OrangeHRM - GDPR What you need to know?

Version 1 - February 26th 2018

Background

General Data Protection Regulation (GDPR) is in force in Europe from 25 May 2018. This is all about strengthening and unifying data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU, enforces penalties for breach and defines stronger conditions for consent.

At its heart, GDPR is about protecting the rights of individuals (think employees and job candidates). GDPR provides the following rights for individuals:
1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

GDPR not only applies to organizations based within the EU but it also applies to those that are tracking the personal data of staff located in the EU. For more background information on GDPR, please refer to the OrangeHRM white paper located at http://blog.orangehrm.com/2017/11/17/gdpr/.

GDPR Compliance Review

During 2017, OrangeHRM underwent an extensive review of it's own processes and software capabilities to determine and address our compliance with GDPR. We leveraged the approach recommended by the ICO (Internet Commissioner Office, UK), the details of which can be found at https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf, a summary of which is as follows:

1. Awareness
2. Information you hold
3. Communicating Privacy information
4. Individuals' Rights
5. Subject Access Requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data Breaches
10. Data Protection by Design and Data Protection Impact Assessments
11. Data Protection Officers
12. International

Through this exercise, we were able to validate that - for the most part - our internal processes and software were largely aligned with the GDPR requirements but we did identify some areas of improvement. In the remainder of this document, OrangeHRM will discuss GDPR compliance in the context of OrangeHRM Software, OrangeHRM Processes and OrangeHRM SaaS Service.

OrangeHRM Software

It's important to note that software is a small part of what is required for GDPR compliance - the largest part relates to the processes you use to manage personal data. For example, if you generate a report with employee personal details and store it on a shared drive that everyone can access, then you're not GDPR compliant!

From the start, OrangeHRM has provided all customers with an extensive range of data protection capabilities – from role-based access control to data encryption; from tools to publish corporate policies to data management with extensive audit logs. The capabilities provided have evolved over time so any analysis of software compliance with GDPR must consider the various generations of functionality provided, specifically:

- Customers running on software versions prior to 5.3
- Customers running on software versions between 5.3 and 6.3.7
- Customers running on software versions 6.3.8 and beyond

Versions Prior to 5.3

During 2017, OrangeHRM undertook an outreach campaign to assist all clients running on older software versions to upgrade to the most recent releases.

If you are running on versions prior to OrangeHRM Version 5.3, we recommend that you contact OrangeHRM to discuss the compliance of your system with GDPR.

OrangeHRM Version 5.3 to Version 6.3.7

If you're running on OrangeHRM between Version 5.3 and 6.3.7, you're nearly there! There are a couple of specific issues which are addressed after these versions which will require you to upgrade at some point in time, namely:

- When an employee is deleted from OrangeHRM (after the statutory period of time that you must keep their employment records), a footprint of their data remains in the OrangeHRM database. This impacts the long-term right of an employee to be forgotten. A new feature was introduced in 6.3.8 to fully purge personal information related to ex-employees from the OrangeHRM database.
- If you are using the OrangeHRM recruitment module, when a candidate is unsuccessful in the recruitment process and is deleted from OrangeHRM, a footprint of their data remains in the OrangeHRM database. This impacts the right of a candidate to be forgotten. A new feature was introduced in 6.3.8 to fully purge personal information related to a candidate in the recruitment process from the OrangeHRM database.

OrangeHRM Version 6.3.8 and Beyond

If you're running on OrangeHRM Version 6.3.8 and beyond, you're currently running on a version that provides you the right software capabilities for GDPR compliance. Specific capabilities include:

- Newly introduced maintenance section in the Admin module will allow you to purge terminated employees and candidates from the entire system including audit trails.
- Job application consent where you can outline your data policy and require an explicit check in the checkbox before allowing a candidate to apply.

There are certain assumptions and decisions made while introducing these features that are important to understand. Our main goal was to maintain the right balance between the integrity of the product and compliance with data protection. The following table summarises the assumptions which were made.

