



## HR module and GDPR

### Overview

The HR Module within Claromentis is designed to follow GDPR (The General Data Protection Regulation). GDPR is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It's all about protecting and respecting the privacy of personal data, in this case, employee files and data.

### HR Passcode

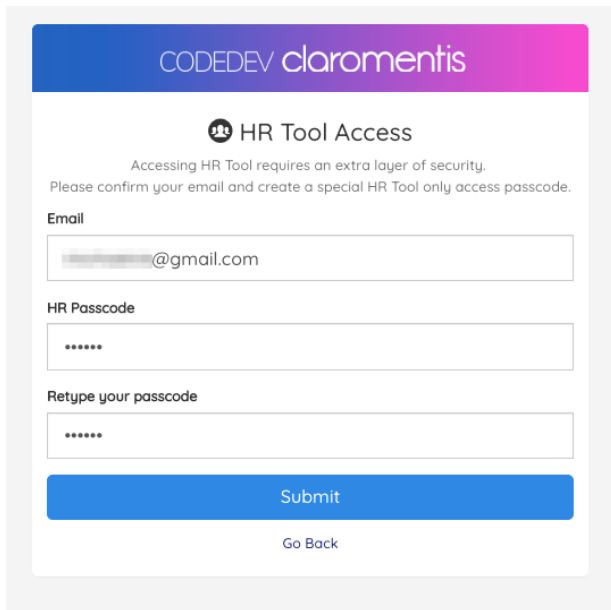
Access to HR sensitive data is protected by a **Passcode** in addition to the regular sign-in process. Please note that you can also have Two-factor authentication enabled for added security to the regular sign-in process.

A screenshot of a web login interface. At the top is a blue and pink gradient header with the text 'CODEDEV claromentis'. Below the header is a user profile section with a small circular photo of a man, the text 'Hi, Michael Christian', and 'To continue, first verify it's you' followed by the email 'michael.christian@claromentis.com'. Underneath is a section titled 'HR Passcode' with a text input field containing a key icon. Below the input field is a blue button labeled 'Sign in to HR'. At the bottom are two links: 'Forgotten passcode?' and 'Go Back'.

A user will be prompted to set up a HR Passcode upon their first login to the HR system.

# Recovery Email

When setting up an HR account for the first time, it is possible for a user to use choose a different email address such as personal email for HR-related recovery passcode. This is to ensure that your personal data is within the user's control and cannot be accessed by IT department personnel who may have access to employee's work email.



The screenshot shows a web form titled "CODEDEV claromentis" with a sub-header "HR Tool Access". Below the title, it states: "Accessing HR Tool requires an extra layer of security. Please confirm your email and create a special HR Tool only access passcode." The form contains three input fields: "Email" (with a placeholder "@gmail.com"), "HR Passcode" (with a masked input "\*\*\*\*\*"), and "Retype your passcode" (with a masked input "\*\*\*\*\*"). At the bottom, there is a blue "Submit" button and a "Go Back" link.

# Time Out

Upon 10 minutes of inactivity within HR application (on both admin and front-end application), users will be automatically logged out of HR

# Database Encryption



HR sensitive SQL database is encrypted using **AES-256 public key encryption**, It's considered among the top cyphers, meaning in the event of a database leak, sensitive HR data is protected.

# HR Files & Document

HR Files and documents are also encrypted prior storing them to the server using RC4 Encryption for added security meaning users with access to the server won't be able to download and read the file on the server directly.

