## 1.1 Business VPN Internet

### 1.1.1 Overview and Definitions

(a) The Business VPN Internet is an optional and billable feature of the Business VPN Service, provides the Users of the Business VPN Service with access to the Internet by integrating the Internet access and the Intranet traffic through a single Tail Circuit and single CE router. The breakout to the Internet is implemented either within the Orange Internet Network (as hereinafter defined) or at the access connection supplied by the local ISP (as defined below), depending on the type of Internet Profile (as hereinafter defined) purchased by Customer. Depending also on the Internet Profile purchased by Customer, the access to the Internet is secured via:

(i) a Customer-provided and managed dedicated firewall;

(ii) an Orange-provided and managed dedicated firewall that can be purchased by Customer, and provided by Orange, as a separate and billable Service;

(iii) a virtual firewall hosted at the Orange-managed CPE Router (as hereinafter defined), or

(iv) a virtual firewall hosted in the Shared Platform (as hereinafter defined).

(b) As used in the context of the Business VPN Internet Service, the following capitalized words shall have the meaning defined below notwithstanding anything to the contrary set forth elsewhere in the Agreement. Capitalized words used but not defined herein will have the meanings ascribed to them in the Service Description or Service Level Agreement for Business VPN or elsewhere in the relevant portion of the Agreement.

"**Committed Service Bandwidth**" means the service bandwidth purchased by Customer in respect to each Business VPN Corporate connection. For clarity, the Committed Service Bandwidth does not include the Internet bandwidth for the Business VPN Internet Service, which Customer must purchase in addition to the Committed Service Bandwidth.

"**Inbound Internet Traffic**" means the Internet session is initiated by the source of the Internet traffic from the Internet into Customer's Location where the Business VPN Internet Service is provided.

"**ISP**" means the local Internet service provider.

"**Orange-managed CPE Router**" means the CE router for the Business VPN Service that is installed by Orange at Customer's Location as an Orange-owned and managed CPE device.

"**Orange Internet Network**" means the Orange backbone network that provides: (a) the Internet Protocol ("**IP**") internetworking, and (b) the Business VPN Internet Users with connectivity to the Internet. The Orange Internet Network excludes Tail Circuits, public networks (e.g. Internet, public WiFi, etc.) and CPE devices.

"**Outbound Internet Traffic**" means the Internet session is initiated by the source of the Internet traffic from the Location where the Business VPN Internet Service is provided.

"**Shared Platform**" means the Orange point of presence ("**PoP**") in the Orange Internet Network where the virtualized firewall environment for the Browsing Internet Profile (and for the Content Internet Profile, but only if Customer purchases the virtual firewall feature) is hosted.

### 1.1.2 Internet Profiles

The Business VPN Internet is segmented into two (2) profiles, namely the Browsing Internet Profile and the Content Internet Profile (collectively, "**Internet Profiles**"):

(a) **Browsing.** The Browsing Internet Profile is designed for a Business VPN Location that mainly has Outbound Internet Traffic, and such Internet Profile includes an Orange-managed virtual firewall hosted in either the Shared Platform (in the case of Distributed Breakout) or the Orange-managed CPE Router (in the case of Local Breakout). The Browsing Internet Profile is further split into the Local Breakout feature and the Distributed Breakout feature, and Customer will select which of these Browsing Internet Profile features is appropriate to its needs. The Browsing Internet Profile and its Local Breakout and Distributed Breakout features are described more fully at length in Clause 1.1.3 and Clause 1.1.4 below.

(b) **Content.** The Content Internet Profile is designed for a Business VPN Location that needs full bi-directional Internet traffic (i.e. Inbound Internet Traffic and Outbound Internet Traffic). The Content Internet Profile provides Customer with the following three (3) firewall options:

(i) Customer can purchase an Orange-managed virtual firewall, which is hosted in the Shared Platform;

(ii) Customer can provide and manage its own dedicated firewall appliances; or

(iii) Customer can purchase a dedicated Orange-managed firewall service, which Orange will provide as a separate and billable Service via its Secure Gateway Service offering.

