MAF InfoCom™

Statement GDPR Technical and Organizational Measures

Version 1.1 November 2022

MAF InfoCom™

MAF InfoCom™ Statement GDPR Technical and Organizational Measures

Introduction

MAF InfoCom™ has implemented a number of technical & organizational measures to ensue Confidentiality of personal data in compliance with GDPR and we will always comply with GDPR and takes measures to protect personal data as described in the MAF InfoCom™ Privacy Statement.

Building access and security

MAF InfoCom™ has robust measures and protocols in place for securing access to any office or building and all our employees are aware of these controls include CCTV, security lighting, biometric access to areas with access to personal data and alarms. Visitors are escorted at all times and sign in/out of MAF offices. Visitors never get access to areas processing Data which are secured with biometric locks, restricted access and access logs.

Data access control

MAF InfoCom™ monitors and stores each companies' network access, Data access and file changes or deletion. Access to Data is restricted to those only needing to access this Data to perform our obligations towards our Clients and, Partners. Data access is secured by two-factor authentication. Our Wi-Fi networks use a very high level of encryption.

Password policy

MAF InfoCom™ enforces using strong passwords with a minimum defined length, number of bits and characters. Passwords are changed on a regular basis as a standard part of our security approach. MAF InfoCom™ employees are aware not to share passwords or leave systems unlocked when unattended.

Disposal

MAF InfoCom™ has procedures in place for the correct disposal of paperwork, devices, hardware and disks, along with protections for those that are lost as these form an essential part of the technical measures required by the GDPR. Measures such as shredding and certified un-reversable disposal of hard-copy records are used where personal data is contained in paper formats. Our IT departments is in charge of IT un-reversable disposal to guarantee effective and complete erasure of any personal data or access.

Cyber security, devices, networks and servers protection

MAF InfoCom™ takes a great number or technical measures to protect itself against advanced forms of hacking, vulnerabilities and constantly evolving threats. At the most basic level we use firewalls, malware scans and protection, anti-virus protection for all the devices, networks and hardware access points to personal data. Further we ensure having up-to-date software and operating systems on all devices and install updates and patches as soon as they become available.

Data protection and encryption

MAF InfoCom™ has taken precautions against unauthorized data copying. We use data encryption and secured personal data transfer over SSL channels. We have a defined interval for changing the keys.

Data breach and business continuity

MAF InfoCom™ has protocols and measures in place to back-up encrypted personal data and ensure that it can be recovered and maintained in the event of an incident. In case of a data breach or possible data breach MAF will inform its clients and partners without any unreasonable delay with sufficient information and will keep clients and partners informed of new developments and the measures that MAF InfoCom™ has taken to limit and terminate the size of the data breach and to prevent a similar incident in the future.

BYOD & remote access

MAF InfoCom™ maintains a 'bring your own device' policy and allows employees to use MAF InfoCom™ company devices outside the office. These devices are often used to access the MAF InfoCom™ network and common applications such as emails, and are therefor protected, secured and regularly reviewed by our IT department.

Storage and data location

MAF InfoCom™ stores data on site, on Microsoft Azure cloud servers and in ISO 27001 certified secret datacenters. The cloud servers and datacenters are not physically accessible.

High risk data

MAF InfoCom™ does not process high risk data.

Policies and procedures

MAF InfoCom™ has robust policies and procedures in place, providing intent, objectives and guidelines for adhering to regulations so our employees, contractors and any third-party working for or with the MAF InfoCom™ know what their obligations are and what to do if certain situations occur.

MAF InfoCom™ has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

MAF InfoCom™ personnel with access to Data are subject to confidentiality obligations.

MAF InfoCom™ maintains an inventory of all media on which Data is stored. Access to the inventories of such media is restricted to MAF personnel authorized to have such access.

MAF InfoCom™ imposes restrictions on printing Data and has procedures for disposing of printed materials that contain such Data.

MAF InfoCom™ personnel must obtain MAF InfoCom's authorization prior to storing Data on portable devices, remotely accessing such Data, or processing such Data outside MAF InfoCom's facilities.

Third parties

For those third parties MAF InfoCom™ uses for its Services, these third parties are classified as a sub-processor. In those cases MAF has concluded a processing agreement with these sub-processors with the same data protection obligations imposed on as those set out in this statement.

Awareness & training

MAF InfoCom™ has a culture of security and data protection awareness which ensures that employees, contractors and any third-party working for or with the MAF InfoCom™, know what is expected of them and how to maintain compliance. Regular and ongoing information security training sessions will ensure that they latest information, guidance, legislations and regulations are known and understood.

Termination of employee agreements

MAF InfoCom™ has strict procedures and measures in place in case of a termination of an employee agreement. All access to MAF InfoCom™ systems, networks offices and cloud are blocked from the moment of termination of any employee agreement. BYO devices are mandatory controlled by the IT department to ensure deletion of any access to MAF InfoCom™ networks and to ensure deletion of any personal data. This procedure is signed of by IT department and management. Each employees has signed a confidentiality agreement to ensure to keep the data secret.

Reviews & audits

MAF InfoCom™ regularity reviews and audits all the policies, controls and measures that we have in place against procedures and regulations to ensure they are working and are still relevant, effective and fit for purpose. Audits are lead by the Data Protection Officer and IT Department.

Due diligence

MAF InfoCom™ understands that who we are working with is just as important as what we do ourselves. There is little point putting extensive security and data protection measures into place if we would pass data to a third-party who cannot guarantee its safety or protection. Carrying out due diligence checks on suppliers and service providers is an essential part of our measures.

Reviews & audits

MAF InfoCom™ regularity reviews and audits all the policies, controls and measures that we have in place against procedures and regulations to ensure they are working and are still relevant, effective and fit for purpose. Audits are lead by the Data Protection Officer and IT Department.

Management Reporting

MAF InfoCom™ management receives reports and information on regular intervals enabling the adequate resources and funding are made available to ensure all appropriate measures continue the be implemented and for accountability at all levels.

MAF InfoCom™

Who we are

Formed in 2000, MAF InfoCom™ is a leading innovative technology provider with over two decades experience delivering solutions for Unified Communications and Collaboration including Monitoring, Analytics, Reporting, Recording, Headset & Device Management and DID Management.

We serve tens of thousands customers around the globe, in a large variety of branches. We have installations in over 50 countries ranging from SME's to multi-national global enterprises. In Europe MAF InfoCom™ is the largest provider of UC reporting solutions.

With the market trend towards Unified Communications and Collaboration we expand our sales across the globe rapidly. Our solutions work with every major UC&C technology.

Our solutions are offered from the Cloud, On-Premises and Partner Hosted to enable our customers and partners to choose the best model for their needs.

MAF ICIMS™

UC&C Monitoring Analytics & Reporting

MAF ICIMS CC™

Live Wallboards, Real Time Agent Status

MAF NMS™

Number Management System, DID Range Management

MAF UCR™

Microsoft Teams Voice Recorder

MAF LMS™

Microsoft Teams License Management System

MAF QMS™

Microsoft Teams Call Queue Management System

www.mafinfo.com   info@mafinfo.com