PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE SD-WAN

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.

"**Dynamic Host Configuration Protocol**" or "**DHCP**" means the network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so that it can communicate with other IP networks.

"**Edge Router**" means the hardware or software provided and managed by Orange and used to connect the Overlay Network to the Network. The Edge Router may either be physically installed by Orange at a Location as a CPE device or hosted in an Orange PoP.

"**EMS**" or "**Equipment Management System**" collectively means all equipment (including hardware and software) that Orange assembles into a system to manage the operation (e.g. routing function) of the Edge Routers that are within the same VPN.

"**Gateway**" means a network device (i.e. hardware or software) or node that facilitates the interface between the Network and the Customer's network by performing the translation between different communication protocols at the boundary where the Customer network connects to the Network.

"**Incident**" means a malfunction in the Service. Incidents do not include Service unavailability during Scheduled Maintenance.

"**IPSec**" or "**IP Security**" means a framework of protocols that secures the communication transmitted through an IP network by establishing virtual tunnels and data encryption.

"**Location**" means the Customer site to be connected to the Overlay Network.

"**Network**" will have the meaning given in the Specific Conditions for Orange Network Services.

"**Overlay Network**" means the virtual network established between the Locations by means of IPSec virtual tunnels that overlay the Underlay Connectivity.

"**PoP**" means an Orange Point of Presence.

"**Scheduled Maintenance**" means the maintenance scheduled by Orange to occur during low traffic periods in the Network to implement changes to, or version updates of the Network. Maintenance takes place typically 3 to 5 times per year and lasts an approximate average of 5 minutes each.

"**SD-WAN Module**" means a SD-WAN Technology module attached to this Service Description (see Exhibit A SD-WAN Module 1 - Fortinet® SD-WAN Technology) and that describes the Overlay Network features associated with the SD-WAN Technology chosen by Customer.

"**SD-WAN Technology**" means the Overlay Network technology (e.g. Cisco Meraki, Cisco Viptela, Fortinet, etc.) that Customer chooses to use for the Software-Defined WAN.

"**Service**" collectively means: (a) the Overlay Network components described in Clause 1.4 (Overlay Network Standard Service Elements) below, (b) the Overlay Network features described in the SD-WAN Module that corresponds to the SD-WAN Technology chosen by Customer; and (c) the optional Flexible SD-WAN features described in Clause 1.5 that Customer may order from Orange.

"**Software-Defined WAN**" means a network architecture that enables the WAN to be centrally managed by using software-based controllers.

"**Underlay Connectivity**" means the physical network infrastructure and the access medium (e.g. broadband Internet access, dedicated Internet access, Orange Business VPN Service, etc.) that transport the traffic across Customer's WAN.

"**VPN**" means Virtual Private Network.

"**WAN**" means Customer's wide area network.

1.2 Overview

The Specific Conditions for Network Services and the Specific Conditions for Security Services apply to the Service. Software-Defined WAN is comprised of the Overlay Network and the Underlay Connectivity. The Service only provides the features and functionalities set forth in the main body of this Service Description and in the Service Module for the SD-WAN Technology selected by Customer.

Unless Customer orders from Orange the Underlay Connectivity optional service, the Flexible SD-WAN service only concerns the provisioning of the Overlay Network to the Locations. The standard elements of the Overlay Network are set out in Clause 1.4 (Overlay Network Standard Service Elements), and these elements apply regardless of the type of SD-WAN Technology that Customer selects for the Software-Defined WAN. The Overlay Network standard features that are described in the SD-WAN Module that corresponds to the SD-WAN Technology chosen by Customer supplements Clause 1.4 (Overlay Network Standard Service Elements).

Customer will provide the Underlay Connectivity for the Software-Defined WAN unless it orders from Orange the Underlay Connectivity as an optional service.

