3141 Commerce Parkway
Miramar, Fl 33025, USA
1-888-783-1493
www.easyclocking.com

EasyClocking's GDPR Commitment

Our Commitment to You and Protection of Your Data

We're committed to helping EasyClocking customers and users understand, and where applicable, comply with the General Data Protection Regulation (GDPR). The GDPR is the most comprehensive EU data privacy law in decades and went into effect on May 25, 2018.

Besides strengthening and standardizing user data privacy across the EU nations, it introduces new or additional obligations on all organizations that handle EU citizens' personal data, regardless of where the organizations are located. On this page, we explain how we help our customers comply with the GDPR.

GDPR Compliance

The GDPR's updated requirements are significant and our global team has adapted EasyClocking's product offerings, operations and contractual commitments to help customers comply with the regulation. Measures we have implemented include:

- Investments in our security infrastructure and certifications
- Updates to relevant contractual terms
- Maintaining EU area customer provisioning, management and support to EU partners.
- Offering data portability and data management tools including:
    - Import and Export Tools.
      Businesses and organizations may access, import, and export their Customer Data using EasyClocking's tools. The details are provided in the help center that can be accessed from the software.
    - User Profile Management
      Help customers respond to user requests to manage including delete personal information, such as names and email addresses, from an EasyClocking account.
    - Access Privileges and Settings
      See your access privileges and settings or contact an admin who controls these settings.

- API Access
  Businesses and organizations may access their customer data using EasyClocking API that is enabled as a module by request from the respective businesses authorized user. API access is restricted by credentials and security tokens to ensure data privacy and protection. The details can be found at https://easylink.easyclocking.net/docs/index

We also monitor the guidance around GDPR compliance from privacy-related regulatory bodies and update our product features and contractual commitments accordingly. We'll provide you with regular updates so that you're always current.

Security Infrastructure and Certifications

Protecting our customers' information and their users' privacy is extremely important to us. As a cloud-based company entrusted with some of our customers' most valuable data, we've set high standards for security. We have the following certifications and compliances for our data storage, protection and hosting:
- SAS 70
- SSAE 16 Type II SOC 1, SOC2, and SOC3 Examinations
- HIPAA Compliance
- PCI Compliance

EasyClocking has invested heavily in building a robust security team, one that can handle a variety of issues — everything from threat detection to building new tools. In accordance with GDPR requirements around security incident notifications, EasyClocking will continue to meet its obligations and offer contractual assurances.

If you'd like to learn more about EasyClocking's information security policies and procedures, please request a copy of our Information Security Policy

Information and Data Security

Purpose

The purpose of this Information Security Policy is to:

1. Protect the integrity and validity of the company data
2. Assure the security and protection of sensitive information in the company's custody.
3. Provide policies, guidelines and procedures to manage and control information considered sensitive and/or confidential
4. Prescribe mechanisms which will help identify and prevent the compromise of information security and misuse of customer data, software application, internal applications including third party software, networks and computer systems.

Scope

The policy covers all data and information in company's custody including, but not limited to operational, financial, product related, customer and customer-user related that EasyClocking computer systems and software applications maintains, processes, or distributes that are deemed sensitive and confidential.

Roles and Responsibilities

Team Lead/Managers

These individuals shall be responsible for oversight of the employees' authorized use and access to the data in their area of supervision. They will:

- Ensure the employees' access to the various data is appropriate for the duties performed.
- Ensure that the management and control of risks outlined in this policy are adhered to by employees in their unit.
- Identify the data access needs of the team members and ensure they receive adequate training to perform the duties.
- Provide employees with approved resources and methods to handle the data they need to perform their duties.
- Regularly review employee access to the various information they seek and bring up any concerns to the Information Office.
- Operate as information security monitors in their departments.
- Be the primary point of contact for the team for suspected or actual data breaches and report the information to the Information Office.

Information and Infrastructure Department

- Assist in identifying internal and external risks to security and confidentiality of the information collected and managed by the company.
- Provide guidance in data handling with utmost importance to information security.
- Promote and encourage good security procedures and practices
- Develop and maintain security policies, plans, procedures, strategies and best practices in-regards-to internal systems, network infrastructure, external interfaces, and software products.
- Review equipment including servers, network components, storage devices periodically for security updates and policy adherence.

