



GDPR

SOLUTION BRIEF

GDPR & PeopleSoft: Essentials for Compliance

Abstract

Aimed at protecting the data privacy of European citizens, the General Data Protection Regulation (GDPR) was put into effect on May 25, 2018 – transforming how organizations handle and manage personally identifiable information (PII).

According to a survey¹ by PWC, “GDPR compliance is a top data protection priority for 92% of US organizations”. Rightfully so, since non-compliance carries severe monetary penalties: up to €20 million or 4% of worldwide annual revenue from the prior fiscal year, whichever is higher. Given the implications, data protection has evolved from a security issue into a business issue.

GDPR gives all EU citizens the right to demand disclosure of how organizations are using their data and the “right to be forgotten.” When it comes to data management practices, organizations usually focus their resources on protecting customer information. However, GDPR requires companies to re-strategize how they use, manage and store the PII of not just customers, but employees, former employees, alumni, contractors, job applicants, vendors and business associates alike.

Your PeopleSoft applications are the core of your business. Accounting, HR, recruitment, and logistics functions house critical PII on hundreds of pages – making them a significant factor in your GDPR compliance strategy. It is crucial now more than ever that the huge amount of PII gathered across your PeopleSoft applications isn't left unmanaged and unaccounted for. Under GDPR, organizations are obligated to ensure that PII of all EU citizens (even those who are not directly associated with the company) is stored and processed lawfully.

Many organizations today are taking a reactive approach, waiting until they are affected by a threat to implement a security solution and dealing with the consequences post-breach. However, GDPR now introduces a time-stipulated breach notification requiring organizations to report a data breach to affected users within 72 hours. The ‘wait and see’ approach could result in unrecoverable penalties and preparing the notification will only complicate matters in a moment where your top priority should be remediation.

Apart from the urgent need of the hour, establishing GDPR compliance is an excellent opportunity for organizations to review and reinforce their PeopleSoft data perimeters and shift towards a proactive approach rather than waiting to be reactive.

Featured Highlights

Challenges

GDPR has highlighted the need for essential security features missing from PeopleSoft's standard functionality. Even though inherently robust and secure, out-of-the-box PeopleSoft applications are lacking some features that make GDPR compliance easy to establish and maintain.

- Current logging of user activity is limited to credentials logging-in and out. Granular user activity is not available
- Compliance audits can only be executed by triangulating multiple log files – making rapid responses nearly impossible
- Masking and redaction of sensitive PII is difficult to implement and governed by rigid rules, increasing risks for misconfiguration and exposure
- Absence of integrated analytics prevents security teams from effectively identifying and responding to breaches

Solution

Designed to control the unwanted exposure of personally identifiable information, Application Security Platform (ASP) by Apsian equips security teams with all the details they need to quickly identify and remediate breaches.

ASP extends logging capabilities to record transaction-level (user activity) data, providing organizations with the direct visibility needed for GDPR compliance in PeopleSoft. Logs are further improved through log enrichment and fed into a visualized analytics platform for real-time detection and improved response capabilities.



Important articles in GDPR and how they impact organizations leveraging PeopleSoft

Preventing breaches must be an organization's mission critical strategy for GDPR compliance. However, security teams must also be equipped with fast-tracked detection and response capabilities when a breach does occur. Backed by the experience of numerous successful PeopleSoft security projects, Apsian recommends a 3-tiered Assess, Prevent, and Detect approach for keeping your PeopleSoft systems compliant with GDPR. In the following sections, we will talk about assessing data usage, identifying avenues for preventing breaches, and detecting breaches quickly for faster response.



Assess

To ensure that your organization is prepared to respond to audits or potential breaches under GDPR, you must start with the identification and classification of sensitive data stored in your PeopleSoft applications. In the case of temporary records such as job applicants, prospective students, contractors or vendors (who may or may not end up being associated with your organization), organizations should determine which specific PII is essential for the said business function. Building a protection strategy relies heavily on a thorough assessment of your PeopleSoft systems and processes to understand what PII you already have, where that data is stored, who is using it, how often is it being accessed, and what data is minimally necessary.



Prevention

Article 32 – "...the controller, and the processor shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk..."

From GDPR's perspective, controlling the unnecessary exposure of PII can significantly reduce the likelihood of a successful breach. Since your PeopleSoft systems contain PII across multiple applications, redacting or masking sensitive data (direct deposit numbers, social security numbers, etc.) is an ideal preventive measure. To track how sensitive data is being accessed, organizations can also use checkpoints such as click-to-view data fields or multi-factor authentication (MFA). These checkpoints record transaction data on the field-level, allowing security teams to view a filtered stream of PII access logs for improved visibility, detection, and response.