#	Module	Exception
1	Admin	Audit log records related to changes to the employee salary performed prior to Version 6.3.4 are not purged from the audit log as they are not directly traceable back to their employee record.
2	Audit Trail	If an ex-employee has been nominated to provide leave absence cover for another employee, the audit log record will continue to reference the ex-employee name but will not be directly traceable back to their employee record.
3	Time	Ex-Employee time sheets are not purged in order to preserve project reporting. Instead, the employee name is no longer available and the record refers to the original job title of the ex-employee.
4	Time	Audit log records outlining the name of project admins for each project are not purged for ex-employees who were project admins as they are not directly traceable back to their employee record.
5	Recruitment	Vacancy records outlining the name of the hiring manager is not purged for ex-employees who were project admins as they are not directly traceable back to their employee record.
6	Recruitment	Audit log records outlining the name of hiring managers and stage coordinators for each vacancy are not purged for ex-employees as they are not directly traceable back to their employee record.
7	Performance	Appraisals of active staff conducted by ex-employees are not purged as the data is required for active staff. It's possible that these records could contain text identifying the ex-employee. The employee name on the appraisal itself is no longer available and the record refers to the original job title of the ex-employee.
8	Performance	This is only applicable for clients using e-signed documents for appraisals (e-signed providers Slinais and DocuSign). These documents must be manually removed for ex-employees, either by login onto the portal and delete or by contacting OrangeHRM.
9	Time	Email addresses for notifications must be manually removed for ex-employees as this is not done automatically when an employee is purged. This applies to

		all email notifications including those in the Travel & Expense module.
10	System	A system error or crash may result in the operating system or application writing personal data to log files that are stored in an unencrypted format on the server. In general, OrangeHRM mandates that system directories used by the OrangeHRM software are protected from access by non-trusted staff.

OrangeHRM Processes

As part of the normal day-to-day activities at OrangeHRM, some staff may be required to access personal information. As a part of GDPR, we have assessed all such needs and performed specific actions, introduced new processes and implemented technological solutions to securely manage personal information.

Below are the actions, processes and technological enhancements:

- We have purged any historical personal information accidentally sent through unofficial channels, This contains data sheets sent by clients to OrangeHRM via emails, ticketing system or insecure file transfers.
- A new process is in place to securely transfer data files from clients to OrangeHRM.We do not accept any unprotected data files through any unofficial channels such as email, Skype. We have introduced OrangeHRM Vault, a secure file transfer portal where clients can directly upload password protected data files. Only authorized consultants will have access to these files through OrangeHRM Vault. OrangeHRM Vault will automatically validate these files for their security and it will periodically purge these files from the storage.
- OrangeHRM Implementation consultants need access to the data CSV files during the implementation phase. It's required to immediately delete these files from their system once they successfully complete data transfer to OrangeHRM client's instance.
- Copying of client's production data outside the OrangeHRM secure network is prevented by enforcing the necessary policies and rules in the server environment. If trouble-shooting on the production system is required, we have implemented automated tools to provide masked replicas of databases. Masking will make sure all personal information is obfuscated before it copied to a test environment.
- No other users apart from designated support engineers within the OrangeHRM Customer Success department are allowed to access a hosted production system. Only a defined set of administrators have administrative access to OrangeHRM production servers, These are controlled by introducing validation rules in the server environment.

In addition we are in the process of certifying OrangeHRM with ISO 27001, which is a specification for an information security management.

OrangeHRM SaaS Service

OrangeHRM SaaS infrastructure is managed by Rackspace. They maintain various certifications to assist us in verifying the security policies, processes and facilitate for GDPR. Rackspace been assessed and hold validation for the following compliance frameworks.

- **ISO 27001** - Rackspace ISO 27001 certified Information Security Management System (ISMS) is an iterative management system that helps ensure security policies and processes are effective in mitigating identified risks. ISMS at Rackspace certifies the management of information security in the operations of their data center facilities.
- **SSAE 16 and ISAE 3402** (Previously SAS 70 Type II) - Rackspace type II to SOC report can be used to satisfy requirements under both the SSAE 16 and ISAE 3402 standards. This report contains a description of the controls in place and the auditors informed opinion of how effective the controls were during the audit period.
- **PCI DSS** - A qualified security assessor(QSA) validates Rackspace being a PCI DSS Level 1 service provider. It covers.
    - Physical security for data centers.
    - Network infrastructure
    - Rackspace employee access to network devices.

In addition OrangeHRM conducts biannual audits on all the production servers to make sure they are aligned with OrangeHRM corporate security standards.