### 1.1.3 Browsing Internet Profile – Local Breakout

(a) **Browsing Local Breakout Overview.** The Browsing Local Breakout provides the Users of the Business VPN Service with access to the Internet. Breakout to the Internet occurs at the access connection supplied by the local ISP instead of going through Customer's MPLS (i.e. Business VPN) network. Access to the Internet is secured via the Orange-managed virtual firewall located in the Orange-managed CPE Router.

(b) **Implementation of Local Breakout.** Using the access circuit supplied by the ISP for the Business VPN Small connection, a split tunneling is implemented to off-load the Internet traffic directly onto the Internet. The breakout point to the Internet occurs at the access circuit provided by the ISP.

(c) **Business VPN Site Profile.** The Local Breakout option of the Browsing Internet Profile is available only for Business VPN Locations that have either:

(i) a Business VPN Small or Business VPN Small Off-net as their Business VPN Site Profile, and such Locations are connected to the Orange Network (i.e. the Orange backbone network used by Orange to deliver Business VPN Service) via an IPSec tunnel over the Internet (such tunneling protocol also referred to as "**Small-Based Internet Access**"), or

(ii) Business VPN Corporate as their Business VPN Site Profile and such Locations are equipped with a secondary access circuit using either an off-net access or a Small-Based Internet Access.

(d) **Security Features.** Orange will implement a virtual firewall in the Orange-managed CPE Router, as described in Clause 1.1.6 (Security Features Firewall Overview) below. CPE software and hardware leveling may be required, as described in Clause 1.1.6(c) (Leveling Requirements and Customer Security Policy Request). Inbound Internet Traffic to the Business VPN Small Location or Business VPN Small Off-net Location is not supported, and no off-load IPsec tunnel can be established to or from other Business VPN Locations.

(e) **Restrictions.** The Local Breakout does not act as an Internet gateway for other Business VPN Locations, and it does not allow the prioritization of traffic.

(f) **Reporting.** Customer will be able to see via the My Service Space portal the security policy implemented by Orange in the virtual firewall hosted in the Orange-managed CPE Router, as well as the security events and the security logs. The Local Breakout includes a proactive monitoring of the firewall for UDP/TCP port scan, TCP SYN attack, TCP non-SYN First packet, and rules rejection.

(g) **Geographical Coverage.** Unless prohibited by law or regulation, Local Breakout option is generally available in countries where Orange provides Customer with Business VPN. However, the availability of the Local Breakout will be confirmed by Orange at the time of the order.

(h) **Charges.** The Charges for the Local Breakout feature consist of one-time installation charge and monthly recurring charges per Location. These Charges are in addition to the Charges for the Business VPN Service and for the customized configuration of the firewall implemented in the Orange-managed CPE Router.

1.1.4 **Browsing Internet Profile – Distributed Breakout**

(a) **Browsing Distributed Breakout Overview.** The Browsing Distributed Breakout provides Users with Internet access through the Shared Platform.

(b) **Implementation.** Using the Business VPN Small access circuit or the Business VPN Corporate access circuit, the Outbound Internet Traffic is transported via Customer's MPLS (i.e. Business VPN) network to the closest Shared Platform to minimize the traffic latency. The Outbound Internet Traffic is secured through the virtual firewall hosted in the Shared Platform as it goes though the Orange Internet Network.

For Business VPN Corporate Location, Customer must subscribe to an Internet bandwidth in addition to the Committed Service Bandwidth; however, for clarity, the total Business VPN Service's port bandwidth is the sum of the Committed Service Bandwidth and the Internet bandwidth. The sum of the Committed Service Bandwidth and the Internet bandwidth cannot exceed the Business VPN Corporate's access speed. The Internet traffic is classified in the sixth (6th) Class of Service (i.e. the Internet Class of Service) in order to maintain the priority of the Business VPN data (i.e. D1, D2, and D3 COS) traffic.