Article 29 - "...processor who has access to personal data, shall not process those data except on instructions from the controller.."

Compromised credentials cause most data breaches in ERP systems. If a hacker gains access to a high-privilege account, they can easily siphon PII and valuable corporate data. A high privilege user with malicious intent can also misuse their access authority and cause a breach of personal records.

By aligning to the principal of least privilege, organizations can better control who is authorized to access sensitive information and reduce the opportunities for privilege abuse. For example: if a user logs in from an unknown network their privilege will be downgraded to default levels, limiting their access to sensitive data. Additionally, by using MFA, organizations can add an extra layer of security to reconfirm user identity when valid credentials are being used to log in from unknown/unauthorized locations, devices, etc. - thereby reducing the chances of credential misuse, especially for high-privilege users.



Detection

Article 33 - "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.."

Hackers today are getting increasingly sophisticated, and despite your best prevention efforts data breaches are inevitable. Unlike before when organizations could take their time to investigate and report breaches, GDPR requires a breach to be reported within 72 hours. However, to report a breach, organizations must fully understand it first. This means that organizations must now know the source of the breach, identify data assets impacted, and ideally be prepared with a remediation strategy – all within 72 hours.

Under GDPR, the time to respond to breaches has been greatly reduced. In the absence of real-time detection capabilities, breaches can remain undiscovered for weeks or even months (until scheduled audits) putting you in non-compliance of Article 33. Therefore, along with preventive measures, organizations must be prepared for immediate detection of breaches. By now organizations must have necessary security policies and procedures in place that promptly provide information needed to respond to a breach and to minimize, if not avoid penalties.

GDPR Challenges for PeopleSoft

PeopleSoft offers limited logging

Out of the box, PeopleSoft's default user activity logging is high-level, only recording credential activity such as login and logout attempts. PeopleSoft does not have the means to track granular user activity like what PII is being accessed or any details on who obtained it, when, or from where. With GDPR in action, data subjects can request an audit at any point in time and organizations need to be prepared to address multiple requests simultaneously. In the absence of detailed and actionable transaction logs, organizations will not be able to respond to audit requests, putting them in non-compliance of GDPR.

Lack of integrated analytics

PeopleSoft applications contain sensitive data on hundreds of pages, therefore tracking a specific event in the detailed logs can be time-consuming. Traditional security audits performed manually on excel sheets can take weeks or even months. With GDPR mandating that a data breach should be reported to affected users within 72 hours, organizations need to have instant access to real-time transaction data that helps security personnel identify, investigate, report and remediate data breaches quickly.

Lack of dynamic access and privilege controls

Access control within PeopleSoft is governed by rigid rulesets such as static user roles and permission lists. As a result, everyone in a privileged user group/permission list can access sensitive data freely no matter where they are accessing it from. To ensure the security of sensitive data, organizations need to establish dynamic access controls based on location or device, nature of data, user activity and more.



To further reduce PII exposure, PeopleSoft recently released data masking functionalities geared towards GDPR compliance. While it is a start in the right direction, the delivered masking rules cover only the basic security and compliance needs, posing certain limitations:

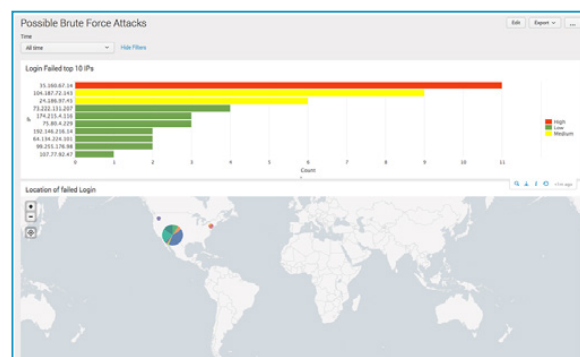
Masking/Redaction based statically on roles only. Users either cannot view sensitive information at all, or they can view all of it. One-way field masking is used. Even if a data field is masked, malicious users/hackers can still change it. Masking is implemented only at the UI-level. Queries can still be used to gain access to otherwise masked data.

Solution

Appian's Application Security Platform (ASP) addresses end-to-end PeopleSoft security and GDPR compliance needs. Equipped with multi-factor authentication, location/privilege-based access, enhanced logging, intrusion response, and integrated security analytics - ASP keeps PII secure and helps you stay compliant with GDPR.