1.3 Underlay Connectivity/Access Requirements

1.3.1 Customer will provide all components of the Underlay Connectivity for the Software-Defined WAN. Customer will: (a) procure the Internet access (e.g. broadband Internet access, dedicated Internet access) for the Underlay Connectivity from an Internet access provider; (b) ensure that the Internet access is installed at the Location, and tested to verify that the Internet access is functioning properly prior to the date that the Location is to be connected to the Overlay Network; (c) manage and maintain the Internet access and all other components of the Underlay Connectivity (e.g. modem, router, switches, etc.) for the entire Service Term; (d) immediately notify Orange of any changes to the Internet access that may affect the Service; (e) promptly resolve any Incidents caused by the Internet access or other Underlay Connectivity components; (f) confirm, before reporting any Incident to Orange, that the Internet access and all other components of the Underlay Connectivity are functioning properly and that they are not the cause of the Service malfunction. Any change to the Internet access that adversely affects the Service may result in additional Charges.

1.3.2 Customer will configure the Internet access according to the specifications provided by Orange. The minimum Internet access configuration includes: (a) Internet modem with DHCP; (b) Ethernet 10/100 Mbit/s or 1 Gbit/s interface (USB interface is not supported) to which the Customer's WAN connections can be connected; and (c) Internet access that enables IPSec passthrough. Customer also must provide a public IP address for use with the Service.

1.3.3 Customer is responsible for the use of the Internet access and for complying with all laws and regulations relating to the possession and use of the Internet access, any limitations or restrictions on the Internet access or its capability (e.g. restriction on the classes of service (i.e. data, voice or video traffic) that can be transmitted by Customer or the Users across the WAN; inter-connection of the Internet access to other networks; etc.).

1.3.4 Orange will not be responsible for any Service failure caused by the Customer's Underlay Connectivity.

1.4 Overlay Network Standard Service Elements

Unless otherwise expressly stated in the relevant SD-WAN Module, the Overlay Network consists of IPSec virtual tunnel, Edge Router, EMS, intelligent dynamic routing, zone-based security firewall, and access to the Flexible SD-WAN Selfcare management tool.

1.4.1 **IPSec.** The Overlay Network establishes IPSec virtual tunnels to enable the Edge Routers within the same VPN can communicate with each other. Orange will configure the Overlay Network's Edge Routers with application-based policy routing and security rules to ensure that traffic is routed to the right path as it is transmitted through the WAN.

1.4.2 **Edge Routers.** Orange will provide and manage the Edge Routers for the Overlay Network. The type of Edge Routers that Orange will provide for the Overlay Network will depend on the type and bandwidth of the Underlay Connectivity. Customer will provide Orange with all relevant Underlay Connectivity information requested by Orange. Orange will configure the Edge Routers with application-based policy routing and security rules to organize how traffic will be routed through the WAN.

1.4.3 **EMS.** Orange will virtually manage the Edge Routers using the EMS.

1.4.4 **Dynamic WAN Path Selection.** The Overlay Network provides intelligent dynamic routing to route traffic based on current conditions of the Customer WAN (e.g. bandwidth usage, application content, etc.) in an effort to improve the performance of Customer's applications.

1.4.5 **Firewall.** Orange will implement a zone-based security firewall policy into the Edge Router, and the security firewall will be configured using an Orange default configuration during the installation of the Service; provided, however, the implementation of such firewall policy does not guarantee that the Service is impervious to unauthorized intrusion or access. Customer is solely responsible for maintaining appropriate security measures to protect its network (including its WAN), systems and facilities against unauthorized access and malicious attacks. Notwithstanding anything to the contrary contained in the Agreement, Orange will not be liable or responsible for any unauthorized intrusion or access into Customer's network, systems and facilities unless such intrusion or access is due to Orange's failure to implement a zone-based security firewall policy into the Edge Router.

1.4.6 **Flexible SD-WAN Selfcare.** Subject to the following conditions, Customer may nominate certain Users to be given access to Orange's online Flexible SD-WAN Selfcare management tool during the Service Term in order to view certain information (e.g. inventory of devices connected to the Overlay Network, the Overlay Network configuration, and the Network's operational status, volume of data, and performance measures, etc.) and to make Service requests (including changes to the Service).

