PUBLICATION 1 SERVICE DESCRIPTION FOR BUSINESS VPN SERVICE

1.1 Definitions

All capitalized terms used but not defined herein will have the meanings given to such terms elsewhere in the Agreement. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions set forth herein will control for purposes of this Service Description.

"**BGP**" means Border Gateway Protocol.

"**CE Router**" means Customer Edge router.

"**CoS**" means Class of Service.

"**D1**" or "**Data 1**", "**D2**" or "**Data 2**", "**D3**" or "**Data 3**" means the data CoS, each as described in Clause 1.3.4(b) (Data CoS).

"**DNS**" means Domain Name System.

"**DSL**" means Digital Subscriber Line.

"**EVC**" means Ethernet virtual connection.

"**FFTx**" means Fiber to the x, which refers to any broadband network architecture using optical fiber to provide all or part of the local loop used for last mile telecommunications.

"**Flexible CoS**" means flexible options for the Gold Service Type and Platinum Service Type.

"**IPSec Passthrough**" means a technique that allows IPSec packets to pass through a NAT device.

"**IPSec**" means Internet Protocol Security.

"**ISDN**" means Integrated Services Digital Network.

"**L2TP**" means Layer 2 Tunneling Protocol, which is a network protocol that encapsulates packets at a peer level or below, used to transport multiple protocols over a common network as well as provide the vehicle for encrypted VPNs.

"**LAN**" means local area network.

"**MPLS**" means the Multi-Protocol Label Switching.

"**NAT**" means Network Address Translation.

"**P Router**" means the Provider edge router that allows a CE Router to connect to the Business VPN Service.

"**PE Router**" means Provider Edge router.

"**PPPoE**" means Point-to-Point Protocol over Ethernet.

"**PSTN**" means Public Switched Telephone Network.

"**RT-Vi**" means the real-time video CoS, as described in Clause 1.3.4(c) (Video CoS).

"**RT-Vo**" means the real-time voice CoS, as described in Clause 1.3.4(d) (Video CoS).

"**Service Bandwidth**" means the IP bandwidth.

"**Site Profile**" means the Business VPN profile (i.e. Business VPN Small, Business VPN Small Off-Net, Business VPN Small VM, or Business VPN Corporate) of a Location.

"**SNMP**" means Simple Network Management Protocol.

"**Telnet**" means a telecommunication network protocol used on Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.

"**VLAN**" means virtual local area network.

"**VPN**" means virtual private network.

"**VRF**" means VPN Routing Forwarding.

"**WiMax**" means Worldwide Interoperability for Microwave Access, which is a wireless industry coalition dedicated to the advancement of IEEE 802.16 standards for broadband wireless access networks.

1.2 Overview

The Specific Conditions for Network Services apply to the Business VPN Service. Business VPN Service only provides the features and functionality set forth in this Service Description. Business VPN Service provides connectivity between Locations in an "any-to-any" environment by enabling any CE Routers within the same VPN to communicate with each other using IP switching. Business VPN Service uses Orange MPLS architecture and is comprised of CE Routers, PE Routers, and P Routers. The CE router is installed at the Location and connects to the PE router through an access medium. Each CE router is equipped with one or more LAN interface types that connect the Customer's LAN to the Orange Network. Unless otherwise agreed and configured by Orange, Business VPN Service does not allow the CE Routers in different VPNs to communicate with one another.

1.3 Standard Service Elements

1.3.1 **Service Bandwidth.** A subdivision of the access bandwidth, the Service Bandwidth represents the short-term bandwidth needs of the Location. The Service Bandwidth parameter is limited to the Tail Circuit's bandwidth; however, the actual Service Bandwidth is less than the Tail Circuit bandwidth due to the overhead. The maximum available Service Bandwidth for real time voice and video traffic varies according to the type of access medium and the country where the Location is situated. Table 1 (Class of Service Bandwidth Allocation) in Exhibit A to this Service Description summarizes the bandwidth allocations for each CoS. Table 2 (Minimum Service Bandwidth Requirement) in Exhibit A to this Service Description sets forth the Business VPN Corporate's minimum Service Bandwidth requirement for real-time traffic.

1.3.2 **CE Router.** An Orange-managed CE router is installed at each Location, unless Customer elects to provide, maintain, and manage its own CE router.

