

PUBLICATION 1 SERVICE DESCRIPTION FOR IOT MANAGED GLOBAL CONNECTIVITY: IOT CONNECT ADVANCED SERVICES, OPTION INTERNET ON THE MOVE

1.1 Service Definition

This Managed Global Connectivity: IoT Connect Advanced Option Internet on the Move Service Description, relating to the Internet on the Move Service ("IoT Service"), complements the IoT Connect Advanced Service Description and cannot be dissociated from it. The Specific Conditions for IoT Managed Global Connectivity: IoT Advanced Services, Option Internet on the Move (B2B2C Mode) shall apply to this Service Description.

Capitalized terms used and not otherwise defined in this Service Description will have the meanings ascribed to them in the Specific Conditions for IoT Managed Global Connectivity: IoT Advanced Services, Option Internet on the Move (B2B2C Mode) or elsewhere in the Agreement.

1.2 Service Overview

The IoT Service is an option for the IoT Connect Advanced Service, which option provides Internet access for Users using a dedicated APN.

The IoT Service includes the following elements:

The ability to separate Consumer Connectivity using the IoT Service from Customer Connectivity using the IoT Service, via separate APNs.

The provision of the IoT Service to the Users, whose conditions of use, as part of a Value Added Solution provided by the Customer, are defined in the IoT Terms of Use. The IoT Terms of Use are defined and provided by Orange to the Customer, who must include them, without any modification of any kind (except for purely editorial purposes subject to Orange's prior review), in the User Terms and Conditions of the Value Added Solution sold to the Users by the Customer.

1.3 User Management and Required User Identity Personal Data

In order for Orange to comply with the regulatory obligations of an electronic service provider towards individual consumers, the Customer is required, before activating and using the IoT Service and when creating an Account, to:

- (a) **Perform a Standard User Personal Data Collection Process:** formally identify the Users through the collection of the User's Personal Data and information related to the Users;
- (b) Perform a **User Identity Check Process** (visual recognition of the correspondence between the User and their identification document); or
- (c) Perform an **ID Cross-Check Process** (online verification via a certified tool of the validity of the identification document provided by the User).

The Customer accepts and acknowledges that in any of cases (a), (b), or (c), before activating the IoT Service when creating an Account, Customer must share and communicate to Orange the required User identity Personal Data, as defined in Table 1.

1.3.1 Standard User Personal Data Collection Process (a)

In the event that, according to local legislation, Personal Data collection is sufficient to identify a User before activating the IoT Service, the Customer must follow the Standard User Personal Data collection process. This process consists of the Customer sharing with Orange the required User identity Personal Data, as defined in Table 1. This sharing of the required User identity Personal Data can be performed, at the Customer's choice, via the API (included in the Service) or via a specific User portal hosted by Orange (an additional optional paid functionality offered by Orange). The specific User portal will be hosted by Orange on behalf of the Customer. The Customer must request its Users to enter directly on this portal the required User identity Personal Data defined in Table 1. When all fields are completed, the User identity Personal Data will be recorded by Orange in the Orange Database, after which the Customer can proceed with the activation of the IoT Service.

1.3.2 User Identity Check Process (b)

In some cases, local legislation may require a User Identity Check of the User's identity Personal Data before activating the Service. In those cases, the Customer must follow the User Identity Check process. The User Identity Check is a process to verify the User's identity using visual information through human inspection. This includes analyzing a government-issued User identity document and an in-person visual inspection for comparison. The Customer must perform the User Identity Check process by establishing a human process whereby the identity data declared by the User and the data on a government-issued User identity document are compared.

In this scenario, the Customer can still use the Orange IoT API to identify the required Users' Personal Data as defined in Table 1 and activate the IoT Service. However, all User identification Personal Data shared with Orange by the Customer via the API for the creation of the User Account shall be deemed verified by the Customer and conforming to the User Identity Check requirements set forth by local legislation. Hence, for countries with the User Identity Check requirement, Orange considers that the Customer has performed the User Identity Check process before sharing the required User identity Personal Data, as defined in Table 1, via the API with Orange. By using the API option, the Customer agrees to these conditions.

