Security

Last Updated: May 20, 2020

Customer trust is essential. We always strive to manage your personal information with integrity and respect, and recognize that protecting your information must be our top priority. Please let us know if you have any questions after reading this, or encounter any issues.

How does Eddy protect data?

- User credentials are securely stored and are not reversible (hashed and salted).
- Eddy utilizes HTTPS for all data transfer.
- All Eddy databases are encrypted at rest.
- Eddy uses additional field-level encryption for highly sensitive data (e.g., social security numbers).
- Eddy users can control employee data access via roles & permissions.
- Eddy customer support tasks are restricted to trained personnel.
- Payment and credit card data is PCI compliant.

Where and how is the data stored?

Payment and credit card data is stored via Stripe. Stripe has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. Learn more at https://stripe.com/docs/security/stripe.

All other Eddy customer data is stored in highly secure AWS data centers. These centers are ISO 27001 certified. The AWS data centers and network architecture are built to meet the requirements of the most security-sensitive organizations. Eddy's AWS instances and data are located in the USA. For more information please see Amazon white papers on security: https://aws.amazon.com/whitepapers.

Who can access the data?

You and your employees have access to your data, based on the roles and permissions you establish for each user. Each user must login to view any information. You can control who has access and what level of access is given to any employee.

Our Customer Support staff will only access your data with your permission and at your request. Only employees who are trained and authorized can access the data.

Is the data backed up?

All Eddy data is backed up at least daily.

Organizational Measures Eddy Has Taken To Protect Your Privacy

The following list outlines measures that Eddy (along with its sub processors) have taken to protect your privacy when processing Personal Data.

- Unauthorized persons are prevented from gaining physical access to our premises and the rooms where data processing systems are located.
- Employees are only allowed access to tasks assigned to them.
- We use video surveillance and alarm devices with reference to access areas.
- Personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times.
- We ensure that all computers processing personal data (including computers with remote access) are password protected, both after booting up and when left, even for a short period.
- We assign individual user passwords for authentication.
- We only grant system access to our authorised personnel and strictly limit their access to applications required for those personnel to fulfill their specific responsibilities.
- We have implemented a password policy that prohibits the sharing of passwords, outlines procedures to follow after disclosure of a password, and requires that passwords be changed regularly.
- We ensure that passwords are always stored in encrypted form.
- We have adopted procedures to deactivate user accounts when an employee, agent, or administrator leaves Eddy HR or moves to another responsibility within the company.
- We prevent the installation and use of unauthorized hardware and software in our premises.
- Except as necessary for the provision of the Services, Your Personal Data cannot be read, copied, modified or removed without authorization during transfer or storage.
- We encrypt data during any transmission.
- We process the personal data received from different clients so that in each step of the processing the Controller can be identified and so that data is always physically or logically separated.
- We create back-up copies stored in protected environments.
- We have created business recovery strategies.
- We do not use personal data for any purpose other than what we have been contracted to perform.
- We do not remove Your Personal Data from our business computers or premises for any reason (unless you have specifically authorised such removal for business purposes).

- We ensure that each computer system runs a current anti-virus solution.
- We have designated a responsible person to perform the functions of a data protection officer.
- We regularly train our staff on data privacy and data security.

How you can do your part

It is also important for you to guard against unauthorized access to your personal information by maintaining strong passwords and protecting against the unauthorized use of your own computer or device. You can control the safety of your password. Here are some important things to keep in mind:

- We will never ask you to disclose your password to us or anyone else, and you should not share it with anyone.
- We recommend that you change your password periodically.
- A strong password contains a mix of numbers, letters, and symbols and is only used for this account
- Always log out of Eddy when you use a computer you share with other people.