celona

Celona Data Privacy FAQ

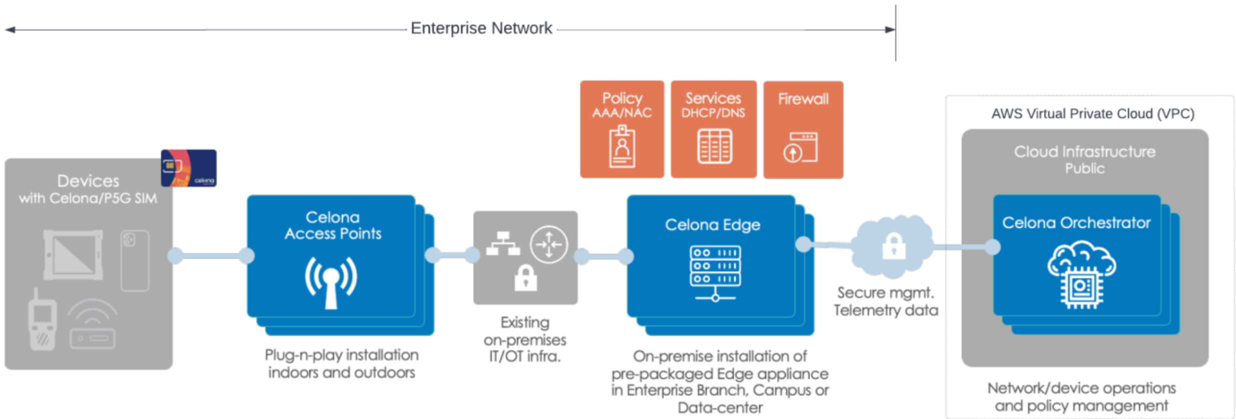
Celona platform enables a highly secure, cloud-native hardware & software stack required to deploy and operate private 4G & 5G networks.

Contents

Introduction

Celona delivers a highly secure, cloud-native hardware & software stack required to deploy and operate private 4G and 5G networks. Celona's solution architecture provides all components required to bring a secure private mobile network to life:

- Celona Access Points - Specifically engineered for indoor and outdoor 4G/5G enterprise use cases and operating environments, Celona Access Points (APs) deliver pervasive coverage, interference-free access, and unmatched wireless performance. Easy to deploy, Celona APs are managed and monitored through Celona's cloud-based Orchestrator platform as part of a complete private 4G/5G turnkey solution.
- Celona Edge Appliance – The Celona Edge Appliance is a physical server delivered as part of Celona's solution that is specially designed to run Edge OS, a scalable and resilient cloud-native network operating system.
- Celona Orchestrator - Orchestrator is a cloud-based network administration platform that centrally coordinates the deployment, management, and operation of the Celona 5G LAN solution. This includes configuration and optimization of network elements, subscriber management, and defining and automating the enforcement of QoS policies for individual applications and devices.



We recognize that sometimes attorneys, contract professionals, and/or procurement specialists may have questions that not easily answered by a privacy policy and contract documents. We hope that these FAQs will be a useful resource.

This resource does not form part of your agreement with Celona whether or not attached to your agreement. It is provided for reference purposes only, and does not create any warranties or obligations on the part of either party.

FAQ

What does the Celona solution do?

Celona delivers a highly secure, cloud-native hardware and software stack used by customers to deploy and operate private 4G and 5G cellular networks. Celona enables enterprise devices to connect to private 4G and 5G cellular networks using SIM and electronic SIM (“eSIM”) cards. These devices rarely include personal devices but more commonly are company issued devices like tablets, handheld barcode scanners, and other industrial devices such as autonomous mobile robots, autonomous guided vehicles, manufacturing robots, and security cameras (“Connected Devices”).

Does the Celona solution collect personal information?

Celona’s solution collects a small amount of personal data from customer administrators (“User Data”) and may collect information from Connected Devices using the Celona network if the devices are linked to an individual (“Device Data”). When a customer administrator registers for the solution, User Data includes the administrator’s personal data in the form of contact information, including name, email, company name, and company address. Celona also collects the IP address of these administrator and other users when they log into Orchestrator.

Device Data collected from Connected Devices includes data such as IMSI, IMEI, SIM ID, ICCID, as well as IP address. While Device Data may be deemed personal when associated with a device used by an individual, because these Connected Devices are not ordinarily tied to an individual user, this data may not always be personal data. If the Connected Devices are tied to an individual, the data may constitute personal data. Further, because Celona does not have linked subscriber identifier information such as subscriber name (which is assigned by and/or maintained by cellular carriers), Celona would not be able to identify a particular subscriber using only the identifiers in its possession at any given point in time.

Celona may also collect network packet information such as LTE control messages (part of the S1AP protocol) upon a customer’s request, which may in certain cases include personal data if the Connected Device is a personal device (“Packet Data”). Such packet information is collected from the Edge Appliance and is limited only to the information passing through the Edge Appliance.

User Data, Device Data, and Packet Data are referred to collectively as “Customer Personal Data.”

The solution does not require and Celona does not collect any sensitive or special categories of data as defined in data protection laws.

How does Celona use Customer Personal Data?

Celona uses Customer Personal Data to provide the solution, including to:

- Enable customer administrators to create Orchestrator accounts for themselves and others.
- Permit Connected Devices that are linked to an individual to connect to APs.
- Using Orchestrator, empower customers to manage its 4G or 5G network and the Connected Devices' use of the network.
- Provide technical support in the event customers would like Celona to review Packet Data to assist in resolving a support ticket.

What privacy protections does Celona utilize?

