

AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND
RUCKUS WIRELESS, INC.
STANDARD STUDENT DATA PRIVACY AGREEMENT

This Student Data Privacy Agreement (“**DPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and as modified by The School Board of Citrus County, Florida, is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

The School Board of Citrus County, Florida, located at 1007 W. Main Street, Inverness, Florida 34450 (the “**LEA**”)

and

Ruckus Wireless, Inc., located at 350 W. Java Dr., Sunnyvale, CA 94089, and its affiliates (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), and applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. Special Provisions. Check if Required

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

- ✓ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (Optional)

If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

- 3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
- 4. This DPA shall stay in effect for three (3) years. **Exhibit "E" (if applicable)** will expire three (3) years from the date the original DPA was signed.
- 5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
- 6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Lance Fletcher

Title: Coordinator of Educational Technology

Address: 3741 W. Educational Path, Lecanto, FL 34461

Phone: (352) 746-3437


Email: FletcherLA@citrusschools.org

The designated representative for the Provider for this DPA is:


Name: Krista Bowen
Title: Deputy General Counsel
Address: 1100 CommScope Place SE
Phone: 800-982-1708
Email: legalnotices@commscope.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: The School Board of Citrus County, Florida.

Signature: 
Printed Name: Douglas A. Dodd
Title: Chairman
Date: Nov. 14, 2023

Ruckus Wireless, Inc.: _____

Signature: 
Printed Name: Bart Giordano
Title: SVP & President, NICS
Date: 18-Oct-23

STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date

of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

Article III. ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide any Student Data required for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data, if applicable.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

Article IV. ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. Any Student Data shared pursuant to the Service Agreement, including any persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to any Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality Agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
 - (a) **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De- Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written

notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

5. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
6. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Article V. ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once every other calendar year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality Agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of

the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of any Student Data maintained by the Provider the Provider shall provide notification to LEA as soon as practically possible of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - iv. A general description of the breach incident, if that information is

possible to determine at the time the notice is provided.

- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with information about said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

Article VII. MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service Agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, then upon LEA's request, the Provider shall destroy all of LEA's Student Data.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license Agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit "H"**, the SDPC Standard Clauses, and/or the

Supplemental State Terms, Exhibit "H" will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire Agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or Agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the

DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or Contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both Parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

EXHIBIT "A"

DESCRIPTION OF SERVICES

RUCKUS Analytics from CommScope is a cloud service for network analytics and assurance. Powered by machine learning (ML) and artificial intelligence (AI), it helps customers get the most from their RUCKUS network. The service gives IT comprehensive visibility into network operations. It accelerates troubleshooting and helps IT teams meet their network service-level agreements (SLAs).

EXHIBIT "B"**SCHEDULE OF DATA**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users*, Use of cookies, etc. * IP Addresses of devices connected to LEA's network are collected but they are not metadata and cannot be used to identify a student	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>

	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>

Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application: Client MAC Address Client IP Address Username OS Manufacturer OS Type Device Type First Connection Time	<input checked="" type="checkbox"/>

	Disconnect Time	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers and are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written Agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services (if applicable) including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files,

photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a Contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

SAMPLE DIRECTIVE FOR DISPOSITION OF DATA

The School Board of Citrus County, Florida, Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

X Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

____ Disposition shall be by destruction or deletion of data.

X Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

X As soon as commercially practicable following LEA's request.

____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF TERMS

1. OFFER OF TERMS

Provider offers the same privacy protections found in this DPA between it and **The School Board of Citrus County, Florida** ("Originating LEA"), which is dated _____, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

*Provider Name

BY: **NOT APPLICABLE - SAMPLE FORM ONLY

Date: _____

Printed Name: _____

Title/Position: _____

1. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between **The School Board of Citrus County, Florida**, and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

The School Board of Citrus County, Florida

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

SCHOOL DISTRICT NAME: THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone
Number: _____

Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity

Frameworks 2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input checked="" type="checkbox"/>	Center for Internet Security (CIS)* * Provider is currently engaged in gaining compliance with CIS Top 18. In the near term, Provider abides by Exhibit H Attachment C	CIS Critical Security Controls (CSC, CIS Top 20)

<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)
--------------------------	--	--

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"

Supplemental SDPC State Terms for [State]

Version _____

[The State Supplement is an **optional** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual Parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

EXHIBIT "H"

Additional Terms or Modifications

THIS EXHIBIT "H" effective simultaneously with attached Student Data Privacy Agreement ("DPA") between The School Board of Citrus County, Florida, (the "Local Education Agency" or "LEA") and Ruckus Wireless, Inc., (the "Provider") is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. The second WHEREAS CLAUSE is amended to add "the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98)" after "15 U.S.C. § 6501-6506 (16 CFR Part 312)".
2. Paragraph 3 on the page 2 of the DPA is deleted in its entirety and replaced with the following: In the event of a conflict between the DPA Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including Provider Terms of Service or Privacy Policy, the terms of Technology Master Service Agreement (if applicable), and then this DPA shall control.
3. The last sentence of Article II, Paragraph 1 is amended as follows: Provider agrees that for purposes of this Agreement, it will be designated a "School Official," under the control and direction of the LEA as it pertains to the use of Student Data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. Provider may transfer student-generated content to a separate account, according to the procedures set forth below. Provider agrees to abide by FERPA and Fla. Stat. 1002.22 while performing its service for the LEA.
4. Article I, Paragraph 2 is amended to add the following: Indemnification. Provider shall indemnify, hold harmless, and defend the LEA and all of LEA's current, past, and future officers, agents, and employees (collectively, "Indemnified Party") from and against any and all causes of action, demands, claims, losses, liabilities, and expenditures of any kind, including attorneys' fees, court costs, and expenses, including through the conclusion of any appellate proceedings, raised or asserted by any person or entity not a party to this Agreement, and caused or alleged to be caused, in whole or in part, by any breach of this Agreement by Provider, third-Parties, or subprocessor(s) related to Attachment A, Exhibit B (Schedule of Data), including but not limited to, failure to notify the LEA of any additional students' PII collected and not

updated by Provider in Exhibit B.

5. Article II, Paragraph 5 is deleted in its entirety and replaced with the following: Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Provider agrees to share the Subprocessors names and Agreements with LEA upon LEA's request.
6. Article III, Paragraph 1 is amended to add the following sentence: LEA will allow Provider access to Student Data necessary to perform the Services and pursuant to the terms of this DPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DPA.
7. Article IV, Paragraph 1 is amended to add the following sentence: The Parties expect and anticipate that Provider may receive personally identifiable information in education records from the District only as an incident of service or training that Provider provides to the LEA pursuant to this Agreement. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to Student Data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this DPA. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records
8. Article IV, Paragraph 2 is amended to add the following sentence: Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta Student Data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
9. Article IV, Paragraph 6 is deleted in its entirety and replaced with the following: Provider is prohibited from using or selling Student Data to (a) market or advertise to

students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from generating legitimate personalized learning recommendations.