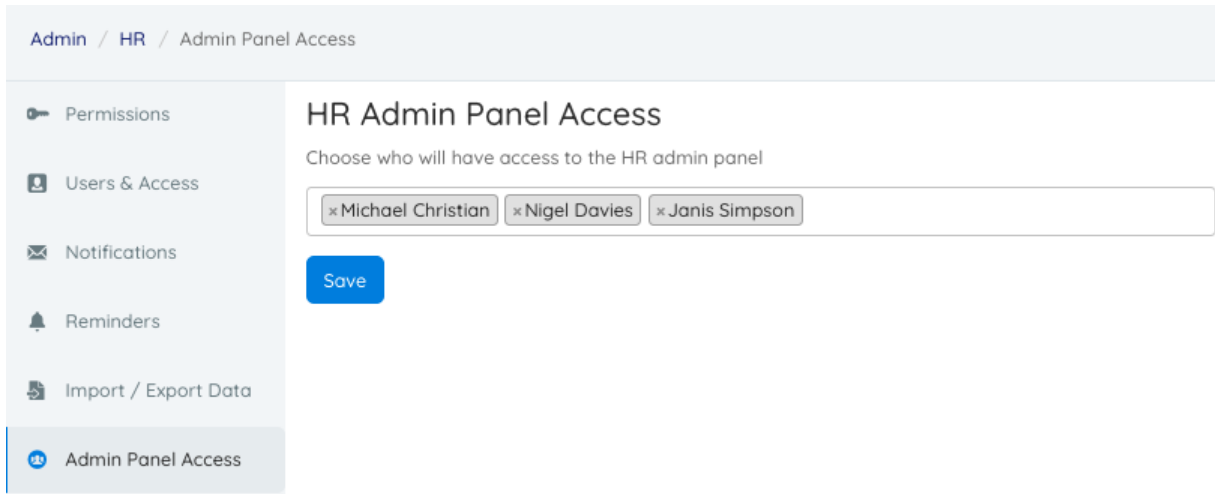
**Note:** We are aware that there are some reports of vulnerability related to RC4 Encryption and we

are currently working on to improve or change it in the near future. It is worth noting that the impact in our use case would be fairly minimal as it is used to provide an extra security level relevant to on-premise deployment.

## HR Special Admin

Users with access to the system admin panel do not necessarily have access to HR Admin. It is part of the onboarding process to nominate two users who wish to be granted access to the HR Admin panel.

Minimum 2 admins are required.



The screenshot shows a web interface for configuring HR Admin Panel Access. At the top, there is a breadcrumb trail: Admin / HR / Admin Panel Access. On the left, a sidebar menu contains several options: Permissions, Users & Access, Notifications, Reminders, Import / Export Data, and Admin Panel Access (which is currently selected). The main content area is titled 'HR Admin Panel Access' and includes the instruction 'Choose who will have access to the HR admin panel'. Below this, there is a search bar containing three user names: Michael Christian, Nigel Davies, and Janis Simpson. A blue 'Save' button is positioned below the search bar.

## Data Retention

To protect user's data after their employment has ended, it is possible to set a disposal schedule of HR Data. For example, HR Records will be permanently destroyed after 5 years from the employment end date. This information is also displayed to the users for complete transparency.



The screenshot shows a configuration box for HR data retention. The text reads: 'HR records will be destroyed permanently after 5 years from employment end date'. The number '5' is entered in a small input field. To the right of the text is an 'Edit' button.

## Audit Log

Activity within HR is fully audited within Clarentis Audit system allowing all activity to be tracked for compliance purposes.

From    To

User name

Category

CSV delimiter  Comma (,)  Semicolon

- ✓ All items
- Change administrators
- Benefit types
- Document types
- Password created
- Request password reset
- Password reset
- Notifications
- Reminders
- Custom Fields
- Users Access

| Date/Time | User name | Impersonated user | IP address<br>Proxy IP | Subcategory | Obj |
|-----------|-----------|-------------------|------------------------|-------------|-----|
|-----------|-----------|-------------------|------------------------|-------------|-----|

## HR Training & Awareness

It is possible to create an E-learning course within the learning management system to make sure your employees are aware of GDPR and Data Protection.

Learning Management System

## HR Policies

Using the policy manager within Claromentis to share and distribute HR policies.

Policy Manager Overview

---

Last modified on 30 November 2023 by Hannah Door

Created on 30 July 2019 by Michael Christian

Tags: hr, gdpr, tool