Data Handling Policy

Last Updated
08 March 2019

Questions?
Tamjid Aijazi
Chief Technology Officer
tamjid.aijazi@miracletek.com.au
+61 409 483091

MiracleTek Pty. Ltd.
68 Hasler Road Osborne Park
Australia

Table of Contents

Data Handling Policy

The data handling policy for Miracle Mobile (we, us, company) ensures our compliance with data protection laws, and adherence to industry best practices. It protects the rights of clients and Miracle Mobile App users by defining the principles for handling data created on users' mobile devices as well as data stored on devices, Miracle Mobile's servers, and clients' virtual private cloud (VPC). It further details the data transmission practices followed, and identifies the entities authorized to access data.

1.1 Data Creation

To support Miracle Mobile App's offline functionality, user specific data is cached in mobile devices' local database and file system. Sensitive information, such as login information, is stored separately and secured with high-grade AES-256 encryption on app users' devices. Encryption keys are re-built dynamically prior to decryption.

1.2 Data Storage

1.2.1 Mobile Devices

Below are platform-specific details of the data stored on app users' mobile devices.

	iOS	Android	Windows
Images	Gallery, Camera, Sharing	Gallery, Camera, Sharing	Gallery, Camera, Sharing
Local Metadata Storage	JSON, File	JSON, File	JSON, File
Local Form Cache	JSON, File	JSON, File	JSON, File
App File Storage	Private Folder	Private Folder	Private Folder
User File Storage	Public Folder	Public Folder	Public Folder
Document Upload Control	Sharing, iCloud	Sharing, File Chooser	Sharing, File Chooser

Images: The Image Picker control in Miracle Mobile App allows users to add images either from Gallery or Camera.

Local Metadata Storage: This is the form metadata cache that is fetched from the server once, and then stored offline for generating forms' user interface and user experience.

Local Form Cache: Forms retained offline temporarily prior to submission to data stores or stored as drafts to be edited later are stored in local flat files in the application's private directory.

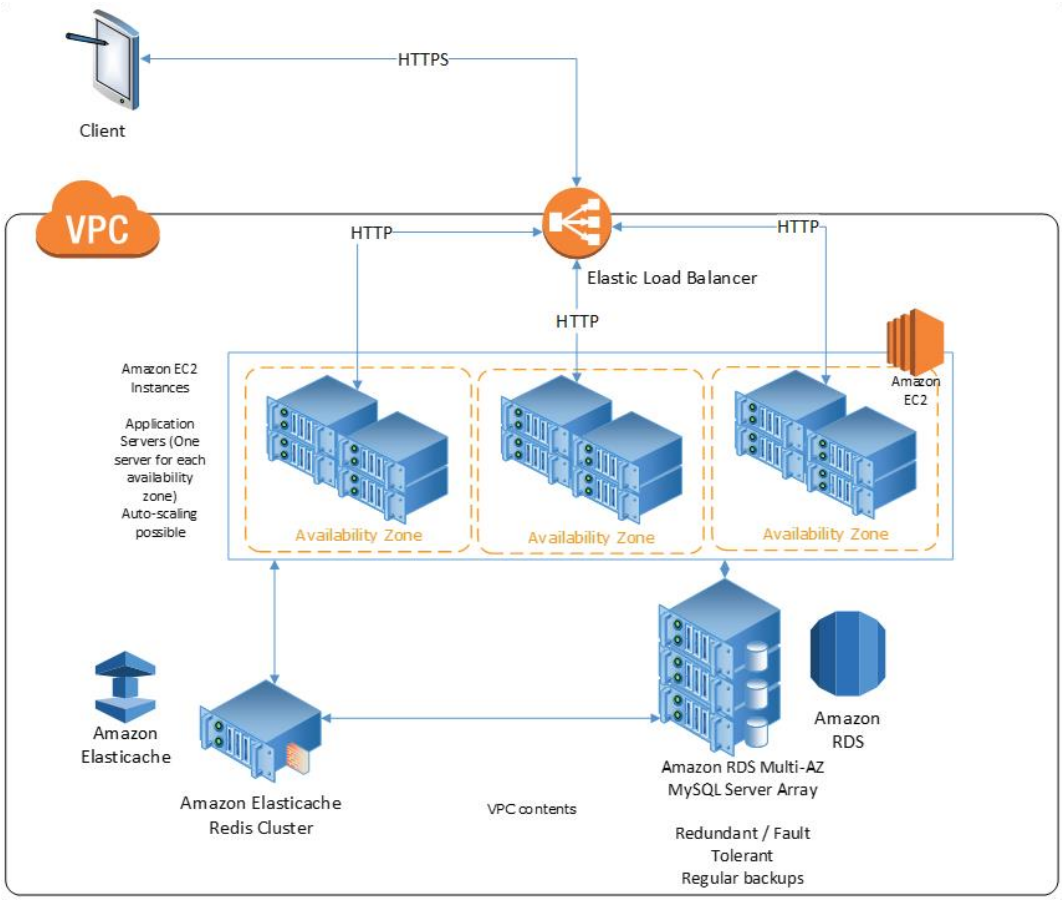
App File Storage: App File Storage files are the files generated by controls like Image Picker and Signature controls. These files are temporarily retained offline to be sent with a submission or stored as part of a draft for later use.