10. Article V, Paragraph 1 is deleted in its entirety and replaced with the following: Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored. Provider shall not, without the express prior written consent of District: Transmit Student Data or PII to any Providers or Subprocessors located outside of the United States; distribute, repurpose or share Student Data or PII with any Partner Systems not used for providing services to the LEA; use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes]; use PII or any portion thereof to develop commercial products or services; use any PII for any other purpose other than in connection with the services provided to the LEA; and engage in targeted advertising, based on the Student Data collected from the LEA.
11. Article VII, is hereby amended to add Paragraph 10 as follows: **Assignment.** None of the Parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other party to this DPA.
12. Article VII, is hereby amended to add Paragraph 11 as follows: **Click through.** Any “click through” terms and conditions or terms of use are superseded by the Technology Master Service Agreement (if applicable) and this DPA, and acceptance of the terms and conditions or terms of use through the “click through” do not indicate acceptance by the entity.
13. Article VII, is hereby amended to add Paragraph 12 as follows: **Security Controls.** Security Controls. Provider represents and warrants that any software licensed hereunder shall not at the time of sale contain any virus, worm, Trojan Horse, tracking software or be capable of identifying non-approved users or tracking any approved user, or any undocumented software locks or drop dead devices that would render inaccessible or impair in any way the operation of the software or any other hardware, software or data for which the software is designed to work with.

14. Article VII, is hereby amended to add Paragraph 13 as follows: **Authority to Execute Agreement.** Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT AND ADDENDUM WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

<p>The School Board of Citrus County, Florida [Redacted Signature] _____ Douglas A. Dodd, Chairman Date: <u>Nov. 14, 2023</u></p>	<p>Ruckus Wireless, Inc.: [Redacted Signature] _____ By: [Redacted] Title: <u>SVP & President, NICS</u> Date: <u>18-Oct-23</u></p>
---	--

ATTACHMENT A
RUCKUS TERMS OF SERVICE

Ruckus Cloud Hosted Service Terms and Conditions for End Users and Partners

This agreement sets forth the terms and conditions under which Ruckus Wireless, Inc. ("Ruckus") is willing to grant the entity identified on the Order ("Customer") access to the Services. In consideration of the covenants and conditions set forth herein, each of Ruckus and the Customer agree as follows:

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY. BY CLICKING ON THE "I ACCEPT" BUTTON, COMPLETING THE REGISTRATION PROCESS, AND/OR USING THE SERVICE, CUSTOMER ACKNOWLEDGES THAT (1) IT HAS READ THIS AGREEMENT AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS, (2) THE PERSON ACCEPTING THIS AGREEMENT IS OF A LEGAL AGE TO FORM A BINDING AGREEMENT WITH RUCKUS, AND (3) THE PERSON ACCEPTING THIS AGREEMENT HAS THE AUTHORITY TO ENTER INTO THIS AGREEMENT PERSONALLY OR ON BEHALF OF THE COMPANY HE/SHE HAS NAMED AS THE CUSTOMER, AND TO BIND THAT ENTITY TO THIS AGREEMENT. IF YOU ARE A RUCKUS CHANNEL PARTNER (AS DEFINED BELOW) READING THIS AT A CUSTOMER'S REQUEST, THE CUSTOMER MUST REVIEW AND ACCEPT THESE TERMS, YOU MAY NOT ACCEPT THESE TERMS ON THE CUSTOMER'S BEHALF. IF CUSTOMER DOES NOT AGREE TO THESE TERMS AND CONDITIONS, CUSTOMER MAY NOT USE THE SERVICE.

1) Definitions

“Authorized Device Limit” means the maximum number of Ruckus access points that the Service will support during the Service Term, as set forth in the applicable Order.

“Cloud MSP” means a Ruckus Channel Partner authorized by Ruckus to onboard End Users on Ruckus cloud platform, manage Ruckus Cloud Service and provide First Call (1st), and Onsite support to their End Users. Ruckus will provide Level 2+ Support.

“Customer Data” means all data collected by the Service (other than authentication keys and related data used by Ruckus to authorize Customer’s use of the Service), including but not limited to any data regarding the devices or users that connect to a network operated by Customer.

“Documentation” means the published technical or user instruction manuals, including any updates thereto, relating to the use of the Service made generally available by Ruckus to its customers.

“Evaluation Term” means a limited period of time during which Customer is permitted to use the Service without placing an Order; provided, that the Evaluation Term is subject to early termination as provided in this agreement.

“End User” means entity that receive support directly from the Customer as part of the Program

“First (1st) Call Support” means providing support including the following:

- Receiving first call from End User
- Performing basic Level 1 troubleshooting of the product and issues. This includes validating that the configuration is appropriate for End User requirements, collecting support logs, traces, dumps and output of basic commands and researching Ruckus technical forums for known solutions

- Determine if the issue is being caused by APs not able to connect to the cloud due to firewall mis-configuration
- Determining if the issue being faced is a known problem
- Providing evidence that debugging has been performed to isolate the issue to a Ruckus product problem (i.e. documentation of commands and logs that indicate a problem with Ruckus products)
- Escalate issues to Ruckus Technical Assistance Center when necessary providing end username and IDs, detailed description of problem and priority level, on behalf of the End User.
- Assisting End User with RMA process, which might include receiving replacement products and installing replacement products at End User's site

"Level 2+ Support" means providing support including the following:

- Provide in-depth technical assistance for reported problems
- Analyze trace and dump information
- Determine if failure was caused by microcode defects or hardware defects
- If the problem was caused by a software defect, determine the software module and line of microcode and recommended corrective action to the microcode
- Perform detailed analysis of gathered traces and processor dumps to confirm defect
- Develop, test and release patches or work-around solutions

- Drive product defects into Ruckus sustaining engineering for permanent fix for a future release
- Implement hardware, software and firmware fixes as directed by Ruckus technical support

“Onsite Support” means the procedure to connect APs so that APs can connect to the cloud.

“Order” means the ordering or quote document, either physical or electronic, accepted by Ruckus that sets forth Customer’s Scope of Use (as defined below) of the Service.

“Ruckus Channel Partner” means an entity authorized by Ruckus to sell subscription licenses to access the Service.

