data (SSN's, addresses, etc.,) and other data that could be used to steal a person's identity.

RECOMMENDED EMBODIMENTS FOR A SOLUTION

Multi-factor authentication has been adopted by many companies and institutions as an additional protection to ensure a compromised password does not lead to undesirable access of sensitive systems. Since the data inside the PeopleSoft pillars – and Oracle cloud ERP products - is extremely sensitive by nature, having a solution that all the pillars could utilize is paramount to protecting this data. Ideally, the solution would be configurable enough to place at either the initial login to these systems, or to be able to be placed on any component in the system, so that only when those components are accessed, would the multi-factor authentication need to take place. However, we realize that striking a balance between security and ease of use is critical for adoption.

2. ENCRYPTING/SCRAMBLING OF NON-PRODUCTION DATA

SUMMARY OF CURRENT FUNCTIONALITY

Existing Functionality in the PeopleSoft pillars:

For customers deployed on an Oracle database platform, Oracle offers Advanced Security Option (ASO) products such as Transparent Data Encryption (TDE) and Oracle Data Masking. These products are an add-on product and would be an additional cost. Additionally, these products are not PeopleSoft-centric, in that there are no pre-built templates that identify PeopleSoft PII data, thus requiring customers to define the fields to be masked and/or encrypted and to continually maintain the list as product changes are introduced.[v]

Oracle TDE and Oracle Data Masking are not available for customers who run their PeopleSoft environments on a non-Oracle database platform.

Existing Functionality in the Fusion framework for Oracle Cloud products:

Similar to the ASO option for Oracle databases, a data masking service is available in the Fusion databases for certain Oracle cloud products built on the fusion framework. However, the data masking service is only available as an add-on product to customers with a paid subscription to the data masking services. Note that only certain specified

PII data points are covered by this masking product and each data point has its own masking techniques that are available based on the type of data. [vi]

KNOWN ORACLE BUGS OR ENHANCEMENT REQUESTS RELATED TO FUNCTIONALITY

Enhancement #: 156012000
Oracle Doc ID #: 1085149.1
Oracle Doc ID #: 400841.1

SUMMARY OF NEED

Over half of the HEUG survey respondents indicated that they have a requirement at their institution to have the PII and institutionally-sensitive data in their non-production environments scrambled, masked and/or encrypted. Most are required by a Data Protection directive, an Audit Finding or a State/Local Law. While there is a need for this functionality, only a third actually have accomplished this task at the time of the survey using a mix of home-grown and other commercial solutions.

RECOMMENDED EMBODIMENTS FOR A SOLUTION

In an era of increased requirements for institutions and companies to keep data safe, encryption and data masking products are no longer a luxury. In many cases it is required by law. While Oracle offers several products for Oracle and Fusion database users, they are an additional cost to the customer and not part of the base product.

Our recommendation is for Oracle to incorporate a data masking and data encryption methodology into the PeopleSoft product line - and cloud product line - for use by all of its customers.

6. DOCUMENT INFORMATION

PLEASE READ OUR DISCLAIMER

This is a publication of the Higher Education User Group, Inc. (HEUG) and was prepared by a Data Privacy Working Group sponsored and facilitated by the HEUG based on HEUG user feedback and consultation with multiple HEUG advisory groups and Oracle product experts. It is offered in the spirit of professional sharing among higher education users and Oracle. Our intention is to provide an accurate picture of our current understanding of the data privacy functionality within all PeopleSoft products - as well as any new, or existing, Oracle cloud ERP products used by HEUG institutions - and offer suggestions to Oracle Corporation for

improvement of that functionality, but the HEUG accepts no responsibility for any decisions made based on information contained in this document.

Thus, as a condition of your reading and using our White Paper, we require that you agree to the following: In no event will you hold the Higher Education User Group, Inc. or its officers, directors, employees, agents, or volunteers responsible for any decision made by individual institutions in their respective planning processes made after reading the information contained herein. Each institution's situation is unique, and must be evaluated within its own context.

Working Group Participants

Name	**Institution**	**Title**	**HEUG and Working Group Affiliation**
Stephen Brawn	Northwestern University	Senior Software Developer	-CC AG Member -Chair of the Data Privacy WG -Sub-Group Leader of the Data Privacy WG – Item 1
Gregory Stanis			-Former HRMS AG Member -Sub-Group Leader of the Data Privacy WG – Item 3
Shareen Thewke	University of Nebraska	Functional Coordinator for Financial Aid	-Former FA AG Member -Sub-Group Leader of the Data Privacy WG – Item 4
Eimear Nelis	Queen's University Belfast	Governance Lead	-CC AG Member -Sub-Group Leader of the Data Privacy WG – Item 2
Josh Harmon	Texas Christian University	Director, Enterprise Application Services	

Jennifer Bayless	Missouri University of Science and Technology	Assistant Director - Admissions	CC AG Member
Benjamin Biltz	University of Wisconsin	Information Process Consultant	PTP AG Member
Maria Lindquist	University of Wisconsin Extension	Financial Aid Systems Analyst & Programmer	Technical AG Member
Michelle Norton	California State University System-wide	Project Manager	PTP AG Member
Michele Thibodeau	Butler University	Senior Information Systems Analyst	Member HEUG Board of Directors
Phillip Curry	University of Colorado	Campus Community Application Manager, UIS	HEUG Member at Large
Candy Davies	University of North Carolina at Chapel Hill	Campus Solutions Manager	
Janene Kalb	Towson University	Information Systems Architect	
Bobbi Walker	University of Missouri	Financial Systems – Principal	PTP AG Member
Jeff Elliott	University of Missouri System	Sr. Manager, Enterprise Data Warehouse and Reporting	RBI AG Member
Joseph Goplin	North Dakota University System	Assistant Director, Financial Systems	PTP AG Member
Ellen Trantas	Bryn Mawr College	Associate Director, Development & Alumni Services	CR AG Member
Tracy Okamura	University of California, Berkeley	Director, Berkeley Financial System	GCB AG Member

[i] Oracle Patch# 26984727 “ENH:EMPLOYEE ID DELETE PROCESS”
[ii] https://docs.oracle.com/cd/E56917_01/cs9pbr4/eng/cs/lsfn/task_ApplyingDemographicDataAccessSecurity-ab5774.html#topofpage
[iii] https://www.oracle.com/assets/advanced-security-ds-12c-1898873.pdf
[iv] Oracle Support Doc ID: 2092389.1 – Oracle Applications Cloud – Data Masking Standalone Service Entitlement
[v] https://www.oracle.com/assets/advanced-security-ds-12c-1898873.pdf
[vi] Oracle Support Doc ID: 2092389.1 – Oracle Applications Cloud – Data Masking Standalone Service Entitlement