



## Data Privacy Compliance Statement

### Introduction

Endmile Technologies, to be referred as “Endmile”, as a data processor, is committed to upholding the highest standards of data privacy and security. Our dedication extends to compliance with global data protection regulations, including the European Union General Data Protection Regulation (GDPR). This statement outlines our approach to data privacy and our commitment to safeguarding the rights of individuals.

### Essential Terms

- **Data Subject:** Individuals whose personal data is processed, encompassing various identifiable information such as name, identification number, or online identifier.
- **Controller:** The entity responsible for determining the purposes and means of processing personal data.
- **Processor:** The entity processing personal data on behalf of the Controller.

### Certification Consideration for Data Processors

While certification for GDPR compliance is not mandatory for data processors under the General Data Protection Regulation (GDPR). It's essential to note that certification is not a strict requirement imposed by the regulation itself.



## **Our Role and Commitment**

Endmile, as a data processor, is committed to assisting our customers (Controllers) in fulfilling their GDPR obligations. We provide tools and features to enable compliance with data protection regulations, including:

- Facilitating data exports, updates, deletions, and processing restrictions upon customer requests.
- Implementing security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction.
- Ensuring transparency and accountability in data processing activities through comprehensive record-keeping and documentation practices.

## **Data Privacy Measures**

Endmile prioritizes the security and confidentiality of user data transmitted through our services. Our platform is designed to uphold data privacy principles by:

- Encrypting data transmission to protect against interception and unauthorized access.
- Implementing access controls and authentication mechanisms to ensure that only authorized personnel can access personal data.
- Conducting regular security assessments and audits to identify and address potential vulnerabilities or threats to data security.



## Data Processing Protocols

Endmile adheres to strict data processing protocols outlined in our agreements with customers. These protocols include:

- **Confidentiality:** Ensuring that personnel involved in data processing activities maintain the confidentiality of personal data.
- **Security Measures:** Implementing technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.
- **Sub-processing Guidelines:** Engaging only trusted third-party sub processors that meet our stringent security and privacy standards.
- **Compliance with Applicable Laws:** Ensuring compliance with all relevant data protection laws and regulations, including GDPR and other applicable privacy laws.

## Assistance with Data Subject Rights

Endmile collaborates with customers to promptly address data subject requests and fulfill obligations under data protection laws. Our team provides:

- Timely notifications of data subject requests to enable customers to respond within the required timeframes.
- Support and guidance on responding to data subject requests, including accessing, rectifying, or deleting personal data as required by law.



## **Cross-Border Data Transfers**

Endmile ensures compliance with data protection laws concerning cross-border data transfers by:

- Implementing appropriate safeguards to protect personal data during transit and processing.
- Adhering to the principles of necessity and proportionality when transferring personal data to countries outside the European Economic Area (EEA) or other jurisdictions with similar data protection standards.

## **Breach Notification Procedures**

In the event of a personal data breach, Endmile follows stringent notification procedures to:

- Promptly inform affected customers of the breach and provide details of the incident.
- Cooperate with customers and regulatory authorities to mitigate the impact of the breach and prevent further unauthorized access or disclosure of personal data.

## **Record-Keeping Practices**

Endmile maintains comprehensive records of processing activities, including:

- Details of data processing activities conducted on behalf of customers.
- Documentation of data subject requests, responses, and any actions taken to address them.
- Records of security measures implemented to protect personal data against unauthorized access, disclosure, or alteration.



## Legal Compliance

Endmile operates in accordance with all applicable data protection laws and regulations, including GDPR and other relevant privacy laws. Our commitment to legal compliance includes:

- Ensuring that data processing activities are conducted in a lawful, fair, and transparent manner.
- Upholding the rights of data subjects and providing mechanisms for exercising those rights in accordance with applicable laws and regulations.

## For Inquiries

For any questions or concerns regarding data privacy and compliance, please contact our team at [gdpr@endmiletechnologies.com](mailto:gdpr@endmiletechnologies.com). We are dedicated to providing transparent and comprehensive support to our customers and ensuring the protection of personal data in accordance with data protection laws and regulations.