“Service” means the online network management service identified in the applicable Order that is made available for use by Ruckus to Customer (using equipment hosted by Ruckus or a third party data center for use and access by Customer), including support services made available through the Service Portal and those provided from the United States or India and any related Documentation, and excluding any Ruckus access points or other hardware products.

“Service Portal” means the online administrative site for the Service located at the URL set forth in the Order.

“Service Term” means the period of time for which access to the Service is authorized, as set forth in the applicable Order.

2) Service

a) Trial Evaluation and License. Upon Customer's request for a trial period to evaluate the Service, Ruckus may make the Service available to Customer via the Service Portal solely for evaluation and demonstration purposes upon Customer's acceptance of these terms. Upon Customer initially accessing the Service, the Evaluation Term shall commence. Customer understands and accepts that during the Evaluation Term, the Service may have limited functionality as well as features that are restricted.

b) Activation and Delivery. Upon acceptance of an Order or Customer's request for a trial period, Ruckus or a Ruckus Channel Partner will provide Customer with instructions to activate the Service. During activation, Customer must confirm the terms of this agreement prior to being provided access to the Service. Once Customer completes activation, Ruckus will make the Service available to Customer and provide Customer with credentials allowing access to and use of the Service.

c) Service License. During the applicable Evaluation Term or Service Term, subject to Customer's compliance with the terms and conditions of this agreement, including the payment of any applicable subscription license fees, Ruckus grants Customer a non-exclusive, non-transferable, non-sublicensable right to access and use the Service via an internet connection in accordance with the Documentation and any limitations or restrictions set forth in the applicable Orders or trial request, including but not limited to the Authorized Device Limit and Service Term (the "Scope of Use"). Only the employees, contractors and agents of Customer acting on Customer's behalf may exercise the licenses granted to Customer in this section. Customer is solely responsible for acquiring, separately from this agreement, any wireless client endpoints or other devices for use in conjunction with its use of the Service.

d) Scope of Use. Customer may use the Service only in accordance with the Scope of Use. If Customer desires to exceed the Scope of Use, Customer may place an Order to increase the Scope of Use. Upon written acceptance by Ruckus or its Ruckus Channel Partner, Customer may use the Service in accordance with the new Scope of Use.

e) Service Operations. Generally, the Service is installed and runs in third party data centers contracted by Ruckus to make the Service available for access to Customer via an internet connection. However, Ruckus may choose to operate such a data center at any time. While Ruckus endeavors to contract with reputable third parties that provide global hosting services, Ruckus bears no responsibility or liability with respect to the actions or malfeasance of such third parties. Licenses to access and use the Service are personal to Customer, and Customer shall be ultimately responsible for the interaction with any

instance of the Service made available to Customer, including but not limited to, (1) the management of all Customer Data stored by or accessed through the Service and (2) the use of or access to the Service by Ruckus support or a third party (including but not limited to a Ruckus Channel Partner) where such use or access is enabled or authorized by Customer. Customer is solely responsible for acquiring, separately from this agreement, any wireless client endpoints or other devices for use in conjunction with its use of the Service.

i) Customer Data. As between Customer and Ruckus, Customer retains sole ownership in the Customer Data. Any functionality in the Service that allows for the collection, storage, access or use of Customer Data is provided solely for Customer's benefit. Neither Ruckus nor any third party is authorized by Ruckus to access Customer Data, unless authorized by Customer or in connection with the provision or operation of the Service by Ruckus. However, Ruckus and such third-party service providers will comply with any lawful process served upon them. Customer hereby grants to Ruckus a limited, non-exclusive, non-transferable, royalty-free license to reproduce, translate, encode, process and use Customer Data for the purpose of providing and improving the Service and to fulfill Ruckus's obligations under this agreement. Ruckus's processing, storage or transmission of any Customer Data shall be governed by the terms of the "Privacy Policy" available here (and any annexes or supplemental policies incorporated by reference): <https://support.ruckuswireless.com/ruckus-cloud-privacy-policy>. Pursuant to the Privacy Policy, the Customer is the data collector and the data controller of all of the personal data contained within the Customer Data and is therefore solely responsible for and represents and warrants that it has provided all

notices and obtained all consents necessary to permit Ruckus to lawfully collect, store, process, access, transfer and use Customer Data in accordance with the terms herein and those set out in the Privacy Policy

ii) Security Breaches. Ruckus believes strongly in providing a secure Service and takes reasonable steps considering industry practices to help secure the Service and any Customer Data stored on the Service from unauthorized access, including those set out in the Security Schedule to the Privacy Policy. However, despite these steps, no method of security is 100% secure, and Customer acknowledges that unauthorized access may occur. Ruckus will promptly communicate to Customer regarding any unauthorized access to Customer Data, of which Ruckus is aware, as soon as reasonably practical upon Ruckus's confirmation of the access. As the owner and collector of the Customer Data, Customer shall be solely responsible for any further communication or announcement regarding any unauthorized access to Customer Data to any individuals or other entities to which the Customer Data pertains or relates, or any governmental, law enforcement, or regulatory authorities having, or purporting to have, jurisdiction over the Customer Data (each a "Governmental Authority") in compliance with all applicable laws; provided, however, that Ruckus shall have the right (but, as between Ruckus and Customer, not any obligation) to provide any legally required notifications regarding any unauthorized access and to cooperate with, or provide information about the Service or the Customer Data to, any Governmental Authority in accordance with applicable laws.

f) Restrictions. Customer will not, and will not permit any third party to: (1) modify, copy, or otherwise reproduce the Service in whole or in part; (2) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code form or structure of the code used in the Service; (3) provide, lease or lend the Service to any third party except as expressly authorized hereunder; (4) remove any proprietary notices or labels displayed on the Service; (5) modify or create a derivative work of any part of the Service; (6) use the Service for any unlawful purpose; (7) interfere with or disrupt the integrity or performance of the Service or third-party data contained therein; (8) attempt to gain unauthorized access to or breach the security mechanisms of

the Service or its related systems or networks; (9) permit direct or indirect access to or use of any Service in a way that circumvents the Scope of Use; (10) access any Service or Content in order to build a competitive product or service or (11) disclose the results of any benchmarking of the Service (whether or not the results were obtained with assistance from Ruckus) to any third party. The Service is not designed, intended, authorized or warranted to be suitable for use in connection with any high risk, mission critical or strict liability activity (including, without limitation, air or space travel, aircraft navigation systems, aircraft communication systems, air traffic control, weapons systems, operation of nuclear facilities and other power plants, military or space equipment requiring radiation hardened components, life support applications, devices or systems or other medical operations, and Enhanced 911 or the E911 emergency calling system). Any such use by Customer is solely at Customer's risk. TO THE MAXIMUM EXTENT ALLOWED BY LAW, CUSTOMER SHALL INDEMNIFY RUCKUS FROM ANY LIABILITY ARISING OUT OF OR RELATED TO CUSTOMER DATA, OR CUSTOMER'S USE OF THE SERVICE IN CONTRAVENTION OF THE TERMS OF THIS AGREEMENT.

g) Proprietary Rights. As between Ruckus and Customer, Ruckus, and its suppliers, own all rights, title and interests in and to the Service and Documentation, including all improvements to the foregoing. If the Service includes software provided by a third party, that software is governed by the applicable third party license. All rights not expressly granted to Customer are reserved by Ruckus.