1.3.3 **Tail Circuit.** The access bandwidth depends on the bandwidth availability in each country where the Location is situated, and the access bandwidth should reflect the Location's mid-term to long-term bandwidth requirement.

(a) **Orange-Provided Tail Circuit.** If possible, Orange will order the Tail Circuit from the TO. The Tail Circuit can be delivered through different technologies (e.g. xDSL, cable, WiMax, Ethernet, leased lines, FTTx, etc.) so long as such technologies are available.

(b) **Customer-Provided Tail Circuit.** Customer will be responsible for providing the Tail Circuit if: (i) Orange cannot provide such circuit because of regulatory reasons, (ii) it elects to provide the Tail Circuit, or (iii) it is required under the Agreement (including this Service Description) to provide the Tail Circuit. In such events, Customer will, at its sole cost and expense: (iv) procure the Tail Circuit from the TO and ensure that the Tail Circuit is installed at the Location before the Business VPN Service installation; (v) test and confirm that the Tail Circuit is in proper operational condition and ready for the installation of the Business VPN Service; (vi) monitor, manage, maintain and repair the Tail Circuit and all related equipment (e.g. modem, router, etc.); (vii) pay the TO any and all charges related to such circuit; (viii) disconnect the Tail Circuit upon the disconnection of the Business VPN Service; (ix) ensure that the Tail Circuit is configured properly in accordance with any Orange specifications; and (x) upon request, provide Orange with all relevant information concerning the Tail Circuit. Notwithstanding anything to the contrary set forth in the Agreement, the Service Select – Service Delivery Service and Service Select – Service Support Service, and Service Management provided by Orange in connection with the Business VPN Service do not apply to any Customer-provided Tail Circuit.

1.3.4 **Class of Service**

(a) **CoS Overview.** There are five (5) CoS whereby: (i) three (3) CoS are dedicated to data traffic; (ii) one (1) CoS is dedicated to video traffic; and (iii) one (1) CoS is dedicated to voice traffic. However, if Customer buys the Business VPN Internet optional feature, a sixth CoS (also referred to as data best effort CoS) is provided for Internet traffic in order to maintain the priority of the D1, D2, and D3 data traffic. The Business VPN Internet is an optional service subject to additional charges and is described in a separate Service Description. The Service Type and the Location's Site Profile will determine the CoS.

The data, video, and voice CoS use bandwidth management and prioritization mechanisms that allocate the available Service Bandwidth in proportion to the "relative weight" of each CoS whenever traffic congestion occurs on the access circuit. These bandwidth management and prioritization mechanisms mitigate traffic congestion by proactively detecting over-capacity needs and by managing the congestion if the capacity needs exceed all of the "buffer" capacity of the CE router and the access circuit.

(b) **Data CoS:** Each data CoS is allowed to use all the available Service Bandwidth on the access up to 100% of the available Service Bandwidth, provided that the voice CoS has priority over the three (3) data CoS in case of network congestion. The data CoS are divided into the following categories:

- **Data 1 (D1):** The D1 CoS is generally used for business-critical data applications that require maximum Service Bandwidth performance and availability. D1 traffic has the highest priority of all the data traffic, and it is given the maximum Service Bandwidth availability and priority in case of network congestion.
- **Data 2 (D2):** The D2 CoS is used for "standard business" data application traffic that requires a high level of Service Bandwidth performance and availability. D2 traffic has an intermediate level of priority when network congestion occurs.
- **Data 3 (D3):** The D3 CoS is generally used for non-business critical data applications. It has the lowest priority when network congestion occurs in order to provide the D1 and D2 traffic the maximum available Service Bandwidth and priority.

(c) **Video CoS.** The RT-Vi CoS is used to transport videoconferencing applications that require Service Bandwidth performance and availability. The RT-Vi CoS uses class-based weight and fair queuing mechanisms, and it will have a guaranteed Service Bandwidth in case of access congestion. All traffic that exceeds the allocated Service Bandwidth, as determined by the speed and number of simultaneous video sessions being supported, is discarded in order to protect the D1, D2, and D3 traffic. This RT-Vi CoS is optional and subject to additional charges.

(d) **Voice CoS.** The RT-Vo CoS uses "real time" priority mechanism to manage the voice traffic over the IP network. Jitter is the quality indicator for voice traffic. RT-Vo CoS has priority over the D1, D2, and D3 traffic; however, it is subject to a maximum allocated Service Bandwidth availability, as specified in the Table 1 (Class of Service Bandwidth Allocation) of Exhibit A to this Service Description. All traffic that exceeds the maximum allocated Service Bandwidth is discarded in order to protect the D1, D2, and D3 traffic. RT-Vo CoS is optional and subject to additional charges.