(a) Customer is responsible for monitoring each User's access to and use of the Flexible SD-WAN Selfcare management tool;

(b) The Customer will, and will ensure that each such User will: (i) maintain the secrecy of his or her Flexible SD-WAN Selfcare management tool login credentials (e.g. username, passwords, access codes, etc.); (ii) not share his or her login credentials with others; and (iii) comply with Orange's instructions regarding the use of the Flexible SD-WAN Selfcare management tool;

(c) All Service change requests made by the Users via the Flexible SD-WAN Selfcare management tool will be deemed authorized by Customer, and Customer will be responsible for payment of all Charges relating to the Service change requests;

(d) Customer is solely responsible for monitoring and validating all Service requests and other activities transacted by the Users via the tool and the effects of Orange's fulfillment of the Service requests; and

(e) Orange will not be liable or responsible for any consequences of its fulfillment of any Service requests, including (without limitation) any adverse impact on the Services or failure meet any Service Levels for the Flexible SD-WAN.

1.4.7 **Customer Care Services.** Orange will provide Incident management and change management in accordance with Service Management standard features described in the Service Description for Service Management. The optional Service Management features (as described in the Service Description for Service Management) do not apply to the Service unless Customer orders such optional features. Unless otherwise expressly set forth in the Order(s) or Charges Schedule for the Service, the charges for the Service Management provided by Orange are in addition to the Charges for the Service. Additional charges will apply to the remediation of any Incident that was not caused by Orange.

1.5 Optional Service Features

All Flexible SD-WAN features described in this Clause 1.5 are optional. The Charges for these optional features are in addition to the Charges for the Overlay Network components and features described in Clause 1.4 and in Exhibit A (SD-WAN Module 1 - Fortinet® SD-WAN Technology).

1.5.1 **Flexible SD-WAN Gateways.** When feasible (as determined by Orange), Customer may elect to connect certain Locations to a Gateway so that the Customer's WAN can connect to the Underlay Connectivity.

1.5.2 **Orange-provided Underlay Connectivity.** In lieu of providing the Underlay Connectivity for the Software-Defined WAN, Customer may procure from Orange the Underlay Connectivity for a Location. The Underlay Connectivity can be: (a) a broadband or dedicated Internet Access that Orange will install at the Location and provision via its Vendor Managed Service Internet Service, (b) a Business VPN Service installed at the Location, or (c) an Internet-based Access Circuit provided as part of the Internet Platinum Service installed at the Location. For clarity, Vendor Managed Service Internet, Business VPN Service and Internet Platinum Service are separate services and are not part of Flexible SD-WAN.

1.6 Customer Responsibilities

1.6.1 The installation and delivery of the Service is conditioned upon Customer promptly providing all information reasonably requested by Orange, including (without limitation) complete and accurate Location address and contact information Customer's representative at the site and information regarding the Customer-provided Underlay Connectivity (e.g. access technology, bandwidth, configuration, Internet-based access line speed, etc.). If the information provided by Customer is incorrect or incomplete and causes Orange to incur additional costs or change one of the Service components (e.g. Underlay Connectivity information given by Customer is incorrect and results Orange needing to get a different Edge Router model) in order to deliver the Service, then Orange may – before proceeding to install the Service – require a Customer to submit a change Order to address any additional Charges for the Service and any changes to the Service.

1.6.2 Customer will comply with all instructions provided by Orange for the Service. Customer will not connect any equipment to the Service (other than Edge Routers provided by Orange) unless approved by Orange in advance and in writing.

1.6.3 Customer will ensure that its systems, network equipment and applications are compatible with the Service.

1.6.4 Customer will obtain all permits and authorizations from the relevant government authorities to enable communicating computers or other host devices to exchange or transmit traffic via IPSec virtual tunnels.