3) Fees & Payment.

In the event that Customer is purchasing the Service licenses from a Ruckus Channel Partner, then the payment terms shall be exclusively as defined between such Ruckus Channel Partner and Customer. In the event that Customer is purchasing access to the Service directly from Ruckus, then Customer shall pay the fees stated in the Order within thirty (30) days of the date of the applicable Ruckus invoice. All payment obligations, including for the length of a Service Term or volume-based fees relating to Scope of Use, are non-cancelable and nonrefundable. Customer acknowledges that a

failure to pay the applicable fees (either to Ruckus directly or to a Ruckus Channel Partner) may result in Ruckus suspending Customer's access to the Service, without prejudicing the rights of any party for remedies of a breach of contractual obligations. Delinquent invoices are also subject to interest of 1.0% per month on any outstanding balance, or the maximum permitted by law, whichever is less, plus all expenses of collection. All fees owed by Customer in connection with this agreement are exclusive of, and Customer shall pay, all sales, use, excise and other taxes that may be levied upon Customer in connection with this agreement, except for employment taxes and taxes based on Ruckus's net income.

4) Support and Services.

a) Technical support services during the Service Term are included in the subscription fees for the Service (as set forth in an Order) and shall be provided in accordance with the technical support information set forth on the Service Portal.

b) Ruckus Cloud MSP are required to deliver onsite support and First (1st) call support. Ruckus will provide Level 2+ support to the Cloud MSPs only on those products sold by Ruckus Cloud MSP in the territory and only for the term of this Agreement.

However, if the Cloud MSP uses spares or components which have not been purchased through a Ruckus authorized distributor, support offered on that unit will no longer be valid.

c) Any additional services, including consulting or training, shall be provided on an as-quoted basis and subject to a separate Order.

d) Technical support services are available to Ruckus Customers and not the End Users without prior approval from Ruckus Technical Assistance Center

e) Ruckus Cloud MSP acknowledges that Cloud MSP End Users do not have the right to contact Ruckus support directly. Person acknowledging this terms and conditions understands this.

5) Training

a) Ruckus Cloud Specialization Training Program. Cloud MSP shall undertake cloud specialization training. All associates responsible for supporting End User support are encouraged to maintain adequate level of training

b) Ruckus Cloud Training Requirements. Cloud MSP shall undertake, at its own cost and expense, all training and certification necessary to meet the compliance requirements for Ruckus Cloud specialization. Cloud MSP will designate the required amount of personnel for initial and ongoing training.

6) Term & Termination

a) Term. This agreement commences as of the date the parties execute the initial Order and continues until the end of the Evaluation Term or Service Term as applicable, unless otherwise terminated earlier as provided for in this agreement. To ensure uninterrupted use of the Service, you must place an Order to renew the Service Term no less than ninety (90) days prior to the expiration of the then current Service Term. Any Service Term renewal shall be subject to the then current terms applicable to the Service, including pricing, which terms will be provided to you by Ruckus or the applicable Ruckus Channel Partner at the time of your Order.

b) Termination for Cause. Either party may terminate this agreement and any licenses granted hereunder (1) for cause upon thirty (30) days written notice to the other party of a material breach of this agreement if such breach remains uncured at the expiration of such period; (2) either party ceases to do business as an operating concern; or (3) Customer is finally adjudged as financially insolvent, makes an assignment for the benefit of creditors, or files for bankruptcy which is not dismissed within sixty (60) days

following the filing. Except as provided herein, Customer hereby waives its right to unilaterally terminate this Agreement pursuant to Article 2125 of the Civil Code of Quebec.

c) Effect of Termination. Termination will not relieve Customer of the obligation to pay any fees due or payable to Ruckus (or a Ruckus Channel Partner, as applicable) prior to the effective date of termination, including any other fees or payments that Customer has committed to under this agreement. Upon termination of this agreement, all rights and licenses granted by Ruckus hereunder shall immediately terminate. The provisions of this agreement that by their nature extend beyond the expiration or other termination of this agreement will survive and remain in effect until all obligations are satisfied. Ruckus will make a file of the Customer Data (as it exists on the effective date of termination) available within 30 days of termination if Customer so requests in writing at the time of termination; provided, that Customer acknowledges Ruckus has no obligation to retain any Customer Data more than 30 days beyond termination, and may delete such Customer Data thereafter. Customer is solely responsible for any data retention requirements under applicable law.

7) Warranties

a) Warranty. During the Service Term, Ruckus warrants that the Service when used in accordance with the Documentation, will operate in all material respects substantially as set forth in the Documentation. If Customer notifies Ruckus of any breach of the foregoing warranty, Ruckus's sole obligation and Customer's exclusive remedy shall be for Ruckus to, at its option, (a) provide an error correction or update to the Service to remedy the failure; or (b) terminate the applicable Service license and provide a prorated refund of fees paid by Customer for the Service. This warranty and the remedies offered are applicable only if: (i) the failure is reasonably reproducible by Ruckus; (ii) Customer reports the failure with reasonable specificity in writing within thirty (30) days from its occurrence; and (iii) Customer provides Ruckus with reasonable assistance in the diagnosis and remedy of the failure.

b) DISCLAIMER OF ALL OTHER WARRANTIES. EXCEPT AS EXPRESSLY PROVIDED IN SECTIONS 4 AND 7(a), AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICE AND DOCUMENTATION ARE PROVIDED "AS IS" AND "AS AVAILABLE", AND RUCKUS AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE. RUCKUS DOES NOT WARRANT THAT THE SERVICE MEETS CUSTOMER'S REQUIREMENTS OR THAT USE OF THE SERVICE WILL BE SECURE, UNINTERRUPTED OR ERROR-FREE. SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO CUSTOMER. THESE WARRANTIES GIVE CUSTOMER SPECIFIC LEGAL RIGHTS AND CUSTOMER MAY HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE OR JURISDICTION TO JURISDICTION.