1.3.5 **Service Types**

(a) **Silver.** The Silver Service Type, which is the basic Service Type for Business VPN Service, allows Customer to obtain an "any-to-any" Business VPN plug for Locations that require IP-only service. It does not provide multi-protocol encapsulation or application prioritization.

(b) **Gold.** The Gold Service Type allows Customer to manage the application traffic by using CoS management standard profiles that allocate and distribute the access bandwidth in case of traffic congestion. It also provides multi-protocol management. Customer can classify its data applications into one of the three data CoS (i.e. D1, D2, or D3 CoS).

(c) **Platinum.** The Platinum Service Type allows multi-protocol management and data application traffic management. This Service Type includes the D1, D2, D3, RT-Vi, and RT-Vo CoS to give greater priority for either voice traffic or video traffic, or for both traffics. The Platinum Service Type is not available when using satellite access or DSL access unless agreed in writing by Orange.

(d) **Flexible Option.** Orange can provide Flexible CoS if Customer requires greater control of the bandwidth management. The Flexible CoS permits customization of the access bandwidth for each CoS and traffic prioritization.

The Service Bandwidth for Silver, Gold, and Platinum Service Types and for the Flexible CoS is subject to the following limitations: (i) for D1 CoS, the minimum Service Bandwidth is 16 kbps; and (ii) for D2 CoS, the minimum Service Bandwidth is 12 kbps.

1.3.6 **Site Profile**

(a) **Site Profile Overview.** Customer can designate the Site Profile of the Location as Business VPN Small, Business VPN Small VM, Business VPN Small Off-Net, or Business VPN Corporate depending on whether the Location is a critical site and whether the following are needed: (i) end-to-end performance levels for the network traffic; (ii) voice or video are to be combined with data traffic on a single IP plug; (iii) multi-protocol encapsulation solution rather than pure IP service for the Location; and (iv) any of the optional service features (e.g. Telepresence Connect, Multicast, etc.) for the Business VPN Service. Table 3 (Site Profile Attributes) in Exhibit A to this Service Description summarizes the main attributes of the Site Profiles.

(b) **Business VPN Small.** Business VPN Small only supports by default the D2 CoS, which means that all network traffic will be prioritized as D2 CoS. As an optional feature and subject to additional charges, with respect to Business VPN Small, Orange may be able to support an additional CoS prioritized over the D2 CoS; however, this feature’s availability and the minimum Service Bandwidth requirement are subject to confirmation by Orange.

Subject to availability, Orange will implement Business VPN Small using xDSL or FTTx cabling. Orange will, at its discretion, implement this Service using PSTN line, ISDN line, fiber or dedicated copper. Orange will: (i) provide the Service Bandwidth and will configure it to support the xDSL or FTTx access downstream speed; (ii) subject to Clause 1.3.3 (Tail Circuit), provide the Tail Circuit (which may be xDSL, FTTx, cable, or WiMax) to connect the CE router to the Orange Network; and (iii) configure the CE router according to the standard Orange IP-only configuration. Business VPN Small excludes the provision by Orange of DNS, and Customer is solely responsibility for providing the DNS.

(c) **Business VPN Small Off-Net.** Except as specified in this Clause 1.3.6(c), Business VPN Small Off-Net also has the same standard service features, requirements, exclusions, and limitations as Business VPN Small. Orange will provide and manage the CE router at the Location. Orange will also provide a Silver Service Type port to the Orange Network. Subject to Clause 1.5.2 (Regulatory Constraint), the connectivity between the VPN and the Off-Net Location is secured via IPSec protocols.

Instead of connecting the Location to the VPN using an Orange-supplied Tail Circuit, the Location will be connected to the VPN via a Customer-supplied public Internet access service. Clause 1.3.3(a) (Customer-Provided Tail Circuit) will apply to Business VPN Small Off-Net. Customer will specify in the Order the configuration of the Internet-based access connection and line speed and will notify Orange immediately of any changes to the Internet-based access connection. The configuration of the Internet-based access connection must include the following: (i) PPPoE with either dynamic or static public IP address with Internet DSL modem or with Internet router configured in bridge mode; (ii) Ethernet 10/100 Mbit/s interface (USB interface is not supported); (iii) access speed no greater than those quoted Table 4 (Business VPN Small Off-Net Maximum Access Speed) in Exhibit A to this Service Description; and (iv) Internet broadband service must enable IPSec Passthrough. Orange will install the Business VPN Small Off-Net Service after Customer has successfully completed the installation and testing of the Internet-based access connection. Any change to the Internet-based access connection may result in additional Charges for Business VPN Small Off-Net.