1.6.5 Customer will comply with all applicable laws and regulations and will obtain all licenses, permits or other approvals that are needed in order for Customer to use the Service, including (without limitation) the permits and certificates to allow Customer and the Users to use IPSec enabled devices and encryption technology.

1.7 Limitations

1.7.1 Orange will not be responsible or liable for any Incidents caused by: (a) any products or services not provided by Orange; (b) Underlay Connectivity components provided by Customer; (c) Customer's implementation of the firewall and security rules, filters, and policy routing, or (d) Customer's failure to comply with its obligations as set forth in this Service Description.

1.7.2 Customer will not, and it will not permit any Users to, use the Service to collect traffic flows on behalf of a third party. Any violation of this Clause 1.7.2 is a material breach of the Agreement.

1.8 Charges

One-time and monthly recurring Charges apply to the standard and optional features of the Service. Orange will invoice the monthly recurring charges in advance for 2 months at a time. Notwithstanding anything to the contrary otherwise contained in the Agreement, the Charges for the Service will not be subject to any benchmarking or price review throughout the Service Term.

1.9 Service Term

Notwithstanding anything to the contrary otherwise contained in the Agreement (including the definition of Order Term in the General Conditions), regardless of the SD-WAN Technology that Customer chooses for the Flexible SD-WAN, the Order Term of the first Order for the Service placed by Customer will be a minimum of 36 months, and all subsequent Orders for the Service will be coterminous with the first Order. Unless otherwise agreed upon by the Parties in writing (which may be in a new Order that sets forth Customer's recommitment to a new, extended Order

Term applicable to all Service Locations on a coterminous basis), upon the expiration of the Order Term for the first Order, all Orders will renew on a month-to-month basis, except that Orange reserves the right to modify the applicable Charges for the Service.

EXHIBIT A SD-WAN MODULE 1 - FORTINET® SD-WAN TECHNOLOGY

ExA.1 Definitions

This SD-WAN Module for Fortinet® SD-WAN Technology (hereinafter "**SD-WAN Module**") describes the standard and optional features of the Overlay Network service when it is provided by Orange using Fortinet hardware, software or services (e.g. FortiGate® appliance, FortiManager®, FortiAnalyzer®, etc.). The Fortinet®, FortiGate®, FortiManager® and FortiAnalyzer® trademarks are owned by Fortinet, Inc. and are used with permission. All capitalized terms used but not defined in this SD-WAN Module will have the meanings given to such terms in the Service Description for Flexible SD-WAN. In the event of any conflict between the definitions provided herein and those provided in the Service Description, the definitions set forth herein will control for purposes of this SD-WAN Module.

"**Branch Office Location**" means – when the WAN is configured according to a hub-and-spoke network topology – a Location that branches out from a Data Center Location, whereby the Data Center Location is the central hub site and such branch Location is the spoke site.

"**Data Center Location**" means – when the WAN is configured according to a hub-and-spoke network topology – the hub Location from which the Branch Office Locations that are directly connected thereto branches out. The Data Center Location is the central Location where the WAN traffic that Branch Office Locations transmit to each other intersect.

"**Dual Light HA**" means the Overlay Network at a Location has two Edge Routers, and each router is connected to a single Underlay Connectivity access circuit. For clarity, Customer is responsible for procuring and installing the Underlay Connectivity access circuit at the Location unless Customer orders the access circuit from Orange.

"**Dual Profile**" means the Overlay Network at a Location consists of two Edge Routers, and each router is connected to an Underlay Connectivity access circuit via switched ports. For clarity, Customer is responsible for procuring and installing the Underlay Connectivity access circuit at the Location unless Customer orders the access circuit from Orange.

"**Fortinet**" means Fortinet, Inc.

"**HTTPS**" means Hypertext Transfer Protocol Secure protocol.

"**IKEv2**" means Internet Key Exchange version 2.

"**SSH**" means Secure Shell protocol.

"**SSL**" means Secure Sockets Layer.