The Celona solution implements the following privacy-protective features:

- The solution does not collect any information from individuals' Connected Devices other than Device Data discussed above. For example, the solution does not collect a list of apps installed on a Connected Device, the real-time location of Connected Devices, or the name of a Connected Device.
- Only minimal User Data is collected, and it is only used to provision and manage accounts for customer users.
- Packet Data is only collected in connection with a support request and only upon a customer's authorization in each case.
- Access by customers and Celona personnel to components of the solution containing Customer Personal Data is subject to access controls and logging, as set forth below.
- Celona does not link Connected Devices with subscriber identifier information such as subscriber name (which is assigned by and/or maintained by cellular carriers).

Where is Celona Orchestrator hosted?

Celona Orchestrator is hosted in a two-tier dedicated AWS Virtual Private Cloud (VPC) and Google Cloud Platform VPC in the United States. Celona personnel who require access to

Customer Personal Data may be located in the European Economic Area and India but are subject to the same security measures no matter their location.

What security measures are employed for Celona Orchestrator?

Amazon Web Services (AWS) and Google Cloud Platform (GCP)

Celona Orchestrator's backend infrastructure is hosted in AWS and GCP availability zones and regions that meet the following standards:

- SOC 1, Attestation Standard Section 801 (formerly SSAE 16)
- SOC 2 / SOC 3, Attestation Standard Section 101

Data centers that house the infrastructure feature state-of-the-art physical & cyber security with reliable designs and strict access policies. More information is available on the following websites:

  - AWS Security Website
  - AWS overview of security processes
  - Google Cloud Compliance Resource Center
  - Google Cloud Trust and Security Website

Encryption and Other Security Measures

Celona continually reviews its security and strengthens its protections to implement additional measures where appropriate.

- Customer Personal Data in transit and at rest in AWS and GCP is encrypted. Encryption keys for data at rest in AWS is provided by the AWS Key Management Service and encryption keys for data at rest in GCP is provided by the GCP Keystore.
- All external connections to Orchestrator connect to the application using SSL.
- Celona Edge Appliances and APs strictly enforce server certificate validation and all Edge(s) and APs are authenticated with the device's client certificates.
- Security controls are enabled for Celona engineers accessing the production environment.

What access controls are in place for the Celona solution?

- Access controls for access by customers

    - Customers have the ability to control access to Celona Orchestrator using the principle of least privilege and role-based access controls.
    - Orchestrator also supports User administration and Identity management via Single sign-on (SSO), using the customer's Identity Provider (IdP).
- Access controls for access by Celona
    - Only Celona personnel with a business need to access the Celona Edge and APs have access.
    - Access to backend servers is strictly controlled by role-based access via multi-factor authentication (MFA) including user certificate, MFA token, and passphrase.
    - All access to backend production servers is logged. Access to the Orchestrator by Celona personnel is also logged. Celona personnel have access to the AWS and GCP accounts only on a strictly as-needed basis with identity access management controls, logging, and periodic (quarterly) reviews.

What are Celona's data retention practices for Orchestrator?

- Celona retains Customer Personal Data for so long as a customer has an active account with Celona and will delete Customer Personal Data 90 days after a customer terminates their agreement for the Celona solution or after their agreement expires without renewal.
- Celona can delete Customer Personal Data at any time upon a customer's written request.
- Upon deleting a customer user's account, Celona will delete their related User Data.
- Celona may retain Customer Personal Data in aggregated or de-identified form for longer periods provided such data no longer identifies the customer.

How does Celona comply with data protection laws?

Celona is committed to protecting Customer Personal Data in accordance with applicable privacy laws around the world and has implemented a global data protection program.

European Data Protection Laws

- Celona is a data processor and its customers are the data controllers under the GDPR and similar laws.

- Celona limits its access to and use of Customer Personal Data as set forth above.
- Celona's Data Processing Agreement ("DPA") incorporates the European Commission's Standard Contractual Clauses and required terms from the GDPR and other similar laws.
- Celona built Orchestrator to incorporate the following data protection principles:
    - Proportionality, Fairness, and Transparency: Processing takes place in accordance with agreements entered into by customers and Celona. Celona promotes transparency by providing documentation about the Celona solution which supports customers' evaluation of whether they would like to provide notices to or obtain consents from data subjects.
    - Purpose Limitation: Celona processes Customer Personal Data as instructed by its customers to provide the solution.
    - Data Minimization: By default, the solution collects only the information required to provide and maintain the solution.
    - Storage Limitation: Celona limits retention of Customer Personal Data as set forth above.
    - Integrity and Confidentiality: The solution employs robust security measures to protect Customer Personal Data as described above.
    - Data Portability: Customers may export certain data from Orchestrator.
    - Data Subject Requests: Orchestrator enables customers to fulfill certain data subject requests on their own, and for any other requests, Celona is available to assist customers.

International Data Transfers

- Please see details above under the heading "Where is Celona Orchestrator Hosted?"
- Celona complies with international cross-border data transfer protections as set forth in the EU Standard Contractual Clauses.
- Not only does Celona have a Government Disclosure Request policy that covers both government requests for personal information, subpoenas, and other related requests, but Celona's DPA also includes commitments regarding Celona's handling of government requests for personal information.

References

- Data Processing Agreement
- Security FAQ
- Privacy Policy

Conclusion

As highlighted above, Celona's solution processes minimal personal data, and any personal data collected is only processed to provide the Celona solution. Celona implements robust security and access control measures to help protect Customer Personal Data and has strict data retention processes. Celona's Data Processing Agreement is designed to align with global data protection laws that apply to Celona and its personal data processing activities.