



Privacy & data protection policy

CANAL MOVERS & LOGISTICS CORP.



0. Table of contents

0. Table of contents 1

1. Introduction 2

2. Definitions of CMLC’s PDPP 2

2.2. Personal data 2

2.3. Processing 3

2.4. Controller 3

2.5. Processor 3

2.6. Recipient..... 3

2.7. Third party..... 3

2.8. Consent of the data subject 4

2.9. Personal data breach 4

3. CMLC Privacy & Data Protection Policy. 4

3.1. PDPP Administration 4

3.2. PDPP Notification..... 4

3.2.1. Purposes for collecting, using, retaining and disclosing information 4

3.2.1.1. Collected Information..... 4

3.2.1.2. Use of Collected Information 5

3.2.2. Disclosure of Personal Information to Third Parties 6

3.2.2.1. How?..... 6

3.2.2.2. Why?..... 6

3.3. Election and Explicit Consent of the Interested Party 7

3.3.1. Personal Information Disposition..... 7

a. Physical Documentation 7

b. Digital Documentation 7

3.4. Personal Information Access..... 7

4. Computer Security..... 7

4.1. Password Protection..... 7

4.2. Information Recovery (Backup) 8

5. PDPP Monitoring and Compliance 8

6. Responsibility for the Consequences of Disclosing Information to Third Parties..... 8



7. **Security Breaches**..... 8
8. **Personal Data Security Breach Protocol** 8

1. Introduction

Canal Movers & Logistics Corp. – *which, from now on is to be referred to as **CMLC*** - is a commercial organization compromised to the fulfilment of the fundamental rights of humanity, as well as principles and good practices related to the protection of people in regards of the processing of personal information.

Therefore, CMLC is committed to protect the information of its customers through the establishment of this *privacy and data protection policy*, this implies, among other things, the strict compliance with the General Data Protection Regulation of the European Parliament and the Council of the European Union, commonly known by its acronym in English, GDPR (General Data Protection Regulation), the Privacy Shield and the principles of privacy & data protection of FIDI.

2. Definitions of CMLC’s PDPP¹

They are part of the rights and responsibilities established by this policy:

2.2. Personal data

“Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can’t be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

¹ [Global Data Protection Regulation link \(Text with EEA relevance\)](#)



2.3. Processing

“Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

2.4. Controller

“The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law...”

2.5. Processor

“The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

2.6. Recipient

“The natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not”.

2.7. Third party

“The natural or legal person, public authority, agency or other body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data”.



2.8. Consent of the data subject

“Any freely give, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

2.9. Personal data breach

“A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. CMLC Privacy & Data Protection Policy.

3.1. PDPP Administration

By means of this document, CMLC defines, documents and communicates to people, their privacy policy and information protection. Moreover, it assigns responsibility for such policies and procedures.

3.2. PDPP Notification

CMLC has a privacy and data protection policy which was established within the internationally accepted principles framework regarding privacy rights and information protection of individuals.

3.2.1. Purposes for collecting, using, retaining and disclosing information

3.2.1.1. Collected Information

CMLC will collect personal information in order to provide its beneficiaries with a dedicated service. Nevertheless, we require your explicit consent ²(written) to collect such information. The information that will be collected is as follows:

² You have the right to revoke your explicit consent (written) for using your personal information.



- Full name
- Address, city and country of origin and/or destination (only if necessary, for the requested service).
- Email
- Mobile and/or residential telephone numbers
- Employer's contact details (in case the costs are covered by the employer)
- Photos of some of the objects or possessions for insurance purposes (fragile and valuable)
- ID and passport copy
- Certificate of ownership for vehicles (if applicable)
- Credit card copy (both sides) and complete AMEX form (only for AMEX payments)
- Social Security number (required only for relocations to the United States)

3.2.1.2. Use of Collected Information

CMLC will use the collected information during the provision of the services agreed with the client.

From the initial contact, CMLC will collect personal information such as: full name, address, telephone numbers and email. This information will be registered to our administrative software³ so our inspector can visit your home and estimate the approximate total to be packed and transported. During this inspection, it might be necessary to photograph fragile and valuable pieces in order to identify them and provide these details to our operative staff in order to make the wooden box where the piece will be packed and then, the packers can easily identify it once they are at your domicile.

The ID copy is requested in order to be able to continue with the export/import procedures of your possessions. The same applies to the certificate of ownership for vehicles.

