Toustone
Better data, smarter decisions.

Toustone Technical and Organisational Measures (TOMs)

These TOMs describe the measures Toustone has put in place to ensure the security of data. Where measures are required by a specific client, it is included and identified as such.

These specific requirements only relate to the specified client.

Security Measure	Toustone Implementation
Information Security Policies	Toustone has appointed a Privacy Manager and an IT Security Officer who are responsible for coordinating and monitoring Toustone security policies and procedures.
	Toustone personnel who have access to data are subject to confidentiality obligations. Additional checks are carried out on Toustone's personnel who have access to Special Category personal data.
	Toustone performs a Data Protection Impact Assessment (DPIA) on all processes containing personal data
IT Security Organisation	Within the Toustone's IT Security department, there are suitably qualified personnel. These personnel will coordinate the implementation of IT security for Toustone data
	Toustone segregates duties, roles and responsibilities where possible and/or when deemed critical. This prevents misuse or unauthorised/unintentional changes of data.
	Toustone promotes a culture of privacy and security in all activities relating to data.
Human Resources Security	Toustone informs and trains all its personnel about relevant security procedures.
	Toustone informs all personel on disciplinary actions for those who have violated security policies and standards.
Asset Management	Toustone has an inventory of all media on which data is stored. Access to the inventories of such media is restricted to Toustone personnel authorised to have such access.
	No personal data is stored unencrypted on portal devices (e.g. USB Memory sticks, external hard drives).
Access Control	Toustone implements a least privilege rule to all data access.
	Toustone audits all users and their privileges to data annually.
	Only anonymised data is used on demonstration systems.
Encryption and Cryptographic Controls	Data in transit to third parties will be encrypted. All client data in transit is encrypted.
	Personal data on the Toustone premises is encrypted.
	Toustone Backup data stored on-site or off site is encrypted.
	Toustone has a policy on the usage of cryptographic controls in order to create, manage, distribute, use, store and revoke of digital certificates and keys.
Physical and Environmental Security	Only authorised users have access to the Toustone facilities where information systems that process data are located.

	Toustone protects against loss of data due to power supply failure or power surges.
	Prior to any physical electronic disposal, Toustone ensures all data is deleted and/or destroyed.
Operations Security	Toustone maintains multiple copies of data, ensuring data can be recovered.
	Toustone uses off-site storage for copies of data and has procedures for recovery of data.
	Toustone has controls to help avoid malicious software gaining unauthorised access to data.
Communications Security	Toustone has implemented network security to protect information systems containing data.
	Toustone has implemented network security safeguards including: network segregation, intrusion detection, and perimeter protection.
Information Systems Acquisition, Development and Maintenance	Toustone will maintain systems and apply appropriate software patching.
	Toustone will identify and evaluate technical vulnerabilities and threats. Toustone will implement an effective patch and vulnerability management policy to mitigate any threat to information systems that process data.
Supplier Relationships	Any third party that Toustone use to process data will have contracts that as a minimum will include General Terms and Agreements, Data Sharing Agreement, Data Sharing Schedule, and a TOM. This TOM as a minimum will be equivalent to this ToM.
	Third Parties that use sub processors will agree with Toustone the content of these contracts prior to any signature.
	Third Parties will not share any data (including with sub-contractors) without clear and unambiguous consent of Toustone.
IT Security Incident Management	Toustone maintains a record of all security breaches.
	Toustone has an incident response procedure for IT security incidents.
Information security aspects of business continuity management	Toustone has a business continuity and disaster recovery plan for all information systems that process data.
Compliance	Toustone complies with security requirements and policies, applicable laws and regulatory requirements.
	No notice internal audits can be given by the Toustone Privacy Manager to Business Process Owners.
	Toustone undertakes a GDPR external audit once a year.