1.3.3 ID Cross-Check Process (c)

In the event the Customer cannot implement or guarantee the proper implementation of a User identity check process when and where required, an alternative option exists, which is the implementation of an ID Cross-Check. An ID Cross-Check is a software-based analysis and comparison between a photo of a government-issued User identity document and the identity Personal Data provided by the User. The benefit of this system is that it can be performed remotely, without the need for an in-person visual inspection guaranteed by the Customer.

The ID Cross-Check software can be developed by the Customer or licensed by the Customer through Orange or through a third party.

If the Customer sources the ID Cross-Check (an additional optional paid functionality offered by Orange) through Orange, the ID Cross-Check can be performed, at the Customer's choice, via the API or a specific User portal hosted by Orange (an additional optional paid functionality offered by Orange). The specific User portal will be hosted by Orange on behalf of the Customer. The Customer must request its Users to enter directly on this portal the required User identity Personal Data, as defined in Table 1. When all fields are completed, the ID Cross-Check will be performed. When the User identity is confirmed, the required User identity Personal Data, as defined in Table 1, will be recorded by Orange in the Orange Database, after which the Customer can proceed with the activation of the IoTM Service.

In case the ID Cross-Check is not sourced through Orange, all the required User identity Personal Data, as defined in Table 1, shared with Orange by the Customer via the API for the creation of the User Account shall be considered verified by the Customer and conforming to the ID Cross-Check requirements set forth by local legislation.

Hence, for countries with the User ID cross-check requirement, Orange considers that the Customer has performed the ID Cross-Check process before sharing the required User identity Personal Data, as defined in Table 1 via the API with Orange. By using the API option, the Customer agrees to these conditions.

For the purpose of streamlining the User identification process, it is always possible to implement an ID Cross-Check process for countries where it is not required by local legislation.

In the following list of countries (this list may change due to regulatory changes), Personal Data Standard Collection (a) is sufficient:

Bulgaria	Hungary	Czech Republic	Denmark	Ireland	Finland	France
Norway	Poland	Portugal	United Kingdom	Spain	Sweden	Netherlands

The Customer can send the required User identity Personal Data, as defined in Table 1, via the API to Orange or, as an option, route the User to the IoTM Portal where the User will enter the required User identity Personal Data, as defined in Table 1.

In this second list of countries (this may change due to the regulatory changes) Personal Data Standard collection is not sufficient and the Customer must perform an Identification Check process (b) and send data to Orange, or as an option, can delegate the performance of a Cross-Check process (c) to Orange via API or via the IoTM Portal.

Austria	Belgium	Greece	Germany	Switzerland
Italy**	Luxembourg	Romania	Slovakia	

** In addition, regulation in Italy requires the storage of the User's identification document.

In all cases, it is the Customer's responsibility to ensure the required User identity Personal Data, as defined in Table 1, shared with and held by Orange is complete and correct. The Customer, having the relationship with the Users, is responsible during the entire Account duration to transfer immediately to Orange any request for modification of a User's Personal Data of which the Customer becomes aware.

The User's Personal Data related to Account creation, modification, or deletion is transmitted to Orange by the Customer having the relationship with the Users to Orange via the API or collected via the IoTM Portal, as an option. The User's Personal Data collected by the Customer is transmitted to Orange and hosted in the Symphonie database used by Orange for the processing of Personal Data related to the IoTM Service.

The required information may include the User Personal Data described in Table 1, depending on the applicable local laws.

