VJDS International Inc. Data Protection Policy

Effective Date: 20th March 2013
Approved By: Directors
Owned By: VJDS International Inc.
Updated: 17th November 2024

1. **Introduction**
VJDS International Inc. is committed to safeguarding the privacy and security of personal data. This Data Protection Policy outlines the principles, practices, and procedures by which we manage and protect the personal and sensitive data entrusted to us by our employees, clients, customers, and other stakeholders. Our objective is to comply with applicable data protection laws and ensure that personal data is handled responsibly, securely, and transparently.

This policy is in accordance with relevant data protection regulations, including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other applicable privacy laws.

2. **Scope**
This policy applies to all employees, contractors, and third-party service providers who process, manage, or access personal data on behalf of VJDS International Inc.. It covers all personal data collected and processed by the company, whether stored electronically or in physical form, and applies across all business functions and activities, including:
- Employee data
- Customer and client data
- Supplier and partner data
- Any other personal data processed by the company

3. **Definitions**
- Personal Data: Any information that can directly or indirectly identify an individual, such as names, addresses, contact details, identification numbers, or online identifiers.
- Sensitive Data: A category of personal data that includes information such as racial or ethnic origin, political opinions, religious beliefs, health data, sexual orientation, etc.
- Data Processing: Any operation or set of operations performed on personal data, such as collection, storage, retrieval, use, disclosure, or destruction.
- Data Controller: The organization or individual that determines the purposes and means of processing personal data (in this case, VJDS International Inc.).
- Data Processor: Any third party that processes personal data on behalf of the data controller, under the data controller's instructions.

4. **Data Protection Principles**
VJDS International Inc. adheres to the following principles in the processing of personal data:

- Lawfulness, Fairness, and Transparency: We will process personal data lawfully, fairly, and in a transparent manner. Individuals will be informed about how their data is used and for what purposes.

- Purpose Limitation: Personal data will only be collected for specified, legitimate purposes and will not be processed in a manner incompatible with those purposes.
- Data Minimization: We will collect only the personal data that is necessary for the purposes for which it is processed.
- Accuracy: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data will be rectified or erased without delay.
- Storage Limitation: Personal data will not be kept in a form that permits identification of data subjects for longer than necessary.
- Integrity and Confidentiality: Personal data will be processed securely, using appropriate technical and organizational measures to protect against unauthorized access, disclosure, or destruction.
- Accountability: We are responsible for demonstrating compliance with the principles outlined in this policy.

5. **Legal Basis for Data Processing**
We process personal data only when we have a valid legal basis for doing so. These legal bases include:

- Consent: Where individuals have explicitly consented to the processing of their personal data for one or more specific purposes.
- Contractual Necessity: Where processing is necessary for the performance of a contract with the individual.
- Legal Obligation: Where processing is necessary for compliance with a legal obligation.
- Legitimate Interests: Where processing is necessary for our legitimate interests, provided these interests are not overridden by the individual's rights and freedoms.
- Vital Interests: Where processing is necessary to protect the vital interests of an individual or another person.
- Public Task: Where processing is necessary for the performance of an official function or public interest.

6. **Data Subject Rights**
We respect the rights of individuals under applicable data protection laws. Individuals have the following rights with respect to their personal data:

- Right to Access: Individuals have the right to request access to their personal data and obtain information about how it is processed.
- Right to Rectification: Individuals have the right to request the correction of inaccurate or incomplete data.
- Right to Erasure (Right to be Forgotten): Individuals can request the deletion of their personal data, subject to certain conditions.
- Right to Restrict Processing: Individuals may request the restriction of processing of their data under certain circumstances.
- Right to Data Portability: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transfer it to another data controller.
- Right to Object: Individuals can object to the processing of their personal data for direct marketing, profiling, or other legitimate interests.
- Right not to be subject to Automated Decisions: Individuals have the right not to be subject to automated decision-making that significantly affects them, unless certain conditions are met.

To exercise these rights, individuals can contact VJDS International Inc.'s Data Protection Officer (DPO) or the designated contact person.

7. **Data Security and Protection**
We are committed to maintaining the security and confidentiality of personal data. This includes implementing appropriate technical and organizational measures to protect data from unauthorized access, loss, alteration, or disclosure. These measures include:

- Encryption: Ensuring that sensitive data is encrypted both in transit and at rest.
- Access Controls: Limiting access to personal data to only those employees or third parties who need it to perform their duties.
- Regular Audits: Conducting regular security audits and assessments to ensure that personal data is adequately protected.
- Employee Training: Providing regular data protection and privacy training to all employees to ensure they understand their responsibilities and the importance of safeguarding personal data.

8. **Data Retention**
Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws or regulations. Once the data is no longer needed, it will be securely deleted or anonymized.

9. **Data Breach Management**
In the event of a data breach, we will:

- Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- Notify relevant authorities (e.g., data protection regulators) within 72 hours of becoming aware of the breach, where required by law.
- Investigate the breach to determine the cause and take corrective actions to prevent recurrence.

10. **Third-Party Data Sharing**
We may share personal data with third-party service providers (data processors) who perform services on our behalf, such as IT support, cloud storage, or marketing services. These third parties are required to sign data processing agreements to ensure they comply with applicable data protection laws and implement adequate security measures to protect personal data.

We will not sell or rent personal data to third parties for marketing purposes.

11. **International Data Transfers**
Personal data may be transferred outside the European Economic Area (EEA) or other jurisdictions with data protection laws. In such cases, we will ensure that appropriate safeguards are in place, such as using standard contractual clauses or other legal mechanisms to ensure the protection of personal data.

12. **Compliance and Monitoring**
We have appointed a Data Protection Officer (DPO) to oversee data protection compliance and ensure that this policy is being followed. The DPO is responsible for:

- Monitoring and auditing data processing activities.
- Providing guidance on data protection and privacy matters.
- Handling data protection inquiries and complaints.
- Ensuring ongoing staff training on data protection.

13. **Policy Review and Updates**
This Data Protection Policy will be reviewed and updated as required to ensure its continued compliance with applicable laws and regulations. Updates and changes to the policy will be communicated to all employees.