OrangeHRM Service Privacy Policy

(***Revision November 2020***)

This Service Privacy Policy covers the privacy practices OrangeHRM employs 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 cover any information or data collected by OrangeHRM for other purposes, such as information collected for marketing purposes. **Please refer to the OrangeHRM Privacy Policy**

Who We are

When we talk about “OrangeHRM”, or “us” or “we” in this policy, we are talking about OrangeHRM Inc.

Data Protection Officer

Our Data Protection Officer oversees how we collect, use, share and protect your information to ensure your rights are fulfilled. You can contact our Data Protection Officer at dpo@orangehrm.com

How we collect information about you

In the normal course of using the OrangeHRM Cloud Service and On-Premise Service, Customers will input electronic data into the OrangeHRM systems (“Customer Data”).

Customers may input Customer Data into data templates and submit to OrangeHRM through secure channels. OrangeHRM Implementation consultants will assist to import such data into OrangeHRM Cloud Service 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 following categories of Personal Data based on the OrangeHRM modules:

- 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 licence, 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: Employe performance information such as performance reviews, ratings
- Leave: Employee leave information such as type of leave, medical reports as attachment.
- Time and Attendance: Employee attendance information (Punch In/Out, Attendance report, 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 maintain a comprehensive, written information security program that contains industry standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Data.

For OrangeHRM Cloud Service, Our infrastructure service provider is Rackspace Inc, They maintain various certifications to assist us in verifying the security policies, processes and facilitate applicable laws such as GDPR and international standards. Rackspace has 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 On-Premise Service, We may temporarily store customer submitted data templates with customer data in the OrangeHRM secure facility, until Customer data is imported into On-Premise Service. We have introduced **OrangeHRM Vault**, a secure file transfer portal where the customer 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.

Your personal information rights

We process Customer Data under the direction of its Customers and has no direct control or ownership of the personal data it processes. You are responsible for complying with any regulations or laws that require providing notice, disclosure and/or obtaining consent prior to transferring the data to OrangeHRM for processing purposes.

We provide 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, It enables Customer to access, rectify and restrict processing of Customer Data.

New functionalities in OrangeHRM software version 6.4 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, it now allows you to obtain job application consent - where you can outline your data policy and require an explicit check in the checkbox before allowing a candidate to apply.

Any data subject request directed to us will be directed to the customer and we will assist the customer in fulfilling any obligation to respond to requests by data subjects. If the customer requests OrangeHRM assistance to comply with data protection regulations, OrangeHRM will respond to their request within 30 business days.

How long we keep your information

In Cloud Service, As far as you have a valid SAAS agreement with OrangeHRM, Your data will be retained in our servers, If you purge any specific employee or candidate record, it will be immediately purged from your service. Such information will be completely removed from OrangeHRM backups after 4 weeks.
Between 10 and 30 days of the termination of the agreement between OrangeHRM and the Customer, 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 subsequent 4 weeks.
In On-Premise service, we will make sure any temporary data such as customer data templates, will be purged between 10 and 30 days of the termination of the agreement between OrangeHRM and the Customer.

Note:
Aforementioned data retention periods will be valid under OrangeHRM standard agreements. The data retention period of a customer, who has subscribed to OrangeHRM extended services will be deviated from 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

When we use sensitive personal information about you for any service enhancement, we ask for your consent. Before you give your consent, we tell you what information we collect and what we use it for. You can remove your consent at any time by contacting us.

How we use your information

We may access customer data within OrangeHRM for the purposes of providing the service, preventing or addressing service or technical problems, responding to support issues, responding to the customer's instructions or as may be required by law, in accordance with the relevant agreement between the Customer and OrangeHRM.

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

We may process anonymized data to track the usage of different components of the Service. These are used to influence feature development and service enhancements and recommend how our product and services are suitable for you. Further OrangeHRM does not sell your information to any party by any means and OrangeHRM does not hold any responsibility on PII data sold by the data controller.

How you access OrangeHRM Service

Customers and their authorized users may access the Service directly through a URL unique to their individual tenant or may elect to use internal launch pages for single sign-on or other purposes. Customers input information for processing and storage as they use the Service. Customers may also configure the Service to allow end users to input information directly into the Service

Your information and third parties

Sometimes we may share your information with third parties to meet any applicable law, regulation or lawful request. We will notify you of such incidents unless prohibited by law.

In Cloud Service, Customer data is stored in Rackspace data centers and Rackspace Inc. has subprocessor contract agreements with OrangeHRM.

In Cloud Service, All service notifications (Eg: Leave notifications) are sent through SendGrid and Mandrill transactional email services.

International Transfer of data

In Cloud Service, We store customer data within the same business region, Eg: European clients data are stored within 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 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, responding to the Customer's instructions.

Right to fair treatment

OrangeHRM will not discriminate against you for exercising any of your privacy rights. Irrespective of your standing on your privacy preferences, OrangeHRM will provide the product and services.

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 through dpo@orangehrm.com.

Updates to this notice

We may update this privacy statement to reflect changes to its information practices. If We make any material changes, We will notify by means of a notice on this site prior to the change

becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.