Table 1: User (Consumer) Personal Data

Data	Comment	For Activation of a User Account	For Notification of Consumption Thresholds
customer.id	OEM consumer.id	X	
customer.creation_date	consumer creation date "2019-06-20T14:10:07.516Z"	X	
customer.cancellation_date	Mandatory when the consumer is cancelled	X	
customer.gender	gender of consumer mandator value : M, F	X	
customer.first_name	Consumer first name	X	

Data	Comment	For Activation of a User Account	For Notification of Consumption Thresholds
customer.name	Consumer family name	X	
customer.street1	Consumer's address line 1	X	
customer.postCode	Consumer's zip code	X	
customer.city	Consumer's city	X	
customer.country	Consumer Country code. ISO 3166-1 alpha 2 (http://en.wikipedia.org/wiki/ISO_3166-1)	X	
customer.type_document	Consumer type of identity document Value :passport/identity/drivingLicence/residenceCard	X	
customer.document_id	id of identity document	X	
contract.state	Account state : value : inUsed (Active), onHold (Suspended), cancelled	X	
contract.creation_date	Account creation date "2019-06-20T14:10:07.516Z"	X	
contract.cancellation_date	Mandatory when the contract is cancelled.	X	
simCard.id	ICCID (Integrated Circuit Card Identifier) of SIM card	X	
simCard.msisdn	MSISDN (Mobile Station International Subscriber Directory Number) of the sim card	IMSI or MSISDN or ICCID must be set	
simCard.imsi	IMSI (International Mobile Subscriber Identity) of the sim card		
device.imei	Equipment IMEI (International Mobile Equipment Identity)	X	
sim.activation_date	Activation date of the SIM "2019-06-20T14:10:07.516Z"	X	
device.id	Device id in which is the SIM card (e.g. for a car VIN)	X	X
device.type	Type of Equipment in which is the SIM card [car/dongle/laptop]	X	X
service.id	consumer identifier of the service customer generally mail address	X	
service.type	Service code value : data	X	
service.activation_date	Service's activation date "2019-06-20T14:10:07.516Z"	X	
service.suspension_date	Suspension date of the service. Mandatory when the contract is suspended.	X	
contact.Mode	Value SMS, Email		X
contact.Email	mail used to notify		X
contact.phone	phone used to notify		X
Contact.notification	threshold choice 100, intermediate, timeout		X

1.4 Consumer Connectivity Management

After the User has an active Account, the Customer can, through the IoTM Portal or through API, create or delete buckets of data plans ("Buckets") allocated to a User for accessing the IoTM Service.

A Bucket is defined as a quantity of data transmitted over the Internet for a defined duration that may or may not be renewable, and within a defined Territory.

It is the responsibility of the Customer to inform the User, through its Terms and Conditions, about the available or chosen level of service (National IP or Simplified Solution) for the User's country of residence as described below. The list of available options per country is specified in Clause 1.10 Territories.

1.5 National IP option (Geographical Contextualization)

Local public IP addresses are associated with the Users depending on their country of residence. This mechanism allows a User, whatever their geographical location within the scope of use of the IoTM Service, to access the Internet of their country of residence.

1.6 Simplified Solution (Without Geographical Contextualization)

When the National IP option is not chosen by the Customer or is not available in the User's country of residence, the User will have access to French National IP addresses only.

1.7 Service Implementation

To deploy the IoTM Service, and upon ordering, the Customer will select the IoT Service Management 'Managed Intense' option (subject to specific charges). The Orange dedicated project manager will coordinate the actions within Orange.

1.8 IoTM Business Portal and API

The IoTM Portal is a web-based application to which the Customer or the User connects via HTTPS (Hypertext Transfer Protocol Secure) using a dedicated login and password. The IoTM Portal exists in different versions depending on the ordering process chosen by the Customer.

The IoTM Portal can also be replaced by the Customer's own portal, connected to Orange information systems via the API (Application Programming Interface). The API allows the Customer's applications to have visibility and control over the Service. The API environment is fully part of the Service delivery cycle.

The API is built upon common web services standards, keeping integration efforts to a minimum and allowing the Customer to immediately control key aspects of connected solutions. The API allows the Customer to develop the integration of its choice: business logic and enterprise security standards ensure the Customer's communications data are available only to the Customer, directly in the Customer's information system, such as a CRM or ERP system. The Customer has the help of the API user guide to develop its integration, test it safely, and put it into production.