"**Service Description**" means the Service Description for Flexible SD-WAN to which this Service Module is attached.

"**Single Profile**" means the Overlay Network service at a Location consists of a single Edge Router.

"**SSL VPN**" means Secure Sockets Layer virtual private network.

"**TLS**" means Transport Layer Security.

"**VNF**" means virtual network functions.

ExA.2 Standard Features

This Clause ExA.2 describes the standard features of the Overlay Network when it is provided by Orange using Fortinet® hardware, software or services. The standard features described in this Clause ExA.2 supplements the standard Flexible SD-WAN service elements described in Clause 1.4 (Overlay Network Standard Service Elements) of the Service Description.

ExA.2.1 **Site Types.** The Overlay Network can be installed at a Location that is designated by Customer as a Data Center Location or a Branch Office Location.

ExA.2.2 **Site Profiles.** A Location's Overlay Network can be implemented with a Single Profile, Dual Profile, or Dual Light HA. Dual Light HA is available only on certain types of Edge Routers.

ExA.2.3 **Edge Router.** If the Overlay Network at a Location has a Dual Profile, each Edge Router can be connected to up to 3 Underlay Connectivity access media (e.g. optical fiber, copper, wireless 4G, broadband or dedicated Internet access, MPLS, etc.). Customer is responsible for procuring and installing the Underlay Connectivity access circuits at the Location unless Customer orders the access circuits from Orange.

ExA.2.4 **Customer LAN interconnection.** The Overlay Network is delivered to the Location using an Ethernet link. The routing between Edge Router and Customer's LAN is configured with static routing. Subject to Orange' validation and additional charge, Customer may request eBGP routing in lieu of static routing.

ExA.2.5 **No IPv6 Support.** The Overlay Network does not support IPv6 internet protocol.

ExA.2.6 **SD-WAN Business Policy.** The standard setup of the Overlay Network includes a single SD-WAN policy that will be applied to all Data Center Locations. The standard setup of the Overlay Network includes a single SD-WAN policy that will be applied to all Branch Office Locations. Customer can specify up to 30 routing rules per policy to define how traffic will be routed through the WAN. Subject to additional Charges, Customer can order up to 5 additional policies.

ExA.2.7 **Security Policy.** All Edge Routers for all Data Center Locations will have one security policy. Likewise, all Edge Routers for all Branch Office Locations will have one security policy.

ExA.2.8 **Selfcare Management Tool Data Availability.** Information made available by Orange through the Flexible SD-WAN Selfcare management tool can be viewed by Customer for a period of ninety (90) days from the date that such information first becomes available in the tool.

ExA.2.9 **Branch Office Location Firewall Policy**

(a) The Edge Router for the Branch Office Locations will be configured with a firewall policy to filter inbound and outbound internet traffic, and traffic transmitted between Locations. Flow-based inspection mode in the firewall policy is used to identify and block detected possible security threat.

(b) Application control filters and controls the internet-based applications (e.g. gaming, upgrades, etc.) using whitelisting and blacklisting mechanisms. Up to three (3) different profiles can be defined.

(c) SSL inspection with certificate intercepts SSL/TLS encrypted internet traffic and inspects the header information (up to the SSL/TLS layer) of the packets to apply filtering decision.

ExA.2.10 **Flexible SD-WAN Selfcare Dashboard.** Customer can use the Flexible SD-WAN's Selfcare dashboard to view the operational status of the Overlay Network and its components. For example only, Customer can use the Selfcare dashboard to view the: (a) the Edge Router's connectivity status to the FortiManager® or the IPSec virtual tunnels; (b) the firewall security rules that are implemented into an Edge Router; (c) the applications' network bandwidth consumption; (d) models of network devices installed in the WAN; (e) Incident and change management cases; (f) the bandwidth of the IPSec virtual tunnels; and (g) the bandwidth of Internet access or wireless 4G access Underlay Connectivity.

