Privacy and Data Protection Policy

This Privacy and Data Protection Policy is formulated by Radiolocus, a brand owned by Amideeptech Technologies Private Limited, CIN - U72300MH2014PTC256018, a company incorporated under the laws of the Republic of India, having its office at 406, Platinum Mall, Jawahar Road, Ghatkopar (E), Mumbai – 400077, India

Radiolocus has appointed Praveen Joshi as its data protection officer who may be contacted at privacy@amideeptech.com and on his hand phone number +91 22 25010902.

1.0 PURPOSE

The purpose of this policy is to inform how Radiolocus collects personal information via its sensors deployed in various retail outlets or any other physical location and stores, processes, and transmits such personal information in compliance with GDPR requirements.

2.0 SCOPE

This policy is applicable to "EU data" (as defined hereinafter) and confirms to the EU General Data Protection Regulations. This Policy outlines how Radiolocus treats EU Data it collects from its sensors as a part of its service offerings. It also outlines rights of the Data Subject (where applicable) vis-à-vis her/his data that is collected and processed by Radiolocus.

3.0 APPLICABILITY

Radiolocus captures the wi-fi probe requests emitted by a Data Subject's mobile phone or wi-fi enabled personal device when the Data Subject visits any store/retail outlet or

other physical location where Radiolocus sensors are deployed. Such information/data includes:

1. Device MAC address
2. Signal Strength
3. Timestamp (Time at which the request was captured)
4. Stored SSIDs broadcasted by a data subject's mobile phone

The Radiolocus sensors that collect such data deploy the latest information security measures to prevent unauthorized access to possible misuse of data. The data is then transferred over an encrypted ("SSL") connection to Radiolocus servers inside the EU.

All EU Data collected from Radiolocus sensors is transferred to Radiolocus servers located in the EU. Radiolocus ensures that its data processing servers adhere to strict information security measures to adequately protect the data stored and processed in such servers. At no point of time is EU data processed at or transferred to any location outside the EU.

In Radiolocus servers, the SSIDs being redundant in processing are purged. Each MAC address along with location of the sensor from where it was captured, and the time of capture are hashed. For each hash thus computed, a random UUID complying with RFC 4122 is generated and is mapped to the said hash. Thereafter, the MAC address is purged from the system. The entire process is achieved within 30 minutes of transfer of data to the processing server.

The mapping of UUID to hash, as well as the hash itself is deleted after 24 hours. Thus, after 24 hours, the same MAC address will generate a different hash and will be mapped to another random UUID that bears no resemblance to the previous UUID making it computationally infeasible to either obtain the original MAC address from the hash or correlate a UUID to a particular MAC address.

The above process, considering that generation of UUID is a random protocol, achieves complete anonymization as at a later point in time, it will be computationally infeasible to re-generate the UUID if the hash of a MAC address (as described above) or the MAC address itself is available from some other source of data.

The hashed MAC addresses are then written into a file for later processing or queued for immediate processing by proprietary Radiolocus software, as the case maybe. The processing of data is achieved over multiple steps to finally generate sessions for each individual hashed MAC address, i.e., when that hashed MAC address was near a particular physical location with its start and end time. These sessions are further used to generate aggregated and anonymous reports that are shared with Radiolocus customers who use such reports for more effective decision-making.

The purging of the raw MAC addresses immediately after pseudonymization and of the pseudonymized MAC addresses after 24 hours of processing makes it impossible for any person including a Radiolocus employee to determine the identity of a data subject at any later point in time.

Radiolocus strictly adheres to the following policy:

1. No hashed MAC address is ever used or combined with any other dataset by Radiolocus to identify a data subject.

2. Radiolocus never shares a hashed MAC address with a third party including its customers to eliminate risk of identification of a data subject.

3. Radiolocus strictly adheres to the “storage limitation” principle and even removes pseudonymized MAC addresses from the system after 24 hours.

Further, Radiolocus collects personal information under a lawful contract for legitimate business purposes and complies with GDPR requirements for protection of personal

information and the interest of Data Subjects.

4.0 IMPORTANT TERMS

4.1 Data

Means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

4.1 Data Subject

You (Person whose data Radiolocus may collect)

4.2 EU Data

Personal information/data belonging to a Data Subject collected by a Radiolocus sensor deployed inside the EU area.

4.3 Information

Includes data, text, images, sound, voice, codes, computer programs, software and database or micro film or computer generated micro fiche"

4.4 Personal Information

"Personal information" for the purpose of this policy means MAC address of a mobile phone and/or any other personal device belonging to you ("Data Subject").

5.0 PURPOSE OF COLLECTION

Radiolocus collects personal information from Data Subjects for the following purposes:

- To aggregate, process, and analyze such information and share anonymized and aggregated reports generated out of such analysis with its customers, enabling them to make public spaces like malls, retail outlets, etc., more consumer centric and to enable public authorities to plan effective delivery of public services at airports, subway stations, bus stands, etc.;

- To enable EU entities that have a legal contract with Radiolocus to improve consumer experience and justify their business decisions;

- To enable EU entities to make smarter decisions by optimising operational effectiveness;

6.0 Radiolocus's RESPONSIBILITY

a) Radiolocus will make it known to the Data Subject, either directly where applicable, or, through the Controller in other cases that personal information/data is being collected;

b) Radiolocus will collect, process and analyze such information/data only in pursuance to its business activities and not otherwise;

c) Radiolocus will handle such information/data according to its documented information security program and information security policies;

d) Radiolocus will address any grievance of the Data Subject with respect to processing of data in a time bound manner.

e) Radiolocus has designated Mr. Harshal Vora as Radiolocus's "Grievance Officer";

f) The Grievance Officer will respond to any such grievance within forty-eight hours from the date of receipt of grievance.

7.0 RIGHTS OF DATA SUBJECT

7.1 Since Radiolocus does not store any personal information about a data subject it is not in a position to identify a data subject and will not be able to provide details relating to such personal information to a Data Subject after 36 hours of collection of data. However, if any Data Subject, inadvertently provides any additional information to Radiolocus enabling his/her identification through email or otherwise, Radiolocus will delete such additional information immediately after informing the Data Subject of its inability to provide details about the information asked for.

7.2 **Right to Opt-out –** All Data Subjects may opt out of the Radiolocus data analytics program by submitting their MAC addresses at ***https://optout.smart-places.org/.***

7.3 Once a Data Subject opts out of the Radiolocus data Analytics program, Radiolocus will no longer store, process or aggregate the Data Subject's data except to maintain the opt-out status of the Data Subject's device.

7.4 Any further queries about the opt-out process specifically or about privacy concerns of a Data Subject may be sent to ***privacy@amideeptech.com***. Radiolocus undertakes to answer all such queries faithfully and earnestly.

7.5 **Right to lodge complaint with the supervisory authority** – All Data Subjects have the right to lodge a complaint with the supervisory authority of

the member State of the EU of which they are citizens if they are aggrieved by any pertaining to collection and processing of personal data by Radiolocus.

8.0 DISCLOSURE OF DATA

8.1 Radiolocus does not use personal information of a Data Subject except for the purpose of generating aggregated and anonymous analytics using such data.

8.2 Radiolocus does not disseminate / disclose personal information of a Data Subject to any third party including its customers.

8.3 Radiolocus will not require any prior permission from the Data Subject when such information/data is to be disclosed under mandate of law.