Orange is not responsible or liable for any faults in the Business VPN Small Off-Net caused by the Internet-based access connection (including related equipment (e.g. modem, router, etc.). Before reporting any Incident to Orange, Customer must confirm that the Internet-based access connection is in proper operational condition.

(d) **Business VPN Small VM.** Except as specified in this Clause 1.3.6(d), Business VPN Small VM also has the same service features, requirements, exclusions, and limitations as Business VPN Small. The Location will be connected to the VPN by using Internet-based access connection; however, Orange may (at its sole discretion) deliver Business VPN Small VM using PSTN line, fiber, dedicated copper, wireless or radio-link in lieu of

Internet-based access connection. Business VPN Small VM cannot use 3G, 4G or satellite link as access connections.

Orange will: (i) provide and manage the CE router at the Location; (ii) subject to Clause 1.3.3 (Tail Circuit), order the Internet-based access connection to the Orange Network from an ISP and manage and maintain such Internet-based access connection. The Internet-based access connection will: (iii) include PPPoE with either a dynamic public IP address or a static public IP address, and (iv) subject to Clause 1.5.2 (Regulatory Constraint), enable IPSec Passthrough. At least one public IPv4 address will be provided by default. Additional public IP address or static IP address is subject to Orange's prior approval and may be subject to additional charges.

(e) **Business VPN Corporate.** Business VPN Corporate may use leased lines, Ethernet or DSL as access circuits. Orange will configure the Service Bandwidth with CoS support for each Location according to Customer's requirements. Orange will provide and manage the CE router, including upgrades to the router's operating system software if Orange deems it necessary to do so. The Service Bandwidth for Business VPN Corporate varies from 64kbps to 5Gbps, and the availability varies per country and per access method.

1.3.7 **Application Management.** The application classification rules define how the CE router manages the application traffic classification (i.e. prioritization) for the outgoing traffic. Customer must define a set of classification rules for its applications during the design of the Business VPN network. When formulating the application classification rules, Customer must focus on the main applications that are to be given top priority in terms of traffic management. The remaining applications will be automatically classified according to the default CoS configured on the access. The classification rules can be modified during the lifecycle of the Business VPN network via Orange Professional Services, and for clarity such services are not included in the Business VPN Service.

Orange will configure the CE router according to Customer's application classification rules. Applications are classified according to their corresponding data, video, or voice CoS. The incoming traffic (i.e. traffic moving from the Orange Network to the CE router) takes precedence over the outgoing traffic (i.e. traffic moving from the CE router to Orange Network), and the Business VPN network will automatically classify the incoming traffic according to its CoS. If the incoming traffic's CoS is not configured on the access, then it is classified as an "unknown type of traffic" and placed in the "by default" CoS that is configured on the access. The per-CoS traffic assignment rules correspond to how traffic flow is mapped to a CoS, and they are similar to the rules for specifying an access control list. If any incoming traffic does not match any of the application classification rules, then this incoming traffic is sent into the lower level CoS (e.g. D2 CoS or D3 CoS).

If Customer selects the Flexible CoS options, then it is recommended that Customer also purchase the Orange Enterprise Application Management Service. The Orange Enterprise Application Management Service is a separate Orange service, and is described in a separate Service Description.

1.3.8 **Border Gateway Protocol.** The total number of BGP routes that Customer is allowed to send into the Orange Network is 500 BGP prefixes per CE router. Any additional BGP routes is subject to validation and approval by Orange, and additional Charges may apply. Static routing is implemented by default with Business VPN Small, BVPN Small VM, and Business VPN Small Off-Net, but BGP can be implemented on demand.

1.3.9 **Acceptance Test.** An Acceptance Test is considered successful when Orange is able to establish Internet Protocol connectivity between a CE router at the new Location and a CE router at another Location within the same IP VPN community. The Acceptance Tests for voice, data, and video CoS are independent from each other.