(c) **Availability of Browsing Distributed Breakout According to Business VPN Site Profile.** Browsing Distributed Breakout is generally available for Locations that have either a Business VPN Corporate connection or a Business VPN Small connection. However, the actual availability of the Browsing Distributed Breakout will vary from country to country, and the availability of this Browsing feature will be confirmed by Orange at the time of the order.

The Browsing Distributed Breakout feature is further defined by the Site Profile of the Business VPN Service at the Location as follows:

(i) For Locations that have either a Business VPN Small connection or a Business VPN Small Off-net connection, the Internet traffic is transported to the closest Shared Platform to breakout to the Internet.

(ii) For Locations that have a Business VPN Corporate connection with a secondary access using either an off-net access or a Small-Based Internet Access, the Internet traffic can be transported on such secondary (i.e. backup) access circuit. The Internet traffic is transported to the closest Shared Platform to breakout to the Internet. There is no defined Internet bandwidth or Internet Class of Service when the Internet traffic is transmitted via the Small-Based access circuit or the off-net access.

(iii) For Locations that have a Business VPN Corporate connection, the Internet bandwidth is defined on the primary connection, and the primary connection is comprised of the Committed Service Bandwidth and the Internet bandwidth.

(d) **Internet Bandwidth and Business VPN Service Bandwidth Usage Policy**

(i) Solely with respect to Locations that have a Business VPN Corporate connection, and provided that: (A) Customer has purchased a separate Internet bandwidth in addition to the Committed Service

Bandwidth, and (B) the data traffic's Committed Service Bandwidth utilization does not exceed the Committed Service Bandwidth purchased by Customer, Orange will allow the Internet traffic to use the remaining Committed Service Bandwidth. Orange will utilize a data collector tool to sample, in 5-minute intervals, the actual Committed Service Bandwidth utilization for Business VPN data traffic. At the end of the calendar month, Orange will compile the samples by listing the actual Committed Service Bandwidth utilization samples from the highest value to the lowest value. The top five (5%) percent of the highest Committed Service Bandwidth utilization samples are discarded (which means that Customer will not be charged for these traffic bursts), and the next highest utilization sample after the top 5% percent of the highest utilization samples are discarded will become the "**95th Percentile Bandwidth Usage**". If the 95th Percentile Bandwidth Usage in respect to the Business VPN data traffic exceeds the Committed Service Bandwidth, then Orange reserves the right to bill Customer for the excess bandwidth usage (hereinafter, the "**Excess Bandwidth Usage Charge**"), and Customer agrees to pay such additional charge. The Excess Bandwidth Usage Charge will be calculated according to the following formula:

$$\text{Excess Bandwidth Usage Charge} = \left\{ \text{95th Percentile Bandwidth Usage} - \text{Committed Service Bandwidth} \right\} \times \text{Mbps Rate}^{\ddagger}$$

‡ Mbps Rate is the quotient of prevailing Orange megabit per second list price for Business VPN service bandwidth divided by the Committed Service Bandwidth.

Orange may also require Customer, and Customer agrees to comply with such requirement, to increase the Committed Service Bandwidth by purchasing additional service bandwidth for the Business VPN Corporate connection in the event the 95th Percentile Bandwidth Usage chronically exceeds the Committed Service Bandwidth. Orange reserves the right to modify the Business VPN Internet Service to limit the actual traffic load or the 95th Percentile Bandwidth Usage from exceeding the Committed Service Bandwidth.

(ii) Although the Internet traffic may be transported through the Committed Service Bandwidth as described in Clause 1.1.4(d)(i) above, the reverse is not allowed. This means that Customer must only use the Internet bandwidth to transport Internet traffic, not Business VPN data traffic. Orange also reserves the right to modify the Business VPN Internet Service in order to implement measures to limit Customer's ability to transmit Business VPN data traffic through the Internet bandwidth.