8) Intellectual Property Infringement

Ruckus agrees to defend Customer and pay any damages finally awarded or, at its option settle and pay any settlement agreed to by Ruckus, with respect to any claim made or brought against Customer by an entity unaffiliated with Customer alleging that Customer's use of the unaltered Service infringes or misappropriates any U.S. patent, copyright or trademark of such entity, provided that Customer (a) provides prompt written notice of such claim to Ruckus, (b) grants Ruckus the sole right to control and defend such claim, and (c) provides Ruckus, at Ruckus's expense, with all information and assistance reasonably requested by Ruckus in the defense of such claim. In the event of such a claim or threatened claim, Ruckus may, at its option, (i) provide Customer with revised Service that is substantially equivalent to the accused Service in functionality in material respects but is non-infringing, (ii) obtain the right for Customer to continue using the Service, or (iii) terminate this agreement upon 30 days' notice and refund any license fees previously paid for the Service that is the subject of a claim on a pro-rata basis for the remaining portion of the Service Term.

Notwithstanding the foregoing, Ruckus shall have no obligation or liability with respect to (a) use of the Service in combination with any materials not provided by Ruckus, if the infringement would be avoided by use of the Service without such combination, (b) any alleged patent infringement related to the implementation of a standard; (c) any modification of the Service by any party other than Ruckus, (d) any open source code contained within the Service, (e) damages based on the value of product, services or business methods not provided by or performed by Ruckus, (f) any use of the Service outside the scope of the license or (g) any use of the Service after Ruckus has terminated access to the Service. THIS PARAGRAPH REPRESENTS THE SOLE AND EXCLUSIVE LIABILITY OF RUCKUS AND THE EXCLUSIVE REMEDY OF CUSTOMER FOR INFRINGEMENT OR MISAPPROPRIATION OF THIRD PARTY RIGHTS.

9) Limitation of Liability.

RUCKUS AND ITS SUPPLIERS SHALL NOT UNDER ANY CIRCUMSTANCES BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, ANY LOSS OF PROFITS, BUSINESS, DATA OR REVENUES, OR THE COSTS OF REPLACEMENT OR SUBSTITUTE PRODUCTS, ARISING FROM THE PURCHASE, USE OR INABILITY TO USE THE SERVICE, WHETHER IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), EVEN IF RUCKUS HAS BEEN INFORMED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. RUCKUS'S TOTAL AGGREGATE LIABILITY FOR DAMAGES OF ANY NATURE, REGARDLESS OF THE FORM OF ACTION, IS LIMITED TO AN AMOUNT EQUAL TO THE FEES PAID BY THE CUSTOMER DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT(S) GIVING RISE TO LIABILITY HEREUNDER. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN LIABILITY, SO THE ABOVE LIMITATION OF LIABILITY MAY NOT APPLY TO CUSTOMER.

10) RUCKUS AND ITS SUPPLIERS SHALL NOT UNDER ANY CIRCUMSTANCES BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, ANY LOSS OF PROFITS, BUSINESS, DATA OR REVENUES, OR THE COSTS OF REPLACEMENT OR SUBSTITUTE PRODUCTS, ARISING FROM THE

PURCHASE, USE OR INABILITY TO USE THE SERVICE, WHETHER IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), EVEN IF RUCKUS HAS BEEN INFORMED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. RUCKUS'S TOTAL AGGREGATE LIABILITY FOR DAMAGES OF ANY NATURE, REGARDLESS OF THE FORM OF ACTION, IS LIMITED TO AN AMOUNT EQUAL TO THE FEES PAID BY THE CUSTOMER DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT(S) GIVING RISE TO LIABILITY HEREUNDER. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN LIABILITY, SO THE ABOVE LIMITATION OF LIABILITY MAY NOT APPLY TO CUSTOMER.

11) General Provisions

a) Governing Law; Venue. The laws of the State of California, excluding its conflict of laws provisions, will govern the validity, construction and interpretation of this agreement. The parties consent to the exclusive jurisdiction and venue of the state courts located in Santa Clara County, California, and the federal courts for the Northern District of California, for any action arising hereunder.

b) Export Requirements. Customer agrees that the Service and Documentation are subject to the Export Administration Regulations of the United States. Customer agrees not to export, re-export or transfer, directly or indirectly, the Service, Documentation or any technical data acquired from Ruckus, or any products utilizing such data, in violation of the United States export laws, regulations and controls.

c) Force Majeure. Notwithstanding any provision contained in this agreement, neither party will be liable to the other to the extent the fulfillment or performance of any terms or provisions of this agreement are delayed or prevented by revolution or other civil disorders; wars; strikes; labor disputes; electrical supply or availability failure; fires; floods; acts of God; government action; or, without limiting the foregoing, any other causes not within its control and which, by the exercise of reasonable diligence, it is unable to prevent. This section will not apply to the payment of any sums due under the agreement by either party to the other.

d) Miscellaneous. Notices will be deemed given on the day actually received by the party to whom the notice is addressed. The relationship of Ruckus and Customer is that of independent contractors. Neither party has any authority to act on behalf of the other party or to bind it, and in no event will the parties be construed to be partners, employer-employee or agents of each other. Headings in this agreement are for reference purposes only and will not affect the interpretation or meaning of this agreement. If any provision of this agreement is held by an arbitrator or a court of competent jurisdiction to be contrary to law, then the remaining provisions of this agreement will remain in full force and effect. No delay or omission by either party to exercise any right or power it has under this agreement will be construed as a waiver of such right or power. A waiver by either party of any breach by the other party will not be construed to be a waiver of any succeeding breach or any other covenant by the other party. All waivers must be in writing and signed by the party waiving its rights. This agreement may not be assigned by Customer by operation of law or otherwise, without the prior written consent of Ruckus, which consent will not be unreasonably withheld. This agreement may be executed simultaneously in any number of counterparts, each of which will be deemed an original, but all of which together constitute one and the same agreement. The parties agree that electronic signatures are valid signatures for enforcement of this agreement. This agreement constitutes the entire agreement between Ruckus and Customer with respect to the subject matter hereof. This agreement supersedes all prior negotiations, agreements and undertakings between the parties with respect to such subject matter. No modification of this agreement will be effective unless contained in writing and signed by an authorized representative of each party. Notwithstanding applicable law, electronic communications will not be deemed signed writings. Any additional orders for Service hereunder shall be governed by the terms of this agreement. No term or condition contained in Customer's purchase order or similar document will apply unless specifically agreed to by Ruckus in writing, even if Ruckus has accepted the order set forth in such purchase order, and all such terms or conditions are otherwise hereby expressly rejected by Ruckus. In the event of a conflict between this agreement and any

