Network as Code (NaC) API Privacy Transparency Notice

This Notice describes how the above designated Product processes Personal Data when Nokia acts as a data processor. It provides the information relevant to assess and document privacy relevant aspects of the use of this Product when integrated in your application. This Notice and the relevant terms of the Nokia NaC Privacy Policy are the authoritative statements relating to the Personal Data processing activities and privacy regulatory compliance aspects associated with the use of this Product.

About this Notice

Product (s) covered by this notice:	1. Device Location APIs (location retrieval, location verification, geofencing) 2. Quality of Service on Demand APIs 3. Specialized networks APIs (Network slicing) 4. Network Insights APIs 5. Sim Swap API 6. Number verify API 7. Device Status APIs (Roaming, Connectivity)

Prior versions of this Notice as applicable to earlier releases of the Product may be available upon request. Where this Notice references other Products marked with an asterisk (*), please refer to the separate Notices of such Products.

About the Product

APIs are offered as a SaaS product on Nokia's "Network as Code" aggregator platform that offers a collection of network APIs from various CSPs (Communication Service providers) globally. These APIs provide seamless integration experience for enterprises to consume network APIs and abstract the complexity of these APIs from enterprise developers.

NaC platform remains a data processor whenever it processes data on behalf of the enterprise or CSP. For example, when Personal Data* such as subscriber mobile number is provided by an enterprise as API request parameters, enterprise is a data controller and NaC product is a data processor and CSP will become a data sub-processor. When Personal Data is provided as API response parameters from CSP to NaC API product, CSP is data controller and NaC product is a data processor, and enterprise will become data sub-processor. NaC product follows instructions provided by respective data controllers to manage Personal Data.

For more information on the purpose, features and technical characteristics of the Product, please refer to the documentation at Documentation | Network as Code.

Product Type:	API
Delivery Model:	SaaS

About the Processing Operation(s) performed by / for the purpose(s) of the Product

Core Features:	☒ This product must process Personal Data to Deliver its core feature(s)

***Personal Data** means any data that, either alone or when combined with other dataset, can directly or indirectly identify an individual. Such data shall include but not limited to identifiers such as IMSI, IMEI, MSISDN, ICCID, Call Detail Records (CDR), location data (latitude/longitude), Billing Information, Service Usage Data, IP Addresses, device information etc.

	☐ This product does not require processing any Personal Data to deliver its core feature(s)
Categories of Personal Data processed:	☐ Non-sensitive Personal Data ☒ Sensitive Personal Data ☐ Not applicable
High Risk Activities:	☐ This product profiles individuals based on personal characteristics ☐ This product automates decision making that produces legal or other significant impact on individuals ☒ Not applicable

The Product is designed to protect confidential information. Such confidential information typically includes Personal Data of a CSP subscriber. Privacy by design approach is followed during development and maintenance of this product. This product is implemented based on data minimization principles and does not process or store data which is not required for delivering API services. This product has implemented security controls like data at rest encryption, data at transit encryption, role-based access controls, integrity protection, intrusion detection, and incident response plans to protect data from unauthorized access, breaches, and loss.

This product does not store and process data other than intended use and does not retain data as necessary by law and regulations applicable to the product. However, this product may use anonymized personal data for analytics purposes. The Product is designed to consider typical compliance objectives under major privacy laws and regulations such as the EU GDPR. Customers should seek qualified legal advice tailored to their specific requirements when deploying, configuring and using this Product in their environment.

About the Personal Data processed by / for the purpose(s) of the Product

API Name	Categories of Personal Data	Categories of Data Subjects	Purpose(s) of Processing	Categories of Data Recipients	Needed for Core Features (Y/N)	Nokia acts as a Processor
All APIs	Device identifier (Phone no, IP address, Network access identifier)	Device identifier	device identification for all API services to route the request towards right CSP	Enterprise application	Y	Yes
Location retrieval, Location verification and geofencing API	Device location (Latitude, Longitude, Civic address)	Subscriber's device location	To verify or retrieve device location	Enterprise application	Y	Yes
Device status	Roaming status, connectivity status	Device status	To identify connectivity status of a device	Enterprise application	Y	Yes
Roaming status	Device roaming status	Device status	To identify roaming	Enterprise application	Y	Yes

***Personal Data** means any data that, either alone or when combined with other dataset, can directly or indirectly identify an individual. Such data shall include but not limited to identifiers such as IMSI, IMEI, MSISDN, ICCID, Call Detail Records (CDR), location data (latitude/longitude), Billing Information, Service Usage Data, IP Addresses, device information etc.

			status of a device			

Presently this product is deployed in AWS or GCP's US and EU locations; however, it can be deployed in CSPs or API consumer's regional location if it is mandated by a law or regulation for data sovereignty requirements.

These APIs may require explicit user consent or Opt-in as required by local regulations and law applicable based on application use case, and API scope and purpose. As Nokia remains a data processor in all cases, respective data controllers may choose a method of their choice to get the consent from their subscribers (data subject) before sharing the data via NaC platform.

About managing the Personal Data processed by / for the purpose(s) of the Product

Privacy Enhancing Technologies

Subject to more detailed information provided in the Product description and other customer literature e.g. on optional Product settings and configurations available, the Product has the following technical and organizational capabilities to enhance and protect the privacy of the Personal Data it processes:

Privacy Objective:	**Privacy Enhancing Measures**	**Data at Rest**	**Data in Transit[b]**
Confidentiality	Access Control Encryption	☒ ☒	NA ☒
Integrity	Change logging	☒	NA
Availability	Disaster Recovery measures Business Continuity measures	☒ ☒	NA NA
Incidents	Detection Response mechanisms	☒ ☒	☐ ☐
Certification(s)	SOC2 Type II	Compliant	

[b]Data in transit encompasses traffic between client systems and NaC endpoints.

Data Subject Rights

The Customer can manage the Personal Data stored on customer premises and submit a support request to amend, rectify or delete data transmitted to the hosted cloud-based Product application. Nokia, as a data processor, will act on these requests as instructed by the data controller.

Nokia will assist the data controller in responding to Data Subject Access Requests (DSARs) by providing the necessary tools and support to access, rectify, or delete Personal Data as required by applicable data protection laws.

Personal Data Retention Schedule

Personal Data which the Customer transmitted to the hosted cloud-based Product application is purged when the Customer's tenant is deleted upon termination of the service.

About Regulatory Compliance Matters

Data Processing Addendum

*__Personal Data__ means any data that, either alone or when combined with other dataset, can directly or indirectly identify an individual. Such data shall include but not limited to identifiers such as IMSI, IMEI, MSISDN, ICCID, Call Detail Records (CDR), location data (latitude/longitude), Billing Information, Service Usage Data, IP Addresses, device information etc.

Where your use of the Product or of related services involves Nokia acting as a Data Processor on your behalf, the rights and obligations of both parties with respect to such Personal Data processing, including as regards disclosures and cross-border transfers of Personal Data to and/or by Nokia and any of their sub-processors, are defined in the applicable Data Processing Addendum available at https://developer.networkascode.nokia.io/legal/data-processing-addendum.

Sub-Processing

The specific sub-processor(s) involved in the delivery of this Product can be found below:

- AWS US northeast and Germany
- GCP US and Germany

This list is subject to change in accordance with the statutory requirements and contractual terms applicable.

*__Personal Data__ means any data that, either alone or when combined with other dataset, can directly or indirectly identify an individual. Such data shall include but not limited to identifiers such as IMSI, IMEI, MSISDN, ICCID, Call Detail Records (CDR), location data (latitude/longitude), Billing Information, Service Usage Data, IP Addresses, device information etc.