taq Automotive Intelligence

Personal Information Handling Policy

December 4, 2024.

Contents

1 Introduction

Personal Information Handling refers to the means by which SCI Technologies Ltd. d.b.a taq (“**taq**”, “**we**”, “**our**”, “**us**”) uses, transfers, discloses, stores, and destroys personal information collected pursuant to and further described in our Privacy Policy.

2 Purpose

This Personal Information Handling Policy (the “Policy”) provides an overview of how we retain and destroy the personal information of our customers (“Personal Information”) and the roles and responsibilities of our personnel at each stage of the lifecycle of our processing of Personal Information.

The Policy is part of our commitment to protecting Personal Information and our customers’ privacy.

3 Policy

Access and Control

Only the following roles at taq will have access to the Personal Information:

- Database Administrators (“DBA”): Have access to and control of Personal Information.
- Customer Service Representatives (“CSR”): Have access to view the Personal Information on the User Interface but cannot change the Personal Information. This is part of their role to help end users with system issues or training.
- Production Support Representatives (“PSR”): Have access to view the Personal Information on the User Interface and in limited respects in the database. The purpose would be to trouble shoot issues in the production environment.
- Concierge Client Service Representatives (“CCSR”): Have access to change and augment the Personal Information in the User Interface on behalf of the customer.

We log and monitor access to all Personal Information.

Retention, Destruction and Archiving

Our DBAs are responsible for the retention, purging and archiving of Personal Information.

Those with access to Personal Information must adhere to the following rules:

- Any backups of Personal Information shall be encrypted at rest.
- Personal Information shall be encrypted while in transit and at rest.
- Personal Information shall not be used or stored in non-production systems/environments.
- Personal information shall not be stored on personal phones or devices or removal media including USB drives, memory sticks etc.

4 Procedure

Those with access to Personal Information must ensure they adhere to the following procedure:

- Personal Information that is gathered through the system must be stored securely and encrypted at rest for up to 270 days.
- Sensitive Personal Information must be masked in the database. Sensitive Personal Information includes but is not limited to: SIN, passport information, driver's license, and bank account numbers.
- After the initial storage time, the Personal Information must be moved to an archive, stored offline and securely for up to seven years. After seven years, the Personal Information is then purged from the system by automated deletion. This process is fully automated and requires no manual intervention.

5 Personal Information Lifecycle Management

Personal Information is accessed by individuals at taq through the system flows at various states set out below in the table. The table below outlines the states and the entities that control or access the Personal Information within our system:

State	Access by taq	Description of Access
Collection	CCSR	During the collection phase, the CCSRs may be responsible for inputting the Personal Information into the system. In addition to the CCSRs, Clients and authorized system users (such as dealers, OEMs) may input the information into the system as well.
Use	DBA CSSR CSR PSR	DBAs are required to ensure that the hygiene and structure of the Personal Information is correct. They have access to the Personal Information in the database for this purpose. During this state, the CSSRs may augment or view Personal Information as required by their role. During this state, the CSRs may view the Personal Information as per their role. During this state, the PSRs may view the Personal Information as per their role.
Disclosure	DBA	DBAs may be required to disclose the Personal Information to third parties

		including law enforcement agencies when required to protect and defend our legal rights, protect the safety and security of users of our Services, prevent fraud, comply with the law, respond to legal process, or a request for cooperation by a government entity. Any disclosure of Personal Information that is required by law will be done in a secure manner.
Retention	DBA	During the retention period, the DBAs may be required to inspect the Personal Information to maintain its hygiene. The Personal Information may move through different states of retention which include being active to being archived. The DBAs ensure that this automated process is maintained.
Destruction	DBA	The DBAs ensure that the automated destruction processes take place in accordance with taq's destruction schedule.

For more information about our privacy compliance program, please review our Privacy Policy.