(e) **Security Features.** Orange will implement a virtual firewall in the Shared Platform, as described in Clause 1.1.6 below.

(f) **Reporting.** Customers will be able to see via the My Service Space portal the firewall security policy that Orange has implemented in the virtual firewall environment hosted in the Shared Platform, as well as the security events and security logs. The Browsing Distributed Breakout includes proactive monitoring of the firewall for UDP/TCP port scan, TCP SYN attack, TCP non-SYN First packet, and rules rejection. For Locations with Business VPN Corporate connection, Customer will be able to see via the My Service Space portal the Internet traffic with the 6th Class of Service (i.e. the Internet Class of Service) bandwidth utilization, in addition to the current Business VPN IP bandwidth utilization reporting.

(g) **Geographical Coverage.** Unless prohibited by law or regulation, the Distributed Breakout option is generally available in countries where Orange provides Customer with Business VPN. However, the availability of the Browsing Distributed Breakout will be confirmed by Orange at the time of the order.

(h) **Charges.** The Charges for the Distributed Breakout feature consist of one-time installation charge and monthly recurring charges per Location. These Charges are in addition to the Charges for the Business VPN Service. The one-time installation charge includes the implementation of Customer's initial firewall security policy. For Locations with Business VPN Corporate connection, the Charges for the Browsing Distributed Breakout will vary depending on the Internet bandwidth purchased by Customer.

1.1.5 **Content Internet Profile**

The Content Internet Profile is available for the Locations that have Business VPN Corporate connection. The Content Internet Profile integrates the access to the Internet and the Intranet traffic through a single Tail Circuit and the Orange-managed CPE Router.

(a) **Implementation.** Content Internet Profile is provided using a single router with an additional layer-2 connection (i.e. permanent virtual circuit ("**PVC**") or virtual local area network ("**VLAN**")) for the Internet traffic. If Customer provides and manages its own dedicated firewall, then the Orange-managed CPE Router will be connected to such Customer-provided dedicated firewall. As an alternative to providing and managing its own dedicated firewall, Customer may purchase either a separate Orange-managed dedicated firewall service (which Orange will provide through its Secure Gateway service offering) or the Orange-managed virtual firewall service feature hosted in the Shared Platform, and in either case the Orange-managed CPE Router will be connected to the firewall appliance used by Orange for the Secure Gateway Service or to the virtual firewall hosted in the Shared Platform (as the case may be).

(b) **Site Profile Availability.** The Content Internet Profile is only available if the Location has a Business VPN Corporate connection. The availability of the Content Internet Profile will vary from country to country, and Orange will confirm the actual availability at the time of the order.

(c) **Security.** Customer must:

(i) provide and manage its own dedicated firewall (or at Customer's request and subject to additional charges, Orange may manage such Customer-provided firewall), which will be located at Customer's Location; or

(ii) purchase the Orange virtual firewall service feature that is hosted in the Shared Platform, and in such event a policy-based routing will be implemented in the Orange-managed CPE Router to ensure that all Internet traffic is processed by the firewall; or

(iii) purchase a separate Orange-managed dedicated firewall service via the Orange Secure Gateway Service offering, and for clarity, the managed firewall service provided through the Orange Secure Gateway Service offering is a separate and billable service and is not part of the Business VPN Internet Service or the Business VPN Service.

(d) **Reporting.** Customers will be able to see via the My Service Space portal the Internet bandwidth utilization in addition to the current Business VPN IP bandwidth utilization reporting. If Customer purchases the virtual firewall feature hosted in the Shared Platform (as described in Clause 1.1.5(c)(ii) above, then it will also be able to view in the My Service Space portal the firewall security policy that Orange has implemented in the virtual firewall environment hosted in the Shared Platform, and the security events and security logs.