1.3.10 **Business VPN Security Components.** The following are the security components of the Business VPN Service:

(a) **Physical Security.** The P routers and PE routers, which maintain the MPLS-VPN logical security, are located in the Orange premises.

(b) **Connection to Network Devices.** Telnet or SNMP access to network devices is restricted to a defined set of management stations located in a protected administration area, and both SNMP and Telnet sessions are controlled by passwords.

(c) **Separate Routing Tables Per VPN.** The PE router holds one VPN table ("**VRF**") per customer. Each PE-to-CE sub-interface is assigned to a VRF by the PE configuration, and each VRF contains only the routes of Customer's VPN. Each VPN is assigned to a unique identifier (i.e. BGP route target attribute), which is used by the network to route and to separately filter Customer's traffic.

(d) **CPE.** The CE router does not hold the VPN definition logically defined on the PE router. Since the PE router is located in the Orange premises, the MPLS-VPN logical security features are not compromised if the CE router configuration is breached.

(e) **Access Security.** While leased lines and ATM-based access services are inherently secure, access connectivity via third party networks (e.g. public Internet or layer 3 IP networks) are secured using a tunneling technology (i.e. L2TP or IPSec). These tunnels ensure the privacy of the IP packets and Customer's VPN. For Ethernet access, traffic isolation is maintained through the EVC and VLAN concepts.

In all cases, and notwithstanding the foregoing or anything to the contrary set forth in the Agreement, Customer is solely responsible for designing and implementing appropriate and comprehensive technical, administrative, or physical safeguards to protect its own network (including, without limitation, establishing its own security policy and security violation response procedures) against any security threats. Although the foregoing Business VPN security components may protect the Business VPN network against unauthorized access, they do not guarantee an absolute network security or that such security components will be fully capable of preventing or defeating all security threats.

1.4 Service Support

If ordered by Customer, Orange will provide service and network management support via the Service Management. Orange will provide installation support via Service Transition. Service Management and Service Transition are separate and billable services, and the Charges for these services are not included in the Charges for Business VPN Service.

1.5 Service Restrictions and Limitations

1.5.1 **Prohibited Use of Voice Traffic.** Customer will not use the Business VPN Service to carry real time voice traffic unless the Order or Order Form expressly indicates that Customer may use the Business VPN Service for voice traffic.

1.5.2 **Regulatory Constraint.** Business VPN Service may not be available in certain countries (e.g. countries where IPSec tunneling or encryption technology is prohibited). Orange reserves the right to modify any applicable Service Levels in order to comply with the regulatory or other government requirements. Customer will comply with all regulatory requirements and will obtain all regulatory approvals in order for Customer to use the Business VPN Service (e.g. obtaining a permit from the appropriate government authority in order to use IPSec-enabled devices and encryption technology in connection with Business VPN Small VM and Business VPN Small Off-Net).

1.5.3 **Optional Service Features.** Certain optional Business VPN service features may not be available for Business VPN Small Off-Net, Business VPN Small VM, Business VPN Small, or Business VPN Corporate. The optional Business VPN service features are described in separate Service Descriptions. Orange will confirm the availability the optional service features upon request. The Charges for optional Business VPN service features are in addition to the Charges for the Business VPN Service.

EXHIBIT A TABLES

Table 1: Class of Service Bandwidth Allocation

Service Type	Class of Service			
	RT-Vi and RT-Vo[‡]	D1	D2	D3
Silver	Not applicable.	Not applicable.	Maximum bandwidth = 100% of total available Service Bandwidth.	Not applicable.
Gold	Not applicable.	Maximum bandwidth = 60% of total available Service Bandwidth.	Maximum bandwidth = 30% of total available Service Bandwidth.	Maximum bandwidth = 10% of total available Service Bandwidth.
	Not applicable.	Maximum bandwidth = 66% of total available Service Bandwidth.	Maximum bandwidth = 33% of total available Service Bandwidth.	Not applicable.
	Not applicable.	Not applicable.	Maximum bandwidth = 100% of total available Service Bandwidth.	Not applicable.
Platinum	▪ In case of Business VPN Corporate built on Leased Lines: maximum RT bandwidth = 75% of total Service Bandwidth. ▪ In case of Business VPN Corporate built on Ethernet or xDSL access: maximum RT bandwidth = 40% of total Service Bandwidth. ▪ With Business VPN service for Telepresence: maximum RT bandwidth = 75% of total Service Bandwidth.	Maximum bandwidth = 60% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.	Maximum bandwidth = 30% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.	Maximum bandwidth = 10% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.
		Maximum bandwidth = 66% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.	Maximum bandwidth = 33% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.	Not applicable.
		Not applicable.	Maximum bandwidth = 100% of total available Service Bandwidth minus RT-Vi and RT-Vo bandwidth.	Not applicable.