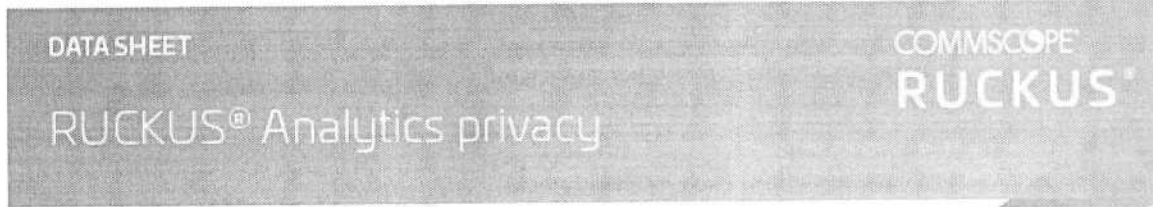
other applicable agreement, this agreement shall govern, unless otherwise expressly stated.

e) Language. It is the express wish of the Parties that this agreement and any related documents be drawn up in English. Il est la volonté expresse des Parties que cette convention et tous les documents s'y rattachant soient rédigés en anglais.

ATTACHMENT B
RUCKUS PRIVACY POLICY

Privacy Policy located at <https://www.commscope.com/about-us/privacy-statement/>

ATTACHMENT C Ruckus Analytics Privacy Data Sheet



BENEFITS

- Provides comprehensive visibility into network operations
- Accelerates network and client troubleshooting
- Identifies, prioritizes and recommends remediation steps for service issues
- Helps IT teams improve the user experience
- Works with your RUCKUS network to automatically validate service levels
- Processes and stores information in regional cloud data centers
- Data center protected by state-of-the-art firewalls
- Data, passwords, keys, and tokens encrypted at rest and in transit
- 24x7x365 support

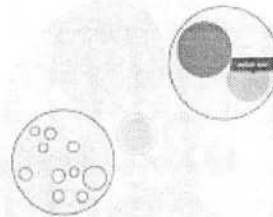
CommScope engaged and consulted independent data privacy risk management provider TrustArc® to understand and interpret GDPR guidelines. RUCKUS® is a business unit of CommScope. The purpose of this document is to provide customers of CommScope with information needed to assess the impact of the RUCKUS Analytics service on their overall privacy posture by detailing how personal information may be captured, processed and stored by and within the service.

RUCKUS ANALYTICS OVERVIEW

RUCKUS Analytics from CommScope is a cloud service for network analytics and assurance. Powered by machine learning (ML) and artificial intelligence (AI), it helps customers get the most from their RUCKUS network. The service gives IT comprehensive visibility into network operations. It accelerates troubleshooting and helps IT teams meet their network service-level agreements (SLAs).

The service identifies service assurance incidents, classifies them by severity, traces root causes, and makes specific recommendations for remediation. It automatically monitors network health relative to configurable thresholds. Advanced client troubleshooting and incident analytics give IT teams the power to address service issues for individual users and devices.

RUCKUS Analytics works with the customer's RUCKUS network to allow it to self-validate—without the need for overlay sensors. IT teams can identify and address many service issues even before they affect users. The service also includes robust reporting and informative dashboards, including the ability to create custom dashboards. The Data Explorer tool allows rich data visualizations and flexibility to explore the network data warehouse with drag-and-drop ease.



This detail from the main dashboard shows a circle packing chart. It provides a graphical representation of the network hierarchy, with color coding that indicates where network incidents have occurred. You can easily zoom in for a closer view by clicking on an area of the chart.

The RUCKUS Analytics service offers two additional means for its customers to get support. RUCKUS customers can invite RUCKUS technical support to help resolve issues with the service. Customers can revoke access at any time before or after the incident has been resolved. In addition, RUCKUS customers can delegate management tasks to trusted partners—also called value-added resellers (VARs). RUCKUS Analytics offers tools to its customers to securely invite, as well as revoke, access to authorized partners.

INFORMATION PROCESSED BY RUCKUS ANALYTICS

RUCKUS Analytics aggregates raw data and automatically transforms it into deep insight into network operations. The high-performance data pipeline ingests and processes the data to serve as the basis for queries, reports and baseline metrics. Raw data insights, reports and metrics are stored in a cloud data center secured by state-of-the-art firewalls. For the Europe region, RUCKUS Cloud uses Google Cloud data centers hosted in Frankfurt, Germany. Access to this information is limited to authorized users over authenticated and encrypted connections. All data, passwords, pre-shared keys or security tokens are encrypted at rest and in transit. RUCKUS Analytics balances data minimization principles with ensuring continued service delivery and the ability to recover from catastrophic failures.

This section describes the information processed by RUCKUS Cloud, which can be broadly separated into the following categories:

CUSTOMER INFORMATION

The main purpose of RUCKUS Analytics is to give IT comprehensive visibility into network operations and accelerate troubleshooting. RUCKUS Analytics helps IT teams meet their network service-level agreements (SLAs).

RUCKUS Analytics is a multi-tenant service and achieves complete separation of customer data by using principles of multi-tenancy in the cloud. To achieve this, RUCKUS Analytics collects basic customer information such as customer name, organization and email address to set up secure authenticated and authorized access to Cloud so customers can access this service from

anywhere over the internet and view their own account. This information is stored in the RUCKUS customer relationship management (CRM) system. The RUCKUS Analytics service may also inform the customer about upcoming maintenance updates or license expiration by email. RUCKUS uses third-party service providers for specific services.

EXTERNAL SERVICE PROVIDERS

RUCKUS Analytics uses the following external service providers for various purposes to deliver and enhance the service:

- Google Cloud Platform™—Google Cloud Platform hosts and delivers service from the cloud. Google Cloud Platform and its suite of software are GDPR compliant. See [here](#) for [more information](#).
- Email service provider—Amazon Simple Notification Service™ and Simple Queue Service™ send alerts and notifications for all customers who elect to receive updates over email. Link to [Amazon GDPR](#).
- Pendo®—Pendo application analytics service measures and enhances user experience. Link to [Pendo GDPR policy](#).

