info@techvisions.com.sa

www.techvisions.com.sa

DATA PRIVACY POLICY

LEGAL DEPARTMENT
TECHVISIONS
Riyadh, KSA

Foreword

Document Control

Prepared By:	Legal Team
Dept:	Legal Dept
Document:	Data Privacy Policy
Version:	1.1
Website:	http://www.techvisions.com.sa

Publication History

Version	Date	By	Description
1.0	01-Sep-2024	Legal Dept	Initial draft
1.1	17-Sep-2024	Abdulaziz Al Yahya CEO	Amendments with KSA PDPL and Approved Final Version for distribution

This Data Privacy Policy has been reviewed and approved by the Techvisions Board, Security Committee, or Executive Leadership Team on 17th Sep 2024.

Statement of Confidentiality

The material contained in this document represents propriety, confidential information pertaining to Techvisions. The information in this document shall not be disclosed outside of Techvisions and shall not be duplicated, copied, used, or disclosed for any purpose other than internal use. Neither this document nor its content may be copied or distributed outside Techvisions without the prior written consent of Techvisions.

Disclaimer

Techvisions at its option, may change, delete, suspend, or discontinue parts or the policy in its entirety, at any time without prior notice.

Introduction

Purpose

This document has been developed by the Legal Team to familiarize employees, contractors, vendors, partners and any stakeholders working with Techvisions to protect personal data in accordance with the **Personal Data Protection Law (PDPL)** of the **Kingdom of Saudi Arabia (KSA)**. This policy outlines how we collect, use, store, transfer, and protect personal data during provision of IT consulting, cloud, professional and managed services.

Scope

This policy applies to:

All personal data we process in the Kingdom of Saudi Arabia.

Personal data collected from clients, partners, employees, vendors, and website visitors.

Data collected through our services, communications, website, and support systems.

All employees, contractors, sub-contractors and third-parties.

Data Privacy Policy

Information Security Objectives

To ensure the confidentiality, integrity, and availability of company information based on good risk management, legal, regulatory, and contractual obligations, and business needs.

To provide the resources required to develop, implement, and continually improve the information security management system (ISMS).

To effectively manage third-party vendors who process, store, or transmit information to identify, manage, and mitigate information security risks.

To create a culture of information security and data protection through effective employee training and risk awareness.

Information Security Policy Framework

The information security management system (ISMS) is built on an information security policy framework, which is made up of the following policies:

Categories of Personal Data We Collect

We may collect the following categories of personal data:

- **Identification Data**: Full name, job title, company name, national ID (where applicable).
- **Contact Information**: Email address, telephone number, business address.
- **Business Data**: Project details, contracts, support tickets, and communication records.
- **Technical Data**: IP address, browser type, operating system, system logs.
- **Employment Data** (if applicable): CVs, qualifications, background check data.

Legal Basis of Processing

We process your personal data only when one of the following legal bases under PDPL is met:

- You have provided **explicit consent**.
- Processing is necessary for the **performance of a contract**.
- Processing is required to comply with a **legal obligation**.

- Processing is for a **legitimate interest** that does not override your rights and freedoms.

that no individual has sole control over all of the company's computer applications. Critical tasks should be reviewed by another employee. Specific separation of duties requirements shall be defined for employees working with computer applications containing confidential data.

Purpose of Data Collection and Use

We use your personal data to:

- Deliver IT consulting and technical services.
- Communicate with you regarding your project, inquiry, or request.
- Improve and secure our systems and services.
- Comply with regulatory obligations.
- Conduct recruitment, onboarding, or HR-related processes (if applicable).
- Perform analytics or anonymized reporting.

Consent and Rights under PDPL

We obtain your clear and informed consent before collecting or processing your personal data unless otherwise permitted under PDPL.

You have the right to:

- **Access** your personal data.
- **Request correction** of inaccurate or incomplete data.
- **Request deletion** of your data.
- **Withdraw consent** at any time.
- **Object** to or **restrict** data processing.
- File a complaint with **SDAIA** if you believe your rights were violated.

Requests can be made by contacting us at privacy@techvisions.com.sa

Data Sharing and Disclosure

We may share personal data with:

- Authorized employees and consultants.

- Third-party service providers and vendors bound by confidentiality and data processing agreements.
- Regulatory authorities when legally required.

We do **not sell** your personal data under any circumstances.

International Data Transfers

We do not transfer personal data outside the Kingdom of Saudi Arabia unless:

- It is strictly necessary for the delivery of our services.
- The transfer complies with **PDPL** and the conditions set by the **Saudi Data and Artificial Intelligence Authority (SDAIA)**.
- Adequate safeguards are implemented and SDAIA approval is obtained where required.

Data Retention

We retain personal data only for the duration necessary to fulfill the purpose for which it was collected or as required by law. Upon expiry of the retention period, we securely delete or anonymize the data.

Data Protection and Security Measures

We implement industry-standard technical and organizational security measures, including:

- Encryption of data in transit and at rest.
- Access control mechanisms.
- Regular vulnerability assessments and audits.
- Staff training and data handling protocols.

Data Brech Notification

In the event of a personal data breach, we will notify:

- The **Saudi Data and Artificial Intelligence Authority (SDAIA)** promptly in accordance with legal timeframes.
- Affected individuals, where the breach is likely to result in harm, with details of the breach and mitigation steps.

Use of Cookies

We may use cookies and similar technologies to improve user experience on our website and gather usage analytics. Users can manage cookie settings via their browser.

Contact Us

If you have questions, concerns, or would like to exercise your data protection rights under PDPL, please contact us:

Data Protection Office (DPO)

Technology Visions for Information Technology (Techvisions)

Email: privacy@techvisions.com.sa

Phone: +966 11 247 2494

Policy Compliance

Compliance Measurement

The Legal team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the owner in advance and reported to the Techvision Management Review Team, Board of Directors.

Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed on a process for continual improvement.

Policy Acceptance

Acceptance	
(Name)	
(Sign)	