TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Category	Measure	Description
Security rules related to third parties, applicable whenever GT MOTIVE hires services that involve the processing of personal data for which GT MOTIVE is acting as the controller or processor (or subprocessor, as the case may be)	Need for a security document	GT MOTIVE will require that the third party in question provide a document, including administrative, technical and material security measures that are adequate to protect the security, confidentiality or integrity of personal data, meeting or exceeding the requirements established in these Rules and in applicable law (specifically Article 32 GDPR)
	Audits	GT MOTIVE may conduct audits on its processors, as often as it deems appropriate. The outcome of these audits will determine whether the processor will bear the auditing costs, or whether GT MOTIVE will do so instead. Auditing results may be notified to national data protection authorities, whenever GT MOTIVE is so requested.
Rules to guarantee data integrity and confidentiality	Access control	GT MOTIVE will adequately control all access, limiting personal data access to those workers and collaborators who are obliged to do so and will guarantee that each worker or collaborator processing GT MOTIVE information holds access credentials, on a single and individual basis, to any systems storing/processing GT MOTIVE information. GT MOTIVE keeps a record of all permits granted to each user.
	Data access control	GT MOTIVE's systems have a surrounding firewall, anti-spoofing filters anti-malware and anti-virus tools. GT MOTIVE periodically completes penetration tests. All of GT MOTIVE's systems have access records and the tracking of all operations, duly protected and subject to limited access control.
	Remote access	Remote access to GT MOTIVE's systems is carried out through VPNs (Virtual Private Networks), with adequate security measures. Remote access to third party systems from GT MOTIVE equipment is carried out through duly licensed remote control tools, fitted with adequate security measures.
	Use of equipment	All employees are informed that equipment should not be used for private purposes, nor should any information unrelated to GT MOTIVE be stored therein. All of GT MOTIVE's desktop computers have disconnected USB ports and Bluetooth technology to avoid data leaks. All GT MOTIVE portable devices (laptops, smartphones, tablets) may be remotely rebooted in order to erase any GT MOTIVE information.

		All equipment is blocked following a period of inactivity. For portable devices, employees are informed that blocking options should remain following inactivity.
	Authentication checks	Any clients and users authorised to access GT MOTIVE systems use private passwords, at least 8 characters long, containing at least one capital letter or number. After several failed attempts, access to GT MOTIVE's systems is blocked. Passwords are stored in encrypted form for GT MOTIVE or any third party.
	Physical access control	GT MOTIVE's facilities in Madrid are located in a building with camera and guard surveillance. GT MOTIVE's offices may be accessed through a personal access code. GT MOTIVE's facilities in La Coruña have a closed camera surveillance system, closed guard surveillance and card-based access control to the building's various areas. Access to the building perimeter demands that the guard complete an identity check. Security areas where third party personal data are stored are protected in such a way that only certain employees may access. All offices have alarm systems to prevent access outside regular working hours. Any centres outside GT MOTIVE, where GT MOTIVE data are stored, have implemented the necessary physical environmental and operational security measures to guarantee GT MOTIVE's data security.

	Hardware encryption	All hard drives and memory units in GT MOTIVE's mobile devices are encrypted (laptops, mobile phones).
	Software encryption	As a general rule and for efficiency purposes, all information stored in GT MOTIVE's production servers is not encrypted. The data centre where GT MOTIVE's servers are hosted has adequate security measures in place to protect the data contained in GT MOTIVE's servers.
	List of systems	GT MOTIVE has a list of all devices, equipment, servers or resources that may contain personal data.
	Data transmission control	Any data transfer is carried out through secure protocols. Preferably, GT MOTIVE will use SSL protocols, of TLS1.2 or above, and will be HTTPS, SFTP or its equivalent in each application.
	Data withholding	GT MOTIVE has a list of the various types of personal data stored, along with each individually configured data withholding, following minimisation and protection principles, as well as applicable follow-up and control measures. Furthermore, GT MOTIVE has a disposal procedure for electronic devices to ensure that any equipment containing GT MOTIVE data are duly erased with sufficient guarantees.
	Development control	Any system development or review must be approved through the process established by GT MOTIVE, to include automatic processes and verification manuals. GT MOTIVE will implement security procedures for the safe testing of applications or any other process outside production surroundings.
Rules to guarantee data resilience	Disaster prevention and recovery	GT MOTIVE periodically completes back-ups. The facilities where GT MOTIVE's servers are hosted have strict security standards that guarantee the highest protection of personal data. GT MOTIVE has duly documented contingency plans in place to cover disasters, periodically tested and in line with the nature of the information processed by GT MOTIVE.