

# RUCKUS & THE GENERAL DATA PROTECTION REGULATION

With the arrival of the General Data Protection Regulation (GDPR), Ruckus Networks, an ARRIS Company, has prepared the following information regarding its compliance with this new European Union regulation.

Certain services that Ruckus provides to its customers, qualify Ruckus as a data processor in the context of GDPR. That is because Ruckus may be storing or accessing limited personal data on behalf of its customers. Ruckus does not share any personal data Ruckus processes with third party vendors except where vendors are identified as sub-processors, and in those circumstances, only to provide the services purchased by its customers. Ruckus end customers have control over how the data stored by Ruckus products is shared; they can give access to APIs to third parties for data sharing, and should have policies in place to ensure they are GDPR-compliant as a data controller.

For more details on Ruckus Networks' Products GDPR Compliance, read [Ruckus GDPR Compliance document](#).

For more in-depth information about the ARRIS GDPR Compliance Plan, visit the [ARRIS website](#).

## **Executive Summary**

- (1) Ruckus does not share personal data processed by Ruckus with anyone other than approved sub-processors – only our venue owners have the ability to do so. In many cases, Ruckus does not even have access to the personal data that is stored on the products it sells and is therefore not a processor in that context.
- (2) Ruckus may use aggregate information to improve product and service efficiency as well as supportability.
- (3) Ruckus is documenting the details of what data might be processed by Ruckus in a service offering or stored in a product purchased by a customer and how the customer has control over such data. Product/Service Privacy Datasheets are available upon request.
- (4) We are improving product-design processes to involve data privacy elements.

## **GDPR Context and Details**

Networking Equipment (such as the products sold by Ruckus Networks) usually stores many types of data. That equipment provides control to buyers (Ruckus customers) who are considered “controllers” under the GDPR. The personal data belongs to the data subjects, that is, natural persons in the EU that fall within the scope of GDPR. Personal data is any information relating to an identified or identifiable natural person. Personal data may include an “online

identifier” such as the MAC address of a mobile device or laptop, even if there are only limited details associated with those identifiers..

Regardless of the levels of sensitivity, data subjects have a right to their personal data and might request that organizations that have deployed Ruckus products provide access to or information about that personal data. Data subjects may also have the right to request that their personal data be deleted (though in some cases, the data may already be overwritten on a routine basis). Data subjects will likely engage a venue owner, such as the mall operator or the enterprise IT or security personnel, to exercise their GDPR rights. Thus, Ruckus’ plans to empower our partners and customers with GDPR disclosures, reports and tools so they can cater to the needs of the data subjects and be GDPR compliant.

Ruckus took a structured approach to addressing GDPR compliance by inviting a 3rd party privacy team to guide us through our GDPR efforts. Ruckus products and service offerings such as Ruckus Cloud Wi-Fi, Cloudpath Enrollment System, Smart Positioning Technology (SPoT), SmartCell Insight (SCI), Ruckus Diagnostic Dashboard, Synesis and SmartZone controllers and services were reviewed in the following areas:

- (1) What data are the products storing that can be considered personal data?
- (2) Who controls this data? Which, if any, sub-processors have access to this data?
- (3) How long is this personal data retained?
- (4) Are we making it simple and easy for our partners and customers to understand, by communicating this information to them through privacy documents, contracts and training?
- (5) Is there an easy way to retrieve personal data if asked by a data subject? Is this built into our products?
- (6) Is there an easy way to delete personal data if requested by data subject? Is this tool built into our products?
- (7) If there is a breach of data in a Ruckus hosted service, or in the product hosted by Ruckus’ customer, can Ruckus inform the affected parties of the extent of the breach and remedies, within the GDPR defined time constraints?
- (8) Is Ruckus taking measures to keep data privacy requirements a top priority in current and future product designs?

Please reach out to your local Ruckus sales or Ruckus reseller if you require additional information.