³ [See the privacy policy of our administrative software provider](#)



When the service has a destination in the United States, CMLC will request your social security number.

Personal Information Retention

- a. Physical Documentation:** This information will be kept in the physical folder that contains all documents related to the service provided. Each folder is archived for a period of 7 years. This is the maximum period in which we have detected that a client may require our services again and this information is critically useful for providing a new required service.

- b. Digital Information:** Our clients' personal information compiled in our database is managed and retained through the application of the following points:

3.2.2. Disclosure of Personal Information to Third Parties

Siempre que cuente con el consentimiento explícito de las personas, CMLC divulgará su información personal a terceros.

3.2.2.1. How?

Your personal information is shared with our agents through emails, fax, telephone, physically or in any other way that allows the continuity of the operation of the services we provide to our clients.

3.2.2.2. Why?

The management of CMLC's clients' possessions is outside of the Republic of Panama and it is carried out through, what we will call from now on, AGENTS. These agents are endorsed by international federations such as [FIDI](#), [LACMA](#), [IAM](#), [OMNI](#). Due to the nature of the services provided, CMLC will share personal information with other providers. CMLC will ensure to monitor the compliance of such providers with the minimum privacy principles and information protection.



3.3. Election and Explicit Consent of the Interested Party

In order to use the information of the persons during the delivery of the agreed services between the client and CMLC, the explicit consent (written) of these persons is required. Nonetheless, this explicit consent may be **revoked** at any time by these persons. CMLC states that the consent can never be inferred from silence or inaction of the persons.

3.3.1. Personal Information Disposition

a. Physical Documentation

After 7 years, the folder where the shipment information was stored is destroyed inside the organization's facilities. It will not be moved to a third party's location for destruction nor for any other purpose, such as storage.

b. Digital Documentation

Digital information related to each shipment is destroyed after 7 years. For example: bills of lading (B/L), customs clearance, service evaluation surveys, customer signatures in inventories, etc.

3.4. Personal Information Access

CMLC provides our clients with access to their personal information for review, update and when required, adherence to the rights to forget and data portability.

4. Computer Security

When addressing computer security, we must bear in mind that there is not 100% secure or reliable security method. We can only reduce the chances of a system being vulnerable or minimizing the duration and damage caused by an attack.

4.1. Password Protection

For automated systems, individual accounts must be assigned that require a periodic password change.



4.2. Information Recovery (Backup)

CMLC keeps a copy of all computer information. Therefore, the information is stored in a portable unit located at any point in Panama City in order to have another backup. In the server's room is the Backup equipment which is comprised of 4 hard drives of 2 Terabytes each. The discs are mirrored configured.

5. PDPP Monitoring and Compliance

CMLC monitors the compliance of our suppliers (recipients) with respect to this privacy and data protection policy and it has procedures to address complaints and disputes related to privacy.

6. Responsibility for the Consequences of Disclosing Information to Third Parties

CMLC monitors, through mandatory evaluations, the compliance with this privacy and data protection policy and it is responsible for the security of the information it collects and discloses to third parties.

7. Security Breaches

CMLC will notify its clients when a violation of personal data security is confirmed. It will communicate to the interested parties about the security breach and will activate the security protocol in the event of personal data security breaches.

8. Personal Data Security Breach Protocol

Cuando se identifique una violación de seguridad de los datos personales retenidos en sus servidores, CMLC responderá de la siguiente manera:

When a personal data security violation of our servers is identified, CMLC will respond as follows:

- 8.1.** We have a procedure for evaluating the risk resulting from the security breach towards individuals.



- 8.2. We know who supervises our processing activities.
- 8.3. We have a process to notify the responsible area for information technology (IT) about the security breach within 72 hours of having identified the security violation.
- 8.4. We know what information we must provide to the responsible IT area about the security breach.
- 8.5. We have a process in order to inform affected individuals about the security breach when a high risk to their rights and freedoms is evident.
- 8.6. We know that we must inform the affected individuals as soon as we have the affectation information report.
- 8.7. We know what security breach information we must provide to individuals and that we must provide advice in order to help them to protect themselves from privacy violation effects.
- 8.8. We document all security violations, even if not all of them need to be reported.



Walter M. Laffitte
President & CEO

Explicit Consent

Dear customer,

Hereby, we kindly request your written consent regarding our privacy policy and information protection, through the means that are most convenient for you.

If you have any questions about our PDPP or CMLC supply chain quality & safety processes, please contact h.rodriquez@canalmovers.com.