1.9 Territories

The IoTM Service permits registration associated with the National IP option for Users located in the following countries:

Austria	Belgium	Bulgaria	Czech Republic
Denmark	Finland	France	Germany
Greece	Hungary	Ireland	Italy
Luxembourg	Netherlands	Norway	Poland
Portugal	Romania	Slovakia	Spain
Sweden	Switzerland	United Kingdom	

When registered and having an active Bucket, the User can use the Service in their country of location but also when traveling within the complete perimeter (as defined in this Clause 1.10):

1.10 Helpdesk

Level 1 User support is provided in the local language by the Customer. Any related concerns regarding the IoTM Service will be escalated to Orange by the Customer. This may cover:

- (a) IoTM Portal Availability
- (b) IoTM Service Availability
- (c) User Registration Concern
- (d) User Subscription Information
- (e) User Connectivity Service Expiry

Orange provides the Customer with a complete tutorial dedicated to the Portal in order to train the Customer's helpdesk staff and provides access via the IoTM Portal to a tool allowing Level 1 Customer support to address User requests.

1.11 Processing when Customer acts as a Controller and Orange as a Processor.

The Parties agree that the Customer is the Controller and Orange is the Processor in respect of the Personal Data ("**Customer Personal Data**") that is made available by the Customer to Orange to provide the IoTM Service.

The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Customer Personal Data, and the categories of Data Subjects are set out in the relevant description of the processing activities ("**Description of Processing**"). The Description of Processing of Personal Data by Orange as Processor and the Customer as Data Controller is described in Exhibit A.

Customer will ensure that it has provided adequate notices (including by reference to Orange Privacy Policy) and has obtained, where required, all necessary and valid consents to enable lawful transfer of the Customer Personal Data to Orange for the purposes set out in this Article. Customer will not by act or omission cause Orange to be in breach of the Data Protection Legislation.

When acting as Processor:

- (a) Orange will only process Customer Personal Data in accordance with the reasonable written instructions of Customer, unless required otherwise by applicable law, lawful government authority or applicable court, and in such case, Orange will notify Customer in advance (unless Orange is prohibited by law from doing so).

- (b) In accordance with the then-current industry practice, Orange will implement appropriate technical and organizational security measures to protect Customer Personal Data against unauthorized or unlawful Processing and against accidental loss or destruction, or damage, appropriate to the harm that might result from the foregoing and the nature of the Customer Personal Data to be protected, considering the state of technological development and the cost of implementing any such measures.
- (c) Orange will assist Customer in responding to reasonable requests from Data Subjects for the exercise of their rights under the Data Protection Legislation in respect of Customer Personal Data. The persons authorized by Customer to request Orange's assistance in respect of Data Subjects' requests are Customer's authorized user(s) of My Service Space.
- (d) Orange will assist Customer, at Customer's cost, with Customer's compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators, upon Customer's written request, insofar as is possible, reasonable and proportionate.

1.12 Sub-Processing

Customer hereby grants its consent to the Processing of Customer Personal Data by Affiliates and/or subcontractors of Orange engaged in the performance of the Contract, some of whom may be based outside the European Economic Area (EEA) or in a country without an adequacy decision from the EU Commission (the "**Sub-processors**"). The approved Sub-processors are listed on the My Service Space portal (Welcome Page\Get Help\General Data Protection). If Customer does not have access to the My Service Space portal, the list of approved Sub-processors will be made available as set out in the Description of Processing provided by Orange. Orange is responsible for the sub-processing and performance of its Sub-processors in accordance with the requirements of the Data Protection Legislation and will ensure that such sub-processing will be on terms substantially equivalent to those in this Article.

Orange will inform Customer of changes or additions of Sub-processor(s), which will be deemed approved by Customer unless Customer objects to such change within fifteen (15) days of having been informed thereof. Any objection must be made in writing to Orange with detailed reasons. Orange will consider Customer's objection in its sole discretion and will inform Customer of its decision. If Orange still requires a change to the approved Sub-processors, Orange will provide at least one alternative proposal, including any additional costs, to Customer for its implementation. If Customer fails to accept either option within fifteen (15) days from the date of Orange's alternative proposal, the change to the Sub-processor proposed by Orange with the least cost to Customer will be deemed approved. Orange will require that its employees, Sub-processors and each of their employees will keep Customer Personal Data confidential.