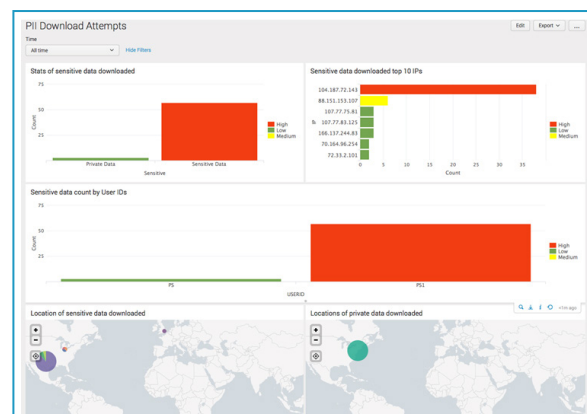
Detection

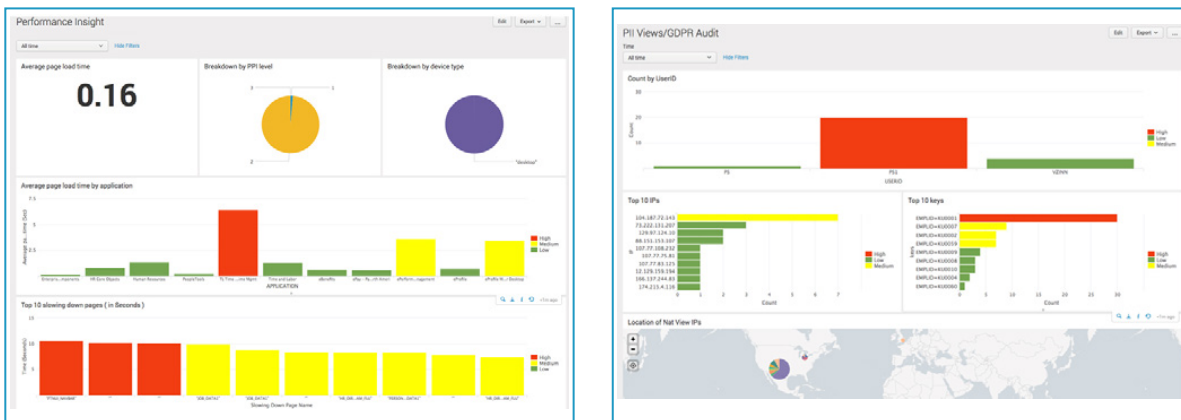
ASP's enhanced logging records all user transactions within PeopleSoft on a granular level, providing the level of detail needed to comply with GDPR, fulfill audit reporting, and to investigate and respond to breaches efficiently. ASP expands PeopleSoft's logging capabilities to capture additional field level information on what was accessed, where it was accessed from, user ids, IP addresses, pages accessed, actions performed and more – information that can be critical for GDPR compliance reporting. The additional logging data does not require additional infrastructure and can be stored within existing security information and event management systems.



Security Analytics

Appian's ASP features an analytics extension called PeopleSoft Security Analytics. While ASP records all transactions within PeopleSoft creating detailed access logs – data trends are aggregated and visualized using engaging and visually rich dashboards. Integrated analytics were always a good-to-have feature for security teams; however, keeping GDPR deadlines of breach identification and reporting in mind, they have become a must-have feature. These advanced dashboards equip security professionals with real-time snapshots of data usage. The deep drill-down capabilities allow for enhanced data discovery and exploration to expedite breach detection and response, thereby helping organizations stay GDPR ready.






Preventive security measures for controlling breaches


ASP combines user privilege, location and transaction context to provide selective data access helping companies comply with GDPR's articles that mandate restricted data access. By extending the protection of traditional perimeter security to the individual field, page, and component levels, ASP helps organizations prevent data from unwanted leakage.

Equipped with features like multi-factor authentication, single sign-on, dynamic data masking and redaction, ASP empowers organizations to improve access controls while reducing the risk of exposure as indicated in Article 32 of GDPR. Moreover, should breaches occur despite preventive measures, ASP allows organizations to detect them faster so that response, reporting and remediation tasks can be fast-tracked and their impacts (fines, legal issues etc.) can be minimized.


To establish compliance without compromising the convenience of mobility, ASP also allows location or device-based access controls. Built to integrate with your PeopleSoft environment seamlessly ASP can be deployed without making any changes to your existing underlying platform.




Single Sign-on




Multi-Factor Authentication



High Privilege access control



Location-based security



Data Masking


References

[1] <https://www.pwc.com/us/en/services/consulting/library/gdpr-readiness.html>



8111 Lyndon B Johnson Fwy. Dallas, TX 75251

© AppSIAN 2019

 (469) 906-2100

 info@appsian.com