OrangeHRM Service Privacy Policy

(***Revision December 2023***)

This Service Privacy Policy covers the privacy practices employed by OrangeHRM when OrangeHRM customers ("Customer", "You") use our Cloud-Based Enterprise Applications (the "Cloud Service") or On-Premise Enterprise applications (the "On-Premise Service") or both ("Cloud Service and On-Premise Service", "Service"). This Privacy Policy does not apply to any information or data obtained by OrangeHRM for any other purpose, such as marketing purposes. **Please refer to the OrangeHRM Privacy Policy**

Who We Are

When we use the terms "OrangeHRM", or "us" or "we" in this policy, we are referring to OrangeHRM Inc.

Data Protection Officer

Our Data Protection Officer oversees how we collect, use, distribute, and secure your information to ensure your rights are respected. Our Data Protection Officer can be contacted at dpo@orangehrm.com

How we collect information

In the normal course of using the OrangeHRM Cloud or On-Premise Service, Customers will enter electronic data into the OrangeHRM systems ("Customer Data").

Customers may input Customer Data into data templates and submit these to OrangeHRM through secure channels. OrangeHRM Implementation consultants will assist with the import of such data into the OrangeHRM Cloud or On-Premise Service.

What Information Do We Collect

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the categories of Personal Data listed below based on the OrangeHRM modules purchased:

- PIM: Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses. Date of birth, Gender, Marital status and dependants, emergency contact information, National Insurance/Social Security number, Bank account details, payroll records and tax status information, Salary, annual leave, pension and benefits information, Location of employment or workplace, driving license, Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the

application process), Employment records (including job titles, work history, working hours, training records and professional memberships), Photographs.

- Performance: Employee performance information such as performance reviews and ratings
- Leave: Employee leave information such as type of leave, medical reports included as attachments.
- Time and Attendance: Employee attendance information (Punch In/Out, Attendance reports, working hours)
- Travel & Expense: Copies of expense receipts
- Recruitment: Candidates Resume and their personal information such as name, address, telephone number, mobile number, email address
- Disciplinary: Employee disciplinary information, such as warning letters.
- Any other information applicable to candidates, workers, contractors, and employees.

How we keep your information safe

We have a comprehensive, written information security program in place that includes industry-standard, administrative, technical, and physical safeguards to protect Customer Data from unauthorized access.

Our infrastructure service providers are Rackspace Inc and Amazon Web Services, Inc. They maintain various certifications that help us validate our security policies and processes as well as comply with applicable legislation such as GDPR and international standards. If you want to know more about OrangeHRM GDPR Compliant please refer to this. The following compliance frameworks have been examined and validated :

OrangeHRM Advanced Cloud Service

Our infrastructure service provider is Rackspace Inc.

- **ISO 27001** - Rackspace Information Security Management System (ISMS) with ISO 27001 is an iterative management system that ensures security policies and processes are effective in mitigating identified risks. Rackspace's ISMS validates the management of information security in its data centre operations.
- **SSAE 18 and ISAE 3402** - Rackspace SOC (1,2,3) reports can be used to satisfy requirements under both the SSAE 18 and ISAE 3402 standards. This report includes a description of the controls in place as well as the auditor's informed assessment of their effectiveness throughout the audit period.
- **PCI DSS** - Rackspace's status as a PCI DSS Level 1 service provider has been verified by a qualified security assessor (QSA). It covers.
    - Physical security for data centres.

- Network Infrastructure
- Rackspace employee access to network devices.

OrangeHRM Open Source Cloud Service

Our infrastructure service provider is Amazon Web Services, Inc.

- **ISO 27001** - AWS ISO/IEC 27001:2013 is a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) outlining how AWS consistently oversees security comprehensively and holistically.
- **SSAE 18 and ISAE 3402** - AWS offers a SOC 1 Type 2 report, which aligns with SSAE 18 and ISAE 3402 standards. This report is valuable for various audit requirements, both within the United States and internationally. It confirms that AWS has appropriately designed control objectives and that the specific measures in place to protect customer data are functioning effectively.
- **PCI DSS** - AWS has obtained validation through AWS Security Assurance Services LLC, a team of Qualified Security Assessors (QSAs) certified to provide guidance and assessments for PCI DSS compliance. AWS successfully completed a Level 1 assessment as a Service Provider in line with PCI DSS requirements.

For the On-Premise Service and the cloud service, we may temporarily retain customer-submitted data templates containing customer data in the OrangeHRM secure facility, until Customer data is successfully imported into the on-premise and cloud Services. **OrangeHRM Vault** is a secure file transfer platform where customers can submit password-protected data files directly. Only authorized consultants will have access to these files through OrangeHRM Vault. OrangeHRM Vault will automatically validate these files for security and remove them from storage regularly.

Your personal information rights

We process customer data at the request of our customers and do not have direct control or ownership of the personal data processed by the system. Prior to sending data to OrangeHRM for processing purposes, you are responsible for complying with any regulations or laws that require you to provide notice, disclosure, and/or obtain consent.