User File Storage: These are files created as a result of a request to download a file and view or open it in an external application. In addition to PDFs, images and videos, images captured via the device's camera are stored in public folders. That way, other applications can access these files when a user needs them. Storing these files in public folders also ensures access to the pictures captured through the device's camera at all times.

Document Upload Control: The Document Upload Control allows users to attach documents such as images to a form.

1.2.2 Miracle Mobile's Servers

Miracle Mobile's data is stored on a back-end MySQL database which is hosted on Amazon AWS Cloud. These data stores are inside Amazon Virtual Private Cloud (Amazon VPC). For enhanced security, we have restricted access to stored data so that it is only accessible from instances within the VPC instead of public networks.



1.2.3 Client's VPC

Clients are provided secure, logically-isolated VPCs hosted on Amazon AWS or Microsoft Azure. These are separate from the encrypted database layer.

VPCs hosted on Amazon AWS are protected by Amazon EC2 Security Groups, which act as virtual firewalls to control traffic. Complementing this security measure is AWS Elastic Load Balancing, which reduces the risk of spam and Denial of Service (DoS) attacks.

VPCs hosted on Microsoft Azure are designed to ensure secure operations through the lifecycle of the services. Azure's secure infrastructure incorporates secure practices and technologies which

control access to data, prevent unauthorized and unintentional transfer of information, and regulate traffic.

1.3 Data Access

Data hosted on Amazon AWS will not be accessed by Miracle Mobile or Amazon for any purpose other than as legally required. Client's data, however, may be consumed by third-party services if authorized. For instance, data to be used in dashboards can be sent to a contracted analytics platform provider.

1.3.1 Government's Right to Access

Miracle Mobile does not disclose client data to governmental or regulatory bodies unless we have to comply with the law or receive a valid and binding order. Clients will be notified prior to disclosing their data unless we are prohibited from doing so, or if there is evidence of illegal conduct in connection with the data in question.

1.4 Data Transmission

Client data is transmitted from Miracle Mobile App to Miracle Mobile's Servers through Secure Sockets Layer (SSL). Sensitive data undergoes asymmetric encryption before being transmitted from the app to our servers. This ensures data is not compromised even if intercepted.

From Miracle Mobile's Servers, data can be transmitted to three destinations:

1. Database hosted in a separate VPC on Amazon AWS (Sydney Region)
2. Client's Database hosted on premises
3. Client's Database hosted on Microsoft Azure

1.5 Data Sovereignty

Client VPCs are hosted on Amazon AWS data centers located in Sydney. Miracle Mobile can set up a disaster recovery site in the Singaporean region upon client request. We comply with the laws set by the governing/regulating bodies in those countries as well as clients' countries.