Simplifying GDPR Compliance with Workday & Smart™

GDPR aims to increase privacy for individuals and gives regulators greater powers to take action against businesses that breach the regulation. You must comply with GDPR if:

- you collect and use personal data as part of the activities in your EU branches; and/or
- you're based outside of the EU but deliver goods and services to EU residents.

As Workday is a hub of organisational data, the arrival of GDPR means that your HR team must ensure the privacy of all data subjects they interact with, including employees, contingent workers, recruitment candidates, student workers, etc. Here's how Workday and Smart can make compliance easier.

1 Protecting privacy by design and default

GDPR requires you to put measures in place to ensure compliance with the regulation. Technical measures must be designed with privacy in mind from the outset and in ways that safeguard privacy, uphold data protection principles, and ensure that access to personal data is limited by default.

In Workday, privacy is controlled by your security configuration. You may have prevented peers from being able to see each other's personal information and managers from seeing sensitive information of staff below them—such as Social Security numbers and religious preferences. But if your configuration allows managers to see personal information of all staff beneath them in the management chain, this could be an issue from a GDPR perspective. Do they have access to more information on lower level workers than they require in order to do their job? Home contact information? Dates of birth?

How Workday Helps

- ✓ Customisation allows you to build an *n*Level security configuration, a more restricted security configuration with enhanced privacy
- ✓ Conditional rules can be applied to control data visibility based on the number of levels the data subject is below the viewing manager
- ✓ Conditional rules can be applied to control data visibility based on workers' locations

2 Proving that security controls are working

Like many regulations, GDPR requires that you be able to demonstrate your compliance measures. In addition, Article 32 takes accountability further by stipulating that you must have a process in place to regularly *test* the effectiveness of those measures. In Workday—where security groups and roles intersect, permissions aggregate, and workers hold multiple positions—sometimes even simple configuration changes can unexpectedly alter what personal information your users can see. So testing is simply good practice.

How Smart™ Helps

- ✓ Executes 1000s of security checks in minutes
- ✓ Checks field level permissions and available actions consistently and accurately every time
- ✓ Provides ongoing assurance and evidence that security settings are intact

But manually testing your Workday security is a tall order. It's a time-consuming and extremely repetitive process, making it highly prone to human error. What's more, tens of thousands of checks are required to achieve adequate breadth and depth of coverage—far more than teams can accurately carry out and document.

- ✓ Reduces risk by catching data visibility issues early, before they become problems
- ✓ Reusable tests make it easy to test weekly and demonstrate robust due diligence
- ✓ Keeps records of all tests to share with auditors and demonstrate compliance

3 Keeping non-production data private

The personal information that lives in your Workday production tenant also lives in your non-production tenants, like sandbox, and is also subject to GDPR. Non-production tenants are busy places. It's where teams carry out testing and training, try out configuration changes, and troubleshoot issues. Commonly, security in non-production tenants is more relaxed to make these tasks easier for staff to complete—meaning often staff have more access to real workers' personal data than they would as users in production.

These additional uses of and access to personal information pose GDPR compliance challenges. GDPR states that data controllers shouldn't use data for anything other than consented purposes and that only those who require access to the data to fulfill processing for the specified purposes should have access to it. Therefore, using personal information for testing, training and troubleshooting in your Workday non-production tenants could be deemed a violation of GDPR.

One solution is to scramble data in sandbox, but this has numerous limitations. It's impossible to scramble history data. It's difficult to scramble data and still maintain its integrity—for example ensuring it still adheres to your custom validation and eligibility rules. Properly scrambled data (ie, it's impossible to unscramble) makes regression testing difficult because you need to identify the correct test subjects each time you want to test.

How Smart™ Helps

- ✓ Lets you automatically create synthetic orgs in sandbox that mirror your real org structures
- ✓ Test data generator creates synthetic workers that mirror real employees using 100% fake data
- ✓ Can use synthetic data to recreate key scenarios that may not occur regularly in production data
- ✓ Restricting access to synthetic orgs with synthetic workers creates a safe zone in sandbox where teams can carry out manual testing, training and troubleshooting with zero exposure to the personal data of real workers
- ✓ Recreates synthetic workers and structures every week after refresh at the click of a button
- ✓ Reduces how often you need your SMEs to help with testing

Workday & GDPR: Reducing Risk and Data Exposure Thru Smart Automated Testing

WATCH THE WEBINAR