NETWORK INFORMATION

RUCKUS Analytics is designed for the unique data profile generated by network devices. On-premises controllers or RUCKUS Cloud securely connects to the RUCKUS Analytics service and streams lightweight health key performance indicators (KPIs) and telemetry. RUCKUS Analytics collects configuration and statistics to offer these features:

- Automated data baselining and insights driven by machine learning (ML) and artificial intelligence (AI)
- Health and SLA monitoring
- Powerful, holistic troubleshooting
- Automatic classification of incident severity
- Webhooks for integration with helpdesk IT service management (ITSM) systems like ServiceNow and Salesforce
- Service validation without the need for an on-site data collector or overlay sensors
- Melissa—AI-powered virtual network assistant

- Granular access to raw data with deep exploration and custom dashboards
- Twelve months of storage with flexible data reporting

END-CLIENT INFORMATION

End clients connect to wired or wireless networks at the venue. As part of using the service, the network learns basic networking information such as unique MAC address, IP address, user name (if using an 802.1X authentication), hostname, device OS type, type of network, connected AP MAC address, RF information, switch name, switch port, zone or venue, amount of data uploaded or downloaded, applications used, and inventory of

devices deployed in the network and their operational status. This raw data is securely tunneled to the RUCKUS Analytics service where it is aggregated, processed, and automatically transformed into deep insight into the network operations. All data collected is encrypted at rest and in transit.

GUESTS USING CAPTIVE PORTAL

When guest users connect to RUCKUS networks using captive portal services, their endpoint information is treated just like all other end-client information described above and tunneled to RUCKUS Analytics service.

PURPOSE OF INFORMATION PROCESSED BY RUCKUS ANALYTICS

The table below describes the purpose of information processed by RUCKUS Analytics.

CATEGORY	PURPOSE	MAY BE CONSIDERED OR CONTAIN PERSONALLY IDENTIFIABLE INFORMATION
Customer Information	To set up, securely access, troubleshoot and measure user experience of the RUCKUS Analytics service	Yes
Network Information	To set up, securely access, troubleshoot and measure user experience of the RUCKUS Analytics service	Yes
End-client Information	To deliver and maintain reliable RUCKUS Analytics service and provide customer support, if required	Yes
Guest Information	To deliver and maintain reliable RUCKUS Analytics service and provide customer support, if required	Yes

WHO CONTROLS INFORMATION PROCESSED BY THE RUCKUS ANALYTICS SERVICE? WHICH, IF ANY, THIRD PARTIES HAVE ACCESS TO THIS INFORMATION?

Information processed by RUCKUS Analytics is controlled by the RUCKUS customer. For ease of management, RUCKUS customer administrators may add other employees as administrators or invite a third-party RUCKUS-authorized partner to manage the RUCKUS Analytics service. Customers can add, delete or modify administrators at any time or revoke access to third-party administrators. In case of trouble, a customer administrator can invite CommScope/RUCKUS tech support for help with troubleshooting and revoke access at any time. CommScope/RUCKUS tech support access is always an explicit request by the RUCKUS customer.

CATEGORY	CONTROLLER OF DATA	IS THIS SHARED BY THIRD PARTIES?	MAY BE CONSIDERED OR CONTAIN PERSONALLY IDENTIFIABLE INFORMATION
Customer Information	RUCKUS customer	<ul style="list-style-type: none"> Specific information may be shared with third-party service providers if authorized by customers Shared with CommScope-authorized VAR if authorized by customer Email address may be shared with Amazon Web Services™ for the purposes of email notification RUCKUS tech support if requested by customer 	Yes
Network Information	RUCKUS customer	<ul style="list-style-type: none"> Shared with CommScope-authorized VAR if authorized by customer Incident information is shared with ITSM systems over webhooks if configured by the customer Customer query is shared with Google natural language understanding platform. RUCKUS tech support if requested by customer 	Yes
End-client Information	RUCKUS customer	<ul style="list-style-type: none"> Shared with CommScope-authorized VAR if authorized by customer RUCKUS tech support if requested by customer 	Yes
Guest Information	RUCKUS customer	<ul style="list-style-type: none"> Shared with CommScope-authorized VAR if authorized by customer RUCKUS tech support if requested by customer 	Yes

HOW LONG DOES RUCKUS ANALYTICS RETAIN DATA?

CATEGORY	DURATION
Customer information	Stored per CommScope record retention policy
Network Information	For the duration of service
End-client Information	Up to 12 months
Guest Information	Up to 12 months

If an EU citizen or data subject, as defined by GDPR, reaches out to a CommScope/RUCKUS customer to retrieve data stored in RUCKUS Analytics, the CommScope/RUCKUS customer is responsible for establishing if the data-subject enquiry is genuine. The RUCKUS Analytics team has tools to retrieve and provide information stored for the data subject. Typically, the customer will need to provide a key attribute such as data-subject email address or MAC address. RUCKUS Analytics will build self-service tools for its customers to purge data in the future.

RUCKUS ANALYTICS PRIVACY POLICY AND TERMS AND CONDITIONS

The RUCKUS Analytics [privacy policy](#) and [terms and conditions](#) are posted on an easily-accessible RUCKUS support site. All RUCKUS Analytics customers must read and accept the terms and conditions before starting the service. For visitors accessing the public CommScope website, the privacy and cookies statement is found [here](#).

HOW DOES RUCKUS ANALYTICS ADDRESS BREACH OF DATA OR INFORMATION?

Customer trust, data security and integrity are of utmost importance to CommScope/RUCKUS. CommScope/RUCKUS recognizes that improving security is an ongoing process and we are committed to implementing changes to improve the overall security posture of the products and services we offer. The gaps we have identified and continue to identify will be addressed and we continually explore enhancing our infrastructure, including that of our partners, or leveraging new partners that can meet or exceed our demands for security and privacy. CommScope/RUCKUS has a dedicated product security team that is responsible for researching, analyzing and responding to security incident reports related to RUCKUS products. This team is the first point of contact for all security incident reports and works directly with RUCKUS customers, security researchers, government organizations, consultants, industry security organizations and other vendors to identify security issues with RUCKUS products. This team is also responsible for publishing security advisories and communicating with outside entities regarding mitigation steps for addressing specific security issues with RUCKUS products. The RUCKUS security incident response policy can be found at this [link](#).

PHYSICAL ACCESS AND ADMITTANCE CONTROL

RUCKUS Analytics has the ability to deny unauthorized persons access to data processing systems in which customer data is processed. RUCKUS Analytics accomplishes this by:

- Using state-of-the-art data centers and data processing systems that are protected by firewalls. The European data center is hosted in an EU region. The EU service is accessible at <https://eu.RUCKUS.cloud/analytics>. Currently, RUCKUS Analytics uses state-of-the-art Google Cloud data centers hosted in Frankfurt, Germany.
- Requiring secure account credentials to access systems.
- Putting in place account security protections (strong passwords and maximum number of failed attempts).
- Using software development life cycle and change management/change control policy and processes.
- Restricting customer data access to personnel based on appropriate business need and limiting it by functional role.