- Develop and provide information security training.
- Evaluate the effectiveness of the current safeguards for controlling risks to the security of the information the company handles.
- Provide recommendations for revisions of this policy as appropriate.
- Perform random audits of departments and individuals as deemed necessary.
- Identify and implement new security processes and standards as necessary.
- Responsible for immediate response to any breach of security.

Employees

- Shall not disclose confidential data to unauthorized individuals and entities.
- Shall only access customer or customer-user data to serve a service or support need of the client.
- Shall not modify or delete data unless authorized to do so.

Policy

Information Confidentiality and Privacy

All employees who are users of information for the need of conducting their work, are expected to respect the confidentiality of the information they access. Users are responsible for maintaining the confidentiality of the data they access or use and the consequences of any breach.

Software Application and Data Security

Introduction
The systems and the architecture help maintain the data security and confidentiality of the customer data that are deemed sensitive. However, the various company personnel that handles the customer information for the purposes of setting up or servicing the customers is expected to not only respect the confidentiality of the information they handle, but also use the information for only the purpose of what they are authorized to do at the time of such help or service is rendered.

Support and Service
The service personnel who handles the customer information for the purposes of helping the customer should log the event as a service ticket and all details of the event should be logged as activity done during the service. Any breach of confidential data will be the responsibility of the

service personnel. It is imperative that any suspicion of breach or possible breach, should be brought to the attention of the Director, Information and Infrastructure.

Cancellation
In the event the customer cancels the service with EasyClocking, the license must be cancelled with immediate effect so that the system and data is inaccessible from the outside. If the customer requests destruction of data upon cancellation, such request must be provided in writing. The customer data is archived after one year of cancellation and non-use.

Device Data Security

Device data is encrypted at rest and in transfer. Any returned device should be factory reset to clear the data before any repurposing is done to it. The data on a device that is remotely connected by a service personnel when requested by the customer, should be considered confidential and handled as such. The service personnel are required to log the events in a support ticket created for the purpose and detail the activities performed during the time.

Client Data Security

Apart from the data that belongs to the users of the company who is a client of EasyClocking, EasyClocking also maintains data about the client for operational and financial purposes. This data remains in the internal systems of EasyClocking and are deemed sensitive and confidential. The client data is not permitted to be shared with any external entity except for the purposes of conducting day-to-day operations to which the client is privy to. The handlers of such data need to respect the client's privacy and need to handle the data maintaining the confidentiality of the client.

Access Control

Logical Access

- All employees must have their own username and use a strong password. The sharing of the usernames and passwords are not allowed.
- The password of empowered users, such as system administrators must be changed every 120 days.
- Password used in EasyClocking's computer systems must not be the same password they use for personal accounts such as banks, personal email etc.

- Passwords must not be common words and must contain numbers and special characters.
- Password must not be placed in emails and chats.
- Passwords must not be written down in visible or accessible location.
- All systems should be set up to change password at first login.
- All workstations should have auto-lock feature enabled that required a password to resume and set to activate at no more than 10 minutes idle time.
- Workstations visible to or accessible by others must be manually locked when left unattended.

Physical Access

- All employees are required to get access only via a biometrically enabled access control system to office premises of EasyClocking
- All visitors must be accompanied by the respective authorized employee within the office premises.
- Any access to the server rooms must be logged in the logbook showing name, date and time, and reason for entry. Only authorized users or authorized agents are permitted to access the server room.

Remote Access

Only authorized are permitted to remotely connect to EasyClocking's computer and server systems to access any information, either related to the company or the customer. Such users should be identified first as having a need to work remotely. They need to request remote access to the Information Office by the approval of his/her respective manager. The information office will then access the need and do appropriate firewall settings for the remote IP to access the systems.

Security Incident Response and Handling

All suspected or actual security breaches should be reported immediately to the Information Office who will consult with the CEO to assess the level of threat and/or liability posed to the organization or affected companies/individuals and respond according to Response Guidelines maintained by the Information Office.

Service Providers

Service providers utilized to design, implement and service technologies must provide contractual assurance that they will protect the company's sensitive information according to the policies and reasonable standards. Such contracts must be reviewed by legal counsel for appropriate measures taken regarding use and protection of sensitive information

Updates

Fulfilling our privacy and data security commitments is important to us. So, we're glad to comply and help you comply with the GDPR. If you have any questions about your rights under the GDPR as a User or how EasyClocking can help you with compliance as a Customer, we hope you'll reach out to us at marketing@easyclocking.com