[‡] When Ethernet access bandwidth is significantly greater than the IP Service Bandwidth (i.e. Ethernet bandwidth is 20% higher than service IP bandwidth), voice traffic can be extended to 75% of the IP Service Bandwidth.

Table 2: Minimum Service Bandwidth Requirement‡‡

Business VPN Corporate Access	Minimum Service Bandwidth
Leased Line Dedicated Access	▪ RT-V o/BTG: 64kbps (FR) / 1Mbps (ATM) ▪ TP: 4M bps ▪ RT-Vi: 256kbps
Ethernet Dedicated Access	▪ 1Mbps
Integrated Access (SHDSL)	▪ RT-Vo: 512kbps ▪ BTG: 1M bps ▪ RT-Vi: 1M bps

Table 3: Site Profile Attributes

	Business VPN Small & Business VPN Small VM	Business VPN Small Off-Net	Business VPN Corporate
Any-to-Any IP Plug	Yes	Yes	Yes
Design and Configuration of the Business VPN	Yes	Yes	Yes
Provisioning and Management of CE Routers	Yes	Yes	Yes
End-to-End IP Performance Levels	No	No	Yes
Application Awareness	No	No	Yes
Multi-Protocol Integration	No (IP only)	No (IP only)	Yes
Multimedia Integration	Yes‡‡	No	Yes‡‡
Optional Business VPN Service Features	Case-by-Case Basis	Case-by-Case Basis	Case-by-Case Basis
‡‡ Availability depends on countries, Service Bandwidth, and Service architecture.			

Table 4: Business VPN Small Off-Net Maximum Access Speed‡‡‡

Speed Category	Symmetric Service Support	Asymmetric Service Support
< 8Mbit/s	8/8 Mbit/s	(Download + Upload speeds) / 2 < 8Mbps
< 16Mbit/s	16/16Mbit/s	(Download + Upload speeds) / 2 < 16Mbps
< 30Mbit/s	30/30Mbit/s	(Download + Upload speeds) / 2 < 30Mbps
< 50Mbit/s	50/50Mbit/s	(Download + Upload speeds) / 2 < 50Mbps
< 80Mbit/s	80/80Mbit/s	(Download + Upload speeds) / 2 < 80Mbps
< 100Mbit/s	100/100Mbit/s	(Download + Upload speeds) / 2 < 100Mbps
< 150Mbit/s	150/150Mbit/s	(Download + Upload speeds) / 2 < 150Mbps
< 200Mbit/s	200/200Mbit/s	(Download + Upload speeds) / 2 < 200Mbps
‡‡‡ If Customer uses the Business VPN Small Off-Net in conjunction with Local Internet Browsing optional features, then the maximum access speed is reduced by 30%.		

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

Name of the Service: Business VPN International

ExB.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
Transmission (carrying the traffic that may include personal data on our network using switching and/or routing, 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.).	Yes
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

ExB.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.).	Yes
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
CRM data (billing information, customer service data, ticketing info, telephone recordings, etc.).	Yes
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 contained in the voice, data, or internet traffic of Customer carried over Orange network.	Yes
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

ExB.3 Subject-Matter and Duration of the Processing

Subject-Matter of Processing		Duration of Processing
Service activation.	Yes	For the period necessary to provide the service to the customer plus 6 months.
User authentication.	Yes (only for Web Portal access)	
Routing configuration.	Yes	
Incident Management.	Yes	
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.	No	
Carry the traffic of customers' end-users.	Yes	For the duration of the transmission.
Hosting.	No	
Other.	No	

ExB.4 Purposes of Processing

Provision of the service to Customer.

ExB.5 Categories of Data Subject

Customer’s employees/self-employed contractors using the service who are natural persons.	Yes.
Customer’s other end-users of the service who are natural persons (client of the Customer, etc.).	According to customer’s usage.

ExB.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.

END OF SERVICE DESCRIPTION FOR BUSINESS VPN SERVICE