ExA.3 Optional Features

Subject to availability at the time of the order and additional Charges, Customer can order the following optional Overlay Network features:

ExA.3.1 **Connectivity Options**

(a) **IPSec Tunnel to Third Party Network.** The IPSec tunneling optional feature allows Customer to securely connect a Location to third party network using the IKEv2 IPsec-based tunneling protocol.

(b) **Remote VPN Access.** The remote VPN access optional feature enables the Users' communication devices with Internet connection to establish remote access VPN connection to Customer's network using SSL VPN. Customer must provide the SSL VPN authentication server through which the endpoint device client connects securely to the Internet. If Customer wants to authenticate the Users' network access, Orange can provide Customer with a list of available authentication methods upon request. Each User communication device is limited to 250 concurrent remote sessions, and there will be an additional Charge if Customer wants additional remote sessions.

ExA.3.2 **Security Options**

(a) **WebFiltering.** The WebFiltering optional feature filters URLs to control the Users' access to certain websites in order to minimize the risk of web-based attacks. The WebFiltering option uses blacklisting mechanisms to prevent the Users from accessing malicious or unsafe URLs, IP addresses or domain names. For encrypted traffic, category-based filtering extracted from the SSL certificate blocks access to certain website categories (e.g. social media websites, gaming sites, video streaming, etc.).

(b) **Threat Protection Light.** The Threat Protection Light security option mitigates the risks of workstation or server vulnerabilities by working to detect and prevent unauthorized intrusion into the network via an intrusion detection system and an intrusion prevention system, respectively. Threat Protection Light can be configured according to high-security profile, monitor-all profile, or protect-client profile, as described in Table 1 below. Detected threats are logged in the Selfcare management tool.

Table 1: Threat Protection Light Profiles

High-Security Profile	Blocks all critical/high vulnerabilities (as defined by Fortinet and detected by the FortiGate® device) impacting servers and their clients.
Monitor-All Profile	Monitors all critical/high/medium vulnerabilities (as defined by Fortinet and detected by the FortiGate® device) without blocking the associated traffic.
Protect-Client Profile	Blocks all vulnerabilities related to the User's PC against known threats (as defined by Fortinet and detected by the FortiGate® device) impacting the Users' equipment.

(c) **Threat Protection.** The Threat Protection option includes the Threat Protection Light features described in Clause ExA.3.2(b), plus the SSL inspection and antivirus features. The SSL inspection inspects the contents of up to 40% of the decrypted traffic before either blocking it or re-encrypting it for further transmission through the network. The antivirus feature inspects all incoming traffic.

(d) **Cloud Security Provider Tunnels.** The Cloud Security Provider Tunnels option allows a Location to connect via IPSec tunnels to the Zscaler's security-as-a-service cloud platform or Palo Alto's Prisma Cloud. This option does not include subscriptions to any Zscaler or Palo Alto cloud services or other service offerings, and

Customer is solely responsible for purchasing such services directly from these companies. Customer must provide Orange with necessary information to enable the configuration of the IPSec tunnels connections. Customer must provide at least one Internet access to connect the Location to the Zscaler or Palo Alto cloud.

(e) **Cloud VNF Option.** The Cloud VNF option extends the SD-WAN network fabric of a Location that has a Single Profile or Dual Profile by deploying and utilizing a Customer-provided Fortinet® virtual machine to the Microsoft Azure, Google Cloud Platform, or Amazon Web as a virtual datacenter. For clarity, this optional service does not include subscriptions to any Microsoft Azure, Google Cloud Platform, or Amazon Web Services cloud services or other service offerings, and Customer is solely responsible for purchasing such services directly from these companies. The Cloud VNF option is not available if the Location has a Dual Light HA profile. The Location must have either a single or dual Internet access Underlay Connectivity, which Customer must provide unless it orders the Internet access from Orange. Orange will inform Customer of the Fortinet® virtual machine model that Customer must provide.

