

General Data Protection Policy: Employment Applicants

1. Overview & Commitment

This policy outlines how **Mexicrew Maritime Services** ("we," "us," or "our") collects, processes, and protects the personal data of job applicants. We voluntarily align our data handling practices with the European Union General Data Protection Regulation (GDPR) standards to ensure high levels of privacy, transparency, and data security.

2. Principles of Data Processing

In accordance with GDPR principles, we commit to handling applicant data:

- **Lawfully, fairly, and transparently** regarding the applicant.
- **Solely for specified, explicit, and legitimate purposes** related to recruitment.
- **Limited to what is necessary** (data minimization) for managing candidate applications.
- **Accurately**, keeping information up to date where appropriate.
- **Securely**, protecting against unauthorized processing, loss, or damage.

3. Personal Data We Collect

We collect and process personal data that you provide during the recruitment process, including:

- **Contact Details:** Full name, email address, phone number, and mailing address.
- **Application Details:** Resume/CV, cover letter, work history, education, certifications, and portfolio links.
- **Assessment Data:** Interview notes, technical test results, and references provided by designated contacts.
- **Communication Records:** Email correspondence and scheduling logs related to your application.

4. Legal Basis for Processing

Under GDPR framework standards, we process your personal data based on:

- **Pre-contractual Measures (Article 6(1)(b)):** Processing necessary to evaluate your application prior to entering into an employment contract.
- **Consent (Article 6(1)(a)):** Where you explicitly agree to us retaining your details for future job openings beyond the current role.
- **Legitimate Interests (Article 6(1)(f)):** For defending legal claims or ensuring network and information security.

5. How We Use Your Data

Your data is strictly used to:

- Evaluate your qualifications and suitability for the position applied for.
- Communicate with you regarding application status and interview scheduling.

- Conduct professional reference checks (with your prior notification).
- Maintain records of recruitment processes for quality control and compliance audits.

6. Data Sharing & International Transfers

We do not sell or rent applicant data. Your information is shared only with:

- **Internal Stakeholders:** HR staff, hiring managers, and interview panel members involved in the recruitment process.
- **Third-Party Service Providers:** Trusted cloud infrastructure, Applicant Tracking Systems (ATS), or communication tools that operate under strict confidentiality and data protection agreements.

7. Data Retention

- **Unsuccessful Applicants:** We retain application materials for **6 months** following the conclusion of the recruitment process to address any hiring queries. After this period, data is securely erased or anonymized.
- **Extended Retention:** If we wish to retain your CV for future open roles, we will request your explicit consent, which you may grant or decline without penalty.
- **Successful Applicants:** If hired, your application data transitions to your employee personnel file and is governed by our clients' Data Privacy Policies.

8. Your Rights Under GDPR Standards

As a job applicant, you hold the following voluntary rights regarding your personal data:

- **Access:** Request a copy of the personal data we hold about you.
- **Rectification:** Request correction of inaccurate or incomplete information.
- **Erasement ("Right to be Forgotten"):** Request deletion of your candidate profile when data is no longer necessary for the recruitment process.
- **Restriction:** Request that we pause processing your data under specific circumstances.
- **Withdrawal of Consent:** Withdraw any consent previously granted (e.g., retaining CV for future roles) at any time.

9. Data Security Measures

We implement technical and organizational measures to safeguard applicant data, including:

- Encrypted data transmission (TLS/SSL) for online applications.
- Restricted access controls limited to authorized HR personnel.
- Regular security reviews of third-party software tools storing applicant information.