(e) **Charges.** The Charges for the Content Internet Profile include the Internet bandwidth charges, but exclude the Charges for the virtual firewall described in Clause 1.1.5(c)(ii) above (which will be invoiced to Customer as a separate and additional Charge). The Charges for Content Internet Profile are in addition to the Charges for the Business VPN Service.

1.1.6 **Security Features Firewall Overview**

(a) S**ecurity Policy for Firewall in the Orange-managed CPE Router Firewall and Shared Platform.** With respect to the Orange-managed virtual firewall hosted in the Shared Platform (in the case of Distributed Breakout and the Content Internet Profile) or in the Orange-managed CPE Router (in the case of Local Breakout), Customer will define its security policy by completing and submitting to Orange a Service Request Form ("**SRF**"). The security policy, as described by Customer in the SRF, sets forth the pre-defined set of security rules and the specific traffic filtering rules against which the Internet traffic is checked. Orange will configure the firewall appliance located in the Shared Platform or in the Orange-managed CPE Router according to the security policy specified by Customer in the SRF. Customer may specify a universal firewall security policy to be implemented for all Locations or a Location-specific firewall security policy. When specifying its firewall security policy, Customer may either choose security rules based on the pre-defined set of Orange security rules, or it may specify customized firewall security rules.

(b) **Applications Firewall.** Application firewall is an additional security feature option that can be implemented in the Shared Platform should Customer desire to monitor, control, and/or block the access to or from certain applications according to the security policy configured in the firewall. Customer will define its security policy for the application firewall by completing and submitting to Orange the SRF. The security policy, as described by Customer in the SRF, sets forth the security rules and application filtering rules against which the Internet traffic is checked. Orange will configure the application firewall appliance according to the security policy specified by Customer in the SRF. The application firewall feature is a billable service, and the Charges for this feature are in addition to the Charges for the Business VPN Service and the Business VPN Internet Service.

(c) **Leveling Requirements and Customer Security Policy Request**

(i) Solely with respect to the Local Breakout feature of the Browsing Internet Profile and the virtual firewall implemented in the Orange-managed CPE Router, to ensure the correct operation of the firewall, a software and hardware leveling towards the Orange-managed CPE Router's firewall appliance may be required. The Charges for such leveling will be in addition to the Charges for the Business VPN Service and the Business VPN Internet Service.

(ii) Customer will provide Orange with a completed SRF that specifies Customer's firewall security policy for the virtual firewall at the time it orders the Browsing – Local Breakout or Browsing – Distributed Breakout (or at the time it orders the Content Internet Profile, in the case where Customer elects to purchase the virtual firewall service feature hosted in the Shared Platform instead of providing and managing its own dedicated firewall devices). Customer can provide either a Location-specific firewall security policy or a universal firewall security policy for all Locations.

(d) **Firewall Configuration**. If Customer does not provide Orange with a completed SRF at the time Customer orders the Business VPN Internet Service, then Orange will set up the virtual as a 'diode' (i.e. all the outgoing traffic from the LAN are authorized and all the incoming traffic into the LAN are blocked). Customer may request Orange to change the security policy configuration of the virtual firewall by completing and submitting an SRF to Orange pursuant to the change management process described in Clause 1.1.6(e)(i) below. If Customer provides Orange with an SRF without specifying any traffic filtering rules, then the firewall will be configured as a 'diode' (i.e. all the outgoing traffic from the LAN are authorized and all the incoming traffic into the LAN are blocked). If Customer purchases the Application Firewall feature, but does not provide any application filtering rules in the SRF, then no application rules will be configured by Orange.