ExA.3.3 **Co-Management Options**

(a) **EMS Access Option.** The EMS access option gives certain Customer network administrator(s) nominated by Customer with either a read-only access or read-write access to the EMS. If Orange provides Customer with read-write access, the changes that Customer will be permitted to make will be limited to the ones that are listed in the change catalog that Orange will provide upon request. Customer is solely responsible for the effects of all changes that it implements.

(b) **Edge Router Access Option.** The Edge Router access option gives Customer remote access to the Edge Router in read-only mode via SSH protocol or HTTPS protocol. Orange configuration information and network traffic information (e.g. IP addresses of the Orange POPs, etc.) accessed by Customer are Orange confidential information, and Customer is not authorized to disclose of such information to any third parties.

(c) **User Authentication Method Option.** Customer can enhance the application control, remote VPN access, and web filtering by subscribing to the user authentication method option. This option will configure the FortiGate® device to requests the Users who try to access Customer's WAN to authenticate themselves with the Customer-provided server.

ExA.3.4 **Reporting Options**

(a) **Security Advanced SD-WAN Reporting Option.** The Security Advanced SD-WAN Reporting option lets Customer view near real-time and historical information about detected threats, most visited websites, and security features (e.g. antivirus, intrusion prevention system, intrusion detection system, and web filtering). The duration of data retention and the Charges for this optional feature will be quoted by Orange on a case-by-case basis depending on Customer's desired data storage parameters (e.g. Customer has 10 sites; Customer wants 2GB of data storage; Customer wants stored data maintained for 4 months, etc.) and the scope of the Service (e.g. activated security features, connectivity options, etc.) ordered by Customer.

(b) **Logs Forwarding Option.** The Logs Forwarding via Syslog option, which is implemented on the Edge Routers, sends reports concerning traffic data (Firewall/NAT), security events, and the Overlay Network to a server that Customer must provide, install and maintain on its premises. Customer must use Syslog protocol to view logs. All Network-related (i.e. the Orange backbone network) information are filtered out from the logs before they are sent to the Customer-provided server.

(c) **Logs Archiving Option.** Data collected by the EMS are stored by Orange for 3 months, and data collected by the Selfcare management tool are stored for 7 days. The amount of data that can be archived depends on the size of data storage capacity (e.g. 1GB, 1TB, etc.) and estimated storage duration (e.g. 6 months, 1 year, etc.) requested by Customer, and the Charges for this option will be quoted by Orange on a case-by-case basis depending on the logs archiving parameters requested by Customer. Customer will provide Orange with the names and contact details of the Customer network administrators who will allowed to access the data.

(d) **SNMP Monitoring Option.** The SNMP Monitoring option permits Customer's IT service management or other network monitoring tools to retrieve information from the Edge Router using SNMP Version 3 protocol. SNMP Version 1 and Version 2 traps are not supported by this option. Requests are only authorized on the RFC 1213-MIB and FortiGate® MIB.

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

Name of the Service: Flexible SD-WAN

This Description of Processing applies to the Processing of Customer Personal Data for the provision of **Flexible SD-WAN**.

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 each Service, such as recording, organization, modification, combination.

Subject Matter of the Processing Activities	Duration
Activating and implementing the Services and changes to the Services. Delivering, operating, and managing the Services (including intrusion detection and monitoring the Services if ordered by Customer). Incident management and support.	For the necessary period to provide the Service plus 6 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 Services.

Types of Customer Personal Data to be Processed	**Contact Data:** first name, last name, 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. **Traffic/Connection Data:** data revealing a communication's origin, destination, route, format, size, time duration, IP address, time zone setting, MAC address.
Categories of Data Subjects	Employees of Customer and of its Affiliates.
Authorized Sub-Processors	Orange Business Affiliates in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated to Customer.
	Orange Business suppliers in the EU and outside of the EU Processing Customer Personal Data for the purpose of this Agreement and communicated to Customer.

END OF SERVICE DESCRIPTION FOR FLEXIBLE SD-WAN