Technical and Organisational Measures

This document describes technical and organizational security measures and controls implemented by Mirago to protect the data of our customers, gathered as part of the Mirago service.

1) **Information Security Management**

i) Mirago's technological infrastructure operates from industry certified, third-party, data centres located across a number of global territories.

ii) This third-party has been and continues to be "assessed by independent, external auditors and currently receives attestations for a long list of internationally recognised certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5) and ENS High. It is also compliant with the CISPE Code of Conduct".

A comprehensive list of all our third-party's certifications can be found in the appendices of this document.

2) Physical Access

i) Our data centre partner describes thus:

"Physical components of our data centre are housed in nondescript facilities, at which physical barriers with controls are used to prevent access to the facilities at both perimeter and building access points. Passage through the physical barriers at the facilities requires either electronic access control validation (e.g. card access systems) or validation by security personnel (e.g. contract or in-house security personnel). Employees and contractors are assigned photo-ID badges that must be worn while the employee or contractors are at any of the facilities, and are continually escorted by authorised employees or contractors while visiting the facility".

"All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the facilities are monitored by CCTV surveillance cameras designed to record all individuals accessing the facilities.
Electronic intrusion detection systems are also maintained, which are in place to detect unauthorised access to the facilities, including monitoring points of vulnerability (e.g. primary entry doors, emergency egress doors, roof hatches etc.) with door contacts, glass breakage devices, interior motion detection, or other devices designed to detect individuals attempting to gain access to the facilities. All access to the facilities by contractors and employees is logged and routinely audited".

ii) Contractors and employees of our data centre partner have their access rights removed when they are no longer required for legitimate business reasons.

3) System Access

i) Access to Mirago white-label platforms is granted to platform owners and, in such cases, only to the particular owner of their respective platform.

ii) Platform owners are never granted access to a platform that they do not own, operate or have an interest in.

iii) Platform owners may grant system access to that of their own personnel, or their customers. Such permission is given independently of Mirago and requires that platform owners ensure their users comply with all relevant data protection legislation, as well as internal company policies.

iv) Mirago staff do not access the systems belonging to white label platform customers, unless there is a requirement to assist in the management and operation of the adserver, or in the event of an issue.

v) All Mirago employees access Mirago platforms with a unique identifier (UID).

vi) Mirago has a password policy that requires staff passwords be changed on a regular basis. Sharing of passwords is prohibited.

vii) Mirago uses a process to deactivate users and withdraw system access when personnel leave the company.

viii) Platform owners are responsible for withdrawing system access from their own personnel and that of customers, when respective employment or business relationships end.

ix) All access to systems are logged and monitored.

4) Data Access

i) Mirago staff do not access the data belonging to white label customers unless there is a requirement to assist in the management and operation of the adserver, or in the event of an issue.

ii) Therefore, access to customer data is implied as granted by platform owners on a 'need-to-know' basis.

iii) Any staff required to access customer data in the interests of maintaining and operating Mirago's ad serving technology are made aware of all appropriate data protection legislation and are required to agree to abide by all such legislation in their employment contracts.

iv) Any access or action taken by staff using Mirago platforms are logged and monitored.

5) Data Transmission & Storage

i) Access to, and use of, Mirago platforms are protected by Transport Layer Security (TLS 1.2).

ii) In addition, encryption is used to protect customer data that is made available to the front end of the platform. This includes use of https:// protocols.

iii) In the event of a serious incident such as fire, flooding, earthquake, or other natural disasters, or other incidents leading to the destruction of equipment or power loss, each data centre - operated by our third-party - can be failed over or back to prevent total loss or destruction of customer data.

iv) All production data centre sites have multiple power supplies, including generators on-site, to ensure constant availability of power.

v) Each data centre site has multiple access points to the internet to ensure connectivity.

vi) Each data centre is monitored 24x7x365 for power, network, and environmental issues. Monitoring is also in place to detect platform technical and performance issues.

6) Credit Cards

i) Mirago provides a facility for payments to be taken from the customers of platform owners via credit cards.

ii) In the event that platforms are configured to enable this feature, a third-party carrier is used to provide the payment processing functionality.
This carrier meets the highest industry guidelines and is validated to level 1 PCI DSS security standards. They are also on Visa's Global Compliant Provider List and Mastercard's SDP (Site Data Protection) List.

iii) Employee and customer activity is monitored to protect against unauthorised activities.

iv) Vulnerability checks are regularly carried out, including extensive penetration testing.

Credit Card Storage

v) Cardholder data is stored and managed using multiple encryption keys using split knowledge and dual control techniques. The data store holding cardholder data cannot be directly connected to via the internet.

Credit Card Data Transmission

vi) Credit card and payment information is transmitted between the user's browser and Mirago's carrier. It is never directly transmitted between Mirago and its payment carrier.

7) Data Separation

i) During processing, data received from all customers is assigned a unique identifier so it is always physically or logically separated.

8) Incident Management

i) In the event of a security breach, Mirago will inform its customers (platform owners) without undue delay when it has become aware of, and confirmed, such a breach.

9) Confidentiality, Integrity & Destruction of Data

i) All Mirago source code is held in a secure repository with access strictly limited to authorised personnel.

ii) Regular code reviews take place to ensure security and penetration testing is periodically carried out to identify flaws.

iii) All changes to Mirago software are logged and controlled by an approved release mechanism within a formalised deployment program.

iv) On request of a platform owner, customer data will be deleted. This action will take no longer than thirty days.

10) Availability of Data

i) Mirago uses significant levels of redundancy when storing customer data. This is managed by our third-party data centre, who achieves this via RDS relational database services.

Appendices

Our third party data centre partner is compliant with the below list of laws, regulations, alignments and frameworks. It also carries the following attestations and certifications of compliance, which are regularly assessed by a third-party auditor:

Appendix 1: Certifications / Attestations:

C5 [Germany]

Cyber Essentials Plus [UK]

DoD SRG

ENS High [Spain]

FedRAMP

FIPS

IRAP [Australia]

ISO 9001

ISO 27001

ISO 27017

ISO 27018

K-ISMS [Korea]

MTCS [Singapore]

PCI DSS Level 1

SEC Rule 17-a-4(f)

SOC 1

SOC 2

SOC 3

Appendix 2: Laws / Regulations / Privacy:

Argentina Data Privacy

CISPE

FERPA

GDPR

GLBA

HIPAA

HITECH

IRS 1075

ITAR

My Number Act [Japan]

U.K. DPA - 1988

VPAT / Section 508

Privacy Act [Australia]

Privacy Act [New Zealand]

PDPA - 2010 [Malaysia]

PDPA - 2012 [Singapore]

PIPEDA [Canada]

Spanish DPA Authorization

Appendix 3: Alignments / Frameworks:

CIS

CJIS

CSA

EU-US Privacy Shield

FFIEC

FISC

FISMA

G-Cloud [UK]

GxP (FDA CFR 21 Part 11)

ICREA

IT Grundschutz [Germany]

MITA 3.0

MPAA

NIST

PHR

Uptime Institute Tiers

UK Cloud Security Principles