GC MARITIME Consulting & Training LLC®

GDPR - Privacy Notice

1. What We Need

Our Personal Data Protection Policy governs the use and storage of your data.

GC Maritime Consulting & Training, LLC is a Controller of the personal data you (data subject) provide us. We collect the following types of personal data from you:

- For Users of our services:
  - General Information
    - Name
    - Phone Numbers
    - Email address
    - Physical Address
    - If you are a responsible for Billing
- For Crew onboard Vessels:
  - General Contact information
    - Vessel Name
    - Sex
    - Whether you are an occasional worker
    - Your Crew Employment Status
    - Whether you are onboard
    - Your position onboard
    - Whether you are a designated Security Officer
    - Whether you are a designated Safety Officer
    - Email addresses
    - Birthday
    - Place of Birth
    - Nationality
    - Phone Contacts
    - Physical Address
    - Notes on your file
    - Photograph
    - Passport and Visa information
    - Passport number
    - Passport Country
    - Passport Place of Issue
    - Passport Date of Issue
    - Passport Expiration
    - Visa Country
    - Visa Date of Issue
    - Visa Expiration
    - Visa Type
  - Employment Information
    - Date Employed
    - Date Ended
    - Port of Departure

[1] Florida Information Protection Act (2014) - *see* https://www.flsenate.gov/laws/statutes/2014/501.171

        - Reason for Leaving
        - Notes
    - Medical Information
        - Emergency Contacts
        - Doctor Contacts
        - Dentist Contacts
        - Blood Type and Rh
        - Allergies
        - Medical Issues
        - Current Medications
        - Medical History/Major Operations/Procedures
        - Medical Insurance
        - Medical Notes
        - Medical Power of Attorney
        - Immunizations Records
        - Prophylaxis Treatments
    - Next of Kin
        - Name
        - Relationship
        - Contact Information
        - Physical Address
    - Financial
        - Salary
        - Financial Notes
        - Bank Name
        - Bank Address
        - Bank Country
        - Bank Contact Information
        - Beneficiary Name
        - Beneficiary Address
        - Bank Aba/Routing Number
        - Bank Account Number
        - Bank Sort Codes
        - Bank IBAN number
        - Bank SWIFT Code
        - Currency

2. Why we need it

We need your personal data in order to provide you with the following services:

- General Contact Information is collected in order to understand your position onboard and communicate with you.
- Passport and Visa Information is collected in order to ensure your travel documents are valid and up to date relating to your employment
- Employment Information is collected in order to verify employment onboard a vessel
- Medical Information may be seen for safety onboard and ensuring your well-being in event of an emergency

[1] Florida Information Protection Act (2014) - *see* https://www.flsenate.gov/laws/statutes/2014/501.171

- Next of Kin Information may be seen in order to ensure we have Emergency contact information during maintenance of safety systems
- Financial Information may be seen during services provided to Clients

3. What We Do With It

Your personal data is processed in GC Maritime Consulting & Training, LLC located in the USA. Hosting and storage of your data takes place in Fort Lauderdale, Florida which is located in United States.

No third-party providers have access to your data, unless specifically required by law.

4. How Long We Keep It

Under Florida law, we are required to keep your documents for three (3) years according to the Data Retention Policy. After this period, your personal data will be irreversibly destroyed. Any personal data held by us for marketing and service update notifications will be kept by us until such time that you notify us that you no longer wish to receive this information.

5. What Are Your Rights?

Should you believe that any personal data we hold on you is incorrect or incomplete, you have the ability to request to see this information, rectify it or have it deleted. Please contact us through gc@gcmaritime.com.

In the event that you wish to complain about how we have handled your personal data, please contact Gabriella Cramer at gc@gcmaritime.com or in writing at 1416 NE 17th Terrace, Fort Lauderdale, FL, 33304. Our Founder will then look into your complaint and work with you to resolve the matter.

If you still feel that your personal data has not been handled appropriately according to the law, you can contact the relevant Data Protection Authority and file a complaint with them.

[1] Florida Information Protection Act (2014) - *see* https://www.flsenate.gov/laws/statutes/2014/501.171

Florida Information Protection Act (FIPA) of 2014

The Florida Information Protection Act of 2014 (FIPA) is a state law that provides procedures for the protection and security of the sensitive personal information of Floridians. It includes a comprehensive set of breach notification requirements.

Under FIPA, a "breach of security" or "breach" means unauthorized access of data in electronic form containing personal information.

(g)1. "Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.[1]

Implementation of Proper Data Security Measures

To comply with the Florida Information Protection Act (FIPA), GC Maritime Consulting & Training, LLC has implemented encryption, secure password policies, and regular monitoring for vulnerabilities. We update our software and hardware infrastructure to ensure optimal security, where applicable.

Timely Reporting of Data Breach

In the case of a data breach, we have implemented an Incident Response Plan. Part of FIPA compliance is promptly reporting the incident. Where applicable, we will notify affected individuals and regulatory authorities as required, typically within 30 days of discovering the breach. We will keep records of the investigation, and include any individuals, types of data involved, and steps taken to address the breach.

Education and Training of Employees

Lastly, to ensure FIPA compliance, our employees and agents will undergo education and training about the requirements and importance of data protection procedures. This includes awareness of data breaches, understanding company policies, and recognizing potential risks.

[1] Florida Information Protection Act (2014) - *see* https://www.flsenate.gov/laws/statutes/2014/501.171