(e) **Change Management.** Following the initial implementation by Orange of Customer's security policy into the virtual firewall hosted in the Shared Platform or in Orange-managed CPE Router (or the set up by Orange of the

virtual firewall using the 'diode' configuration that only allows Outbound Internet Traffic sessions, in the case where Customer does not provide Orange with a completed SRF at the time Customer orders the Business VPN Internet Service), Orange will accept and implement changes to the firewall security policy only in accordance with the Change Management process provided through the Orange Service Select – Service Support Service. For clarity, Service Select – Service Support is a separate Service from the Business VPN Internet Service and the Business VPN Service. All change requests to the firewall security policy and configuration will be subject to verification and approval of Orange and Customer will provide Orange with the following information in addition to any other information reasonably requested by Orange in order to validate and implement Customer's change request:

(i) completed SRF for the affected Location(s), and such SRF must restate and describe in detail the entire security policy for the affected Location(s), not just the change to the security policy;

(ii) supporting details relevant to the specific change action requested by Customer; and

(iii) Customer's contingency plans and the contact details of Customer personnel who will perform any acceptance testing of the changes to the traffic filtering rules for the affected Location(s).

(f) **Incident Management.** The resolution of any failure or malfunction in the proper operational condition of the Orange-managed virtual firewall hosted in the Shared Platform or in the Orange-managed CPE Router will be provided by Orange through its Service Select – Service Support Service. The level of incident management support will depend on which type of Service Select – Service Support feature (i.e. standard support or extended support) Customer has purchased for the Business VPN Service. If an update of the security policy is required in order to resolve the incident, then Customer must complete and submit a change request and a completed SRF to Orange in accordance with the change management process described in the foregoing Clause 1.1.6(e).

(g) **Reporting.** Customer will be able to see via the My Service Space portal the security policy, as implemented by Orange pursuant to the information provided by Customer in the SRF, and the security events and security logs.

(h) **Geographical Coverage.** Unless prohibited by law or regulation, the virtual firewall feature of Business VPN Internet and that is hosted in the Shared Platform or in the Orange-managed CPE Router is generally available in countries where Orange provides Customer with Business VPN Service. However, Orange will confirm the actual availability at the time of the order.

(i) **Limitation of Service.** There is no URL or Web content filtering included in the Business VPN Internet Service. URL filtering and Web content filtering are separate and billable services. Customer will be solely responsible for its own network security policy and for responding to any security violation pursuant to its own security incident response procedures. While the Orange-managed virtual firewall hosted in the Shared Platform may enhance Customer's ability to impede unauthorized access to Customer's networks, systems, applications and data and may assist Customer in detecting potential security breaches and network irregularities, Customer acknowledges and agree that the Business VPN Internet and the firewall do not guarantee in any sense the security of Customer's networks, systems, applications and data, and nor can such virtual firewall absolutely prevent incidents of security breaches. It is Customer's responsibility to design a comprehensive security program in conjunction with any other service providers or professionals chosen by Customer.

1.1.7 **Charges**

(a) The Charges for the Browsing Internet Profile include the virtual firewall hosted in the Shared Platform (in the case of the Distributed Breakout feature) or in the Orange-managed CPE Router (in the case of the Local Breakout feature), except that changes to the firewall after Orange has implemented Customer's initial security policy into the firewall are subject to additional charges, and such additional charges will be quoted to Customer upon request.

(b) The Charges for the Content Internet Profile does not include the virtual firewall hosted in the Shared Platform. The virtual firewall for the Content Internet Profile and any changes thereto are billable services in addition to the Charges for the Business VPN Service and the Content Internet Profile. Such additional charges will be quoted to Customer upon request.

(c) As mentioned in Clause 1.1.6(b) (Application Firewall) above, the Charges for the application firewall are in addition to the Charges for the Business VPN Service and the Business VPN Internet Service. The Charges for the application firewall feature consist of one-time installation charge and monthly recurring charges per Location. These Charges are in addition to the Charges for the Business VPN Internet Service (and with respect to the Content Internet Profile, are in addition to the Charges for the virtual firewall). The one-time application firewall installation charge per Location entitles Customer up to ten (10) customized security rules per Location. Additional customized security rule will be subject to additional charge, which will be quoted to Customer upon request.

1.1.8 **Data Processing**

Exhibit A sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and the categories of Data Subjects of the Processing of Personal Data carried out by Orange as part of this Service.

## EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE BUSINESS SERVICES AS PROCESSOR FOR CUSTOMER - ARTICLE 28 OF GDPR

**Name of the Service: Business VPN Internet International**

### ExA.1 Processing Activities

| | |
|---|---|
| Collection (receiving personal data of employees and users of customer who are natural persons, etc.). | Yes |
| Recording (capturing personal data in a file or software program, including the generation of metadata like Call Details Records, etc.). | Yes |
| Organization (organizing personal data in a software program, etc.). | Yes |
| Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.). | Yes |
| Modification (modifying the content or the way the personal data are structured, etc.). | Yes |
| Consultation (looking at personal data that we have stored in our files or software programs, etc.). | Yes |
| Disclosure or otherwise making available (communicating personal data to another recipient by any means, etc.). Except for disclosure mentioned in the service description or required by law, or otherwise specifically directed by the customer, the categories of potential recipients are only those subcontractors referenced herein or otherwise approved by the customer. | Yes |
| Combination (merging two or more databases with personal data, etc.). | No |
| Restriction (implementing security measures in order to restrict the access to the personal data, etc.). | Yes |
| Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.). | Yes |
| Other use (if "YES" to be detailed). | No |

### ExA.2 Categories of Personal Data Processed (Type of Personal Data)

| **Categories of Personal Data Identifiable by Orange** | |
|---|---|
| Identification data (ID document / number, phone number, email, etc.). | No |
| Traffic / Connection data (IP address, Mac address, CDRs, access and usage data, online tracking and monitoring of services). | Yes |
| Location Data (geographic location, device location). | No |
| Customer Relationship Management data (billing information, customer service data, ticketing info, telephone recordings, etc.). | No |
| Financial data (bank account details, payment information). | No |
| Sensitive Data (racial/ethnic background, religion, political or philosophical beliefs, trade union membership, biometric data, genetic data, health data, sexual life, and/or orientation). | No |
| **Categories of Personal Data Not Identifiable by Orange** | |
| Any categories of personal data that may be recorded or stored (voicemail, call recording, files) by Customer and which recording is hosted on Orange infrastructure. | No |

### ExA.3 Subject-Matter and Duration of the Processing

| **Subject-Matter of Processing** | | **Duration of Processing** |
|---|---|---|
| Service activation. | No | For the period necessary to provide the service to the customer plus 6 months. |
| User authentication. | No | |
| Incident Management. | No | |
| Quality of Service. | No | |
| Invoice, contract, order (if they show the name and details of the contact person of Customer). | Yes | For the period required by applicable law. |
| Itemized billing (including traffic / connection data of end-users who are natural persons). | No | |
| Customer reporting. | Yes | For the duration requested by Customer. |
| Hosting. | No | |
| Other. [if yes please describe] | No | |

### ExA.4 Purposes of Processing

| |
|---|
| Provision of the service to Customer. |

### ExA.5 Categories of Data Subject

| | |
|---|---|
| Customer's employees/self-employed contractors using or managing the service or the contract who are natural persons. | Yes |
| Customer's other end-users of the service who are natural persons (client of the Customer, etc.); usable by users other than internal users. | Yes, according to customer's usage. |

### ExA.6 Sub-Processors

| Sub-Processors Approved by Customer | Safety Measures |
|---|---|
| Orange Business Services entities that are processing information for this Service and that are within the EU/EEA are communicated separately to the Customer. | NA |
| Orange Business Services entities that are processing information for This Service and that are outside of the EU/EEA are communicated separately to the customer. | Intra-group agreements with standard model clauses, Binding Corporate Rules approval request filed with CNIL. |
| Orange Business Services suppliers which are performing one or more processing activities described above in connection with this Service and that are within the EU/EEA are communicated separately to the Customer. | NA |
| Orange Business Services suppliers that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the Customer. | Standard Model Clauses in contract with supplier. |