We offer a comprehensive set of data protection capabilities ranging from role-based access control to data encryption; from corporate policy publishing tools to data management with extensive audit logs. It enables Customers to gain access to, correct, and limit the processing of their personal data.

New capabilities in OrangeHRM software version 6.4 upwards allow you to purge terminated employees and candidates from the entire system including audit trails. This is to help you to practice data subject requests such as the right to be forgotten.

If you are using the Recruitment module, you can now obtain job application consent by laying out your data policy and requiring a check in the checkbox before allowing a candidate to apply for a vacancy.

Any data subject request that is directed to us will be forwarded to the customer and we will assist the customer in meeting any obligation to respond to such data subject requests. If the customer requests help from OrangeHRM to comply with data protection regulations, OrangeHRM will respond to their request within 30 business days.

Data retention period

In the OrangeHRM Cloud Service, if you have a valid SAAS agreement with OrangeHRM, your data will be retained in our servers. Should you purge any specific employee or candidate records, this data will be immediately purged from the system. Such information will then be completely removed from OrangeHRM backups after 4 weeks.
Between 10 and 30 days after the agreement between OrangeHRM and the Customer is terminated, OrangeHRM will remove the customer personal data from the OrangeHRM servers and all customer personal data will be fully purged from OrangeHRM backups after a further 4 weeks.
For On-Premise service, we will ensure that any temporary data such as customer data templates, is purged between 10 and 30 days after the termination of the agreement between OrangeHRM and the Customer.

Note:
Under OrangeHRM standard agreements, the aforementioned data retention periods will be valid. Customers who have subscribed to OrangeHRM extended services will have their data retained for longer than the above-mentioned periods (can go up to 12 weeks).

Meeting our legal and regulatory obligations

OrangeHRM may, where it concludes that it is legally obligated to do so, disclose personal data to law enforcement or other government authorities. OrangeHRM will notify customers of such requests unless prohibited by law.

Consent

Prior to using sensitive personal information about you for any service improvements, we will first request your consent. Before you give your consent, we tell you what information we collect and how we use it. You have the right to withdraw your consent at any time by contacting us.

How we use your information

Per the relevant agreement between the Customer and OrangeHRM, we may access customer data within OrangeHRM to provide the service, prevent or address service or technical problems, respond to support issues, respond to the customer's instructions, or as may be required by law.

We may process anonymized data to troubleshoot customer-specific issues and for quality control purposes.

We may process anonymized data to track how the Service's various components are used. This information is used to drive feature development and service enhancements as well as to provide recommendations on how our products and services can add value for you. OrangeHRM does not sell your information to any party under any circumstances and OrangeHRM is not responsible for any PII data sold by the data controller.

How you access the OrangeHRM Service

Customers and their authorized users may access the Service directly via a URL that is unique to their tenant or may elect to use internal launch pages for single sign-on or other purposes. As they utilize the service, customers provide information for processing and storage. Customers may also configure the Service to allow end users to input information directly into the Service

Your information and third parties (Sub-processors)

To comply with applicable laws, regulations or authorized requests, we may share your information with third parties. We will notify you of such incidents unless prohibited by law.

Sub-processors processing personal data as part of the Services

Company	Location of Data	Purpose of Data Processing	Type of data collected
Rackspace	EU and US	Data hosting provider	End user's data and Customer's data

Amazon Web Services, Inc	UK	Data hosting provider	End user's data and Customer's data
Twilio Inc. Sendgrid	United States	cloud-based email delivery service	End user's data and Customer's data
OrangeHRM Software (Pvt) Ltd	Sri Lanka	technical support for the operation of the SaaS service	End user's data and Customer's data
Celigo Inc.,	USA, India and the Netherlands	IPAAS platform to integrate third-party applications with OrangeHRM	End user's data and Customer's data
Microsoft Power BI	EU	Business analytics service	End user's data and Customer's data
Zoho	US	A ticketing system to track support tickets	End user's data and Customer's data

International Transfer of data

In Cloud Service, we store customer data in the nearest data centre used by OrangeHRM to provide your specific service, Eg: European client data is stored in European Economic Area data centers. This will ensure your rights are protected.

In Cloud Service and On-Premises Service, we may transfer anonymized data from European region Data Centers to North American Rackspace Data Centers and Asian technical support centers for the purposes of providing the Service, preventing or addressing service or technical problems, responding to support issues, and responding to the Customer’s instructions.

Right to fair treatment

OrangeHRM will not discriminate against you for exercising your privacy rights. Regardless of your privacy preferences, OrangeHRM will provide the products and services you require.

Making a Complaint

If you have a complaint about the use of your personal information, please contact your application admin within the organization. If you have a complaint about the OrangeHRM service privacy policy or security, please contact our DPO at dpo@orangehrm.com.

Updates to this notice

We may update this privacy statement to reflect changes in our information practices. If we make any material changes, we will notify you by means of a notice on this site prior to the change taking effect. We encourage you to periodically review this page for the latest information on our privacy standards.