ACCESS CONTROL

RUCKUS Analytics has the ability to prevent data processing systems from being used without authorization. This is accomplished by:

- Using software development life cycle and change management/change control policies and processes.
- Restricting customer data access to personnel based on appropriate business need and limiting it by functional role.

DATA ACCESS CONTROL

RUCKUS Analytics has the ability to ensure that persons authorized to use systems in which customer data is processed have access only to the customer data to which they are entitled in accordance with their access rights and authorizations, and to prevent the unauthorized reading, copying, modification or deletion of customer data. This is accomplished by:

- Restricting customer data access to personnel based on appropriate business need and limiting it by functional role.
- Putting log retention policies and procedures in place.

DATA TRANSFER CONTROL

RUCKUS Analytics has the ability to prevent the unauthorized reading, copying, modification or deletion of customer data—which is processed by the RUCKUS Analytics service while customer data is being transferred electronically, transported or recorded on data storage devices—and to ensure that the intended recipients of customer data who are provided with customer data by means of data communication equipment can be established and verified. This is accomplished by:

- Encrypting communication between RUCKUS access point, controllers, cloud and RUCKUS Analytics, and transporting it over HTTP/SSL.
- Logging the activity of administrators (time, IP of logged-in administrators).
- Storing (at rest) account passwords in encrypted format on RUCKUS Analytics systems.
- Storing and processing data in Europe cloud data center hosted in Frankfurt, Germany.

INPUT CONTROL

RUCKUS Analytics has the ability to ensure it is possible to establish an audit trail as to when and by whom customer data has been entered, modified or removed from systems being used by (or on behalf of) RUCKUS Analytics to process customer data. This is accomplished by:

- Logging the activity of administrators (time, IP of logged-in administrators).
- Restricting customer data access to personnel based on appropriate business need and limiting it by functional role.
- Putting session timeouts in place.

ORDER/INSTRUCTION CONTROL

RUCKUS Analytics has the ability to ensure that customer data processed by or on behalf of RUCKUS Analytics can only be processed in accordance with the customer's instructions. This is accomplished by:

- Using change management, including change logs and change event alerting.
- Putting log retention policies and procedures in place.

AVAILABILITY CONTROL

RUCKUS Analytics has the ability to ensure the protection of customer data, which is under the control of RUCKUS Analytics, against accidental destruction or loss. This is accomplished by:

- Backing up RUCKUS Analytics systems data periodically, every 15 minutes.
- Storing all data in a highly available, highly durable manner in Google Cloud Platform.

INTENDED USE CONTROL

RUCKUS Analytics has the ability to ensure that customer data collected is only used for the intended purpose under the agreement. This is accomplished by:

- Using customer data exclusively to deliver and improve features and functionality available in the RUCKUS Analytics service.
- Automatically processing customer data according to the specific features enabled by the customer and as required to secure and maintain the infrastructure.
- Putting log retention policy and procedures in place.

ADDITIONAL MEASURES

OUT-OF-BAND ARCHITECTURE

Data stored or transmitted by means of the customer's network do not traverse RUCKUS Analytics servers. Lightweight health KPI metrics about the network usage are sent to and processed in RUCKUS Analytics to generate insights about network operation.

CLOUD SERVICES SECURITY

Cloud services are protected via state-of-the-art multi-layered security infrastructure hosted by Google Cloud Platform. See [here](#) for more information.

- Operational and device security.
- Internet communication security.
- Strongly authenticated identity for services and personnel.
- Purpose-built hardware and software for networking with customer security chips on every machine for hardened secure infrastructure.

CLOUD SERVICES INFRASTRUCTURE

RUCKUS Analytics uses Google Cloud Platform to deliver services. Google Cloud Platform and its suite of software are GDPR compliant. See here for [more information](#).

DISASTER PREPAREDNESS

- Hot backup is available, and all data is backed up at 15-minute intervals.
- All data is stored in a highly available, highly durable manner in Google Cloud Platform.

ORGANIZATION AND PERSONNEL

- Rapid escalation procedures across multiple operations teams are in place.
- The RUCKUS NOC is available 24x7x365 days to monitor and respond.

EXAMPLES OF INFORMATION PROCESSED BY RUCKUS ANALYTICS

CATEGORY	INFORMATION PROCESSED BY RUCKUS ANALYTICS	WHO HAS ACCESS?	EXAMPLES	MAY BE CONSIDERED OR CONTAIN PERSONALLY IDENTIFIABLE INFORMATION
Customer Information	Customer name, customer organization name, address, email address, phone number	RUCKUS order processing, DevOps, customer support engineer if required. Third-party service providers: • CommScope uses third-party service providers for specific services. CommScope has agreements in place to not share phone numbers and email addresses outside of the specific service delivery goals. • Amazon Web Services (AWS)—RUCKUS products use AWS email services to send alerts and notifications for all customers who elect to receive updates over email.	Name: "John Smith" Organization: Acme Inc. Email: John.smith@acmeinc.com	Yes
Network Information	Zone or venue or place of business, access point MAC address, model, WLAN information, switch MAC address, model, topology	RUCKUS customer support team if requested by customer; authorized partner if requested by customer; RUCKUS DevOps engineering for maintenance and continued service delivery	Zone/Venue name: Acme HQ Address: Acme Inc. 123 Infinity Way, 94024, CA MAC address: 04:68:4D:22:F2:40 Model: R610 WLAN information: SSID guest-Wi-Fi Authentication: captive portal Switch model: 7150 Switch port: 1/1/10	Yes
End-user or client Information	MAC address, user name, device type, OS, application used, traffic metrics, RSSI/SNR, date and time of connection or disconnection, connected/wired port	RUCKUS customer support team if requested by customer; authorized partner if requested by customer; RUCKUS DevOps engineering for maintenance and continued service delivery	MAC address: 04:68:4D:22:F2:40 WLAN information: SSID guest-Wi-Fi Authentication: captive portal Switch model: 7150 Switch port: 1/1/10	Yes

ABOUT THIS DATA SHEET

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc® has not undertaken an independent audit and does not certify the information contained in this data sheet. However, the information contained herein was believed to be accurate and complete as of the time this data sheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.



commscope.com

Visit our website or contact your local Commscope representative for more information.

© 2021 Commscope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of Commscope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to Commscope products or services. Commscope is committed to the highest standards of business integrity and environmental sustainability with a number of Commscope's facilities across the globe certified in accordance with international standards, including ISO 9001, TL 9000 and ISO 14001. Further information regarding Commscope's commitment can be found at www.commscope.com/About/Our/commitment-to-environmental-sustainability

TM-015883-EN 03/20