Where Orange transfers Customer Personal Data outside the EEA or to a country without an adequacy decision from the EU Commission, Orange will provide appropriate safeguards by using the standard contractual clauses for the transfer of Personal Data to Processors established in third countries approved by the European Commission (the "SCC") or another appropriate safeguard.

During the duration of this Contract, Orange will:

- (a) on thirty (30) days prior written notice from Customer, provide to Customer reasonably and readily available information to demonstrate its compliance with this Article and this Appendix; and
- (b) on sixty (60) days prior written notice from Customer, agree to schedule an audit that Customer may conduct at Customer's cost, provided that:
 - (i) audits are subject to Orange's data protection and security policies and any other measures needed to protect the confidentiality of Orange or its customers' data;
 - (ii) the audit is subject to a mutually agreed audit plan, detailing the scope and conditions of the audit;
 - (iii) the audit does not exceed two days and does not disrupt Orange's operations; and
 - (iv) there is no more than one audit in any rolling twelve-month period.

Orange will notify Customer without undue delay when it becomes aware of a Personal Data Breach of Customer Personal Data.

At Customer's request upon the expiration or termination of the Contract, Orange will delete or return to Customer all the documents and files containing Customer Personal Data after the end of the provision of Services relating to Processing, and will not retain any copy of the Customer Personal Data.

EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE AS PROCESSOR FOR CUSTOMER

This Description of Processing applies to the Processing of Customer Personal Data for the provision of **Internet on the Move**.

Nature of the Processing Activities	Customer Personal Data are processed to provide the Service in accordance with the Service Description or as further instructed by Customer. Processing operations include collection, consultation, transfer, storage, and deletion of Customer Personal Data, as well as other Processing activities in accordance with the configuration and options of the Service, such as recording, organization, modification, combination, pseudonymization or anonymization.		
Subject Matter of the Processing Activities		Duration	
Activating, implementing, delivering and managing the Service. Incident management and support, including changes.		For the necessary period to provide the Service plus 12 months.	
In accordance with the Service Description and the options selected:			
Reporting, i.e. reports on billing, usage, quality of service and other reports if and as required by the Customer.		As per Service Description or Customer instructions.	
Portals, i.e. providing access and use of portals, on-line tools and other applications managed by Orange as part of the provision of its Services.		As long as necessary for the provision of the Service.	
Types of Customer Personal Data to be Processed	Contact Data: first name, last name, language, email address, business address and telephone numbers, job role within the Customer. Usage Data: the usage related data to the extent related to natural persons, that Orange collects from services it provides to its Customers. Support Data: Customer representative or end user service ticket information (including feedback, comments or questions) and if applicable, Customer representative or end user telephone recordings for incident. Identity Data: first name, last name, honorific (e.g. Ms, Mr. Dr., etc.), username or similar identifier. Technical Data: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, as well as other technology on the devices natural persons use to access areas of Orange portals, or other technical data generated through the use of the service.		
Categories of Data Subjects	Employees of Customer, of its affiliates and of their customers and partners. If applicable, other individuals using the Service.		
Authorized Sub-Processors	Orange Business Affiliates and suppliers in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Service. The authorized sub-processors engaged only for the Service are listed below. The authorized sub-processors engaged for centralized support or services provided in connection with the Service are communicated separately to Customer.		

	Authorized Sub-Processors in the EU		Authorized Sub-Processors Outside of the EU	
	Name	Country of the Contracting Entity	Name	Country of the Contracting Entity
Orange Business Affiliates	Orange SA W-Ha	France France	Equant Mauritius Holdings Ltd (Orange Business Mauritius Indian Ocean Service Center)	Mauritius
External Suppliers	Aeris Communications SAS	France		

**END OF SERVICE DESCRIPTION FOR IOT MANAGED GLOBAL CONNECTIVITY:
IOT CONNECT ADVANCED SERVICES, OPTION INTERNET ON THE MOVE**