

Privacy and Data Protection Policy

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.

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. SSID

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 the Radiolocus servers, the individual MAC addresses are immediately hashed via a one-way hash function to a fixed length, unintelligible hash output from which it is computationally infeasible to retrieve the original MAC addresses. After hashing, the original MAC addresses are immediately purged from Radiolocus servers to eliminate any risk of access to the original MAC addresses by any person.

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.

For all EU data stored in Radiolocus servers in the EU area, each hashed MAC address is completely anonymized by using a unique algorithm after which the hashed MAC addresses are deleted from the system within 36 hours of collection.

The anonymization technique makes it impossible for any person including a Radiolocus employee to determine the hashed MAC address from the anonymized data 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.

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 may collect 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 to enable better decision-making and to make such spaces more consumer centric;
- 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 without anonymization, 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 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@amideptech.com. Radiolocus undertakes to answer all such queries faithfully and earnestly.

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.