PUBLICATION 1 SERVICE DESCRIPTION FOR DDOS PROTECTION CLEANPIPE BY ORANGE 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 in this Service Description will control for purposes of this Service Description.

"**Baselines**" refers to the set of traffic behavioral identification gathered from the traffic statistics (network telemetry data) retrieved by network collectors from all peering and transit routers, which are sent to analyzers, where a network-wide view of possible traffic and network anomalies are constructed.

"**BGP**" means the Border Gateway Protocol (BGP), which is the protocol backing the core routing decisions on the Internet.

"**Cleaning Center**" means the Orange Business Services platform that cleans malicious traffic and is managed by the CyberSOC.

"**CyberSOC**" means the Security Operations Centre (SOC) within Orange.

"**DDoS**" refers to 'distributed denial-of-service,' which occurs when attacks are launched as an attempt to exhaust the victim's resources (which can be network bandwidth, computing power or operating system data structures), by flooding the resources with overwhelming malicious traffic or bogus applications that could disrupt or disable Internet-based usage.

"**DDoS Alert**" refers to a notice of a sign of possible DDoS observed from the traffic patterns, monitored either by Customer or Orange.

"**DDoS Protection Cleanpipe by Orange Service**" or "**Service**" means the related security services as described herein.

"**Defense Model**" refers to the specific mechanism deployed to counter a DDoS, as described further in Clause 1.3.1.

"**Enhancement Features**" refers to the features that enhance the Defense Models as described further in Clause 1.3.2.

"**Protection Perimeter**" refers the threshold jointly established by Orange and Customer founded on the Baselines where DDoS Alert will be triggered.

"**Web Portal**" means the Orange web interface that allows Customer and Orange to register, follow and close DDoS incidents.

"**SOC**" means Security Operations Centre (SOC) which is a centralized unit that deals with security issues on an organizational and technical level. Such an organization is called CyberSOC within Orange.

"**Traffic Monitoring**" refers to the service feature described in Clause 1.3.2(a).

"**Trusted Orange**" refers to the service feature described in Clause 1.3.2(b).

1.2 Service Overview

1.2.1 DDoS Protection Cleanpipe by Orange Service ("**Service**") is intended to help Customer reduce the impact of DDoS attacks by applying the appropriate countermeasures under the chosen Defense Model, and thereby maintaining Customer's business continuity.

1.2.2 The Service is operated from several platforms built on Arbor Networks technology which manages the Cleaning Centers. The platforms are located strategically to protect Customer's connectivity to the Internet and are equipped with high scrubbing capacity dedicated to cleaning traffic.

1.3 Service Features

1.3.1 Defense Models

1.3.1.1 The following Defense Models are available:

(a) **Blackholing.** Orange will block all traffic destined for Customer as far upstream as possible, sending the diverted traffic to a "black hole" where it is discarded. Although this Defense Model helps free up the network interface, legitimate packets are discarded along with malicious attack traffic.

The traffic-block will cease after Orange and Customer agree that the detected DDoS is over.

(b) **Cleanpipe.** Orange will redirect traffic to the Cleaning Center, and apply the appropriate countermeasures as may be agreed by Customer for the particular DDoS attack reported.

Traffic re-routing: the Cleaning Center announces the prefix of the range if IP addresses to all peering and transit routers via BGP. BGP performs IP address per IP address (/ 32). Only traffic to the attacked network component will be rerouted to the Cleaning Center. All other traffic to Customer follows the normal routing path.

Countermeasures: based on the type of DDoS attack analyzed, CyberSOC will identify the appropriate measure(s) to counter the attack. Orange will apply such countermeasure upon confirmation by Customer of the recommended countermeasures. CyberSOC will monitor the progress of the DDoS attack and will contact Customer in the event that the applied countermeasure requires modification in order to better defend against the DDoS attack.

The countermeasures that may be deployed include the following:

- Black/white list.
- Payload filter.
- HTTP Mitigation (Malformed HTTP filtering, HTTP Request Limiting, HTTP Object Limiting).
- Zombie removal.
- TCP SYN authentication.
- TCP Connection Reset.
- DNS (Malformed DNS filtering, DNS Authentication).
- Baseline enforcement.
- Shaping (rate limitation to drop packets above a given bits per second (bps) or packets per second (pps) threshold).

When Orange and Customer agree that the attack is over, the BGP will stop the announcement and all traffic will resume its normal path. All countermeasures will be lifted and Orange will close the DDoS attack incident.

1.3.1.2 **Commencement of defense mechanism deployment**

The relevant mechanism will be deployed when a DDoS Alert:

(a) is observed by Orange under the Cleanpipe model with Trusted Orange;

(b) is raised by Orange and confirmed by Customer under the Blackholing and Cleanpipe models, where Customer has ordered Traffic Monitoring;

(c) is raised by Customer to Orange in the case where Customer has not ordered Traffic Monitoring.

1.3.2 **Enhancement Features**

(a) **Traffic Monitoring.** Orange offers traffic patterns monitoring as a feature of all the Defense Models. It is an optional feature for the Blackholing and Cleanpipe models but is a requisite for the Cleanpipe model with Trusted Orange.

When Traffic Monitoring is subscribed, Orange will supervise and monitor Customer's traffic patterns against the Baselines on 24x7 basis. Whenever a DDoS Alert is observed, Orange will notify Customer by telephone.

(b) **Trusted Orange.** With the Trusted Orange enhancement, not only will the traffic rerouting process commence immediately upon observation of a DDoS Alert, the appropriate countermeasures that Orange deems fit will also be applied instantaneously. This immediate reactive manner helps reduce the DDoS impact at the earliest possible stage, while Customer is notified in parallel.

1.3.3 **Other Service Components**

1.3.3.1 **Reporting**

(a) **Incident-specific report**. Within 1 Business Day after closure of a DDoS attack incident, Orange will furnish Customer with a report detailing the duration of the attack, the level of criticality (according to the categorization of the Customer), and the countermeasures applied.

(b) **Monthly summary report.** Within the first 10 Business Days of the month, Orange will furnish Customer with a summary of the consolidated DDoS attack incidents in the previous month. The report will set out how the DDoS attacks were detected, how each of the attacks was handled, and provide recommendations on possible improvements that may be performed on Customer's network or other preventive measures that Customer may request to prevent future DDoS attacks.

1.3.3.2 **Change Management**

(a) **Change of Defense Model and/or Enhancement Features**

- When an upgrade is requested (from Blackholing to Cleanpipe, from Defense Model without Enhancement Feature to Defense Model with Enhancement Feature(s), or from single Enhancement Feature to complete Enhancement Features), the Service Term for the upgraded Service shall start afresh for the longer of 12-months from the date of the applicable Order or the end of the original Service Term.
- When a downgrade is requested, Customer must commit to a Service Term that generates no less than 100% of the Charges under the original Service Order.

(b) **Change of Protection Perimeter.**

- For deletion of one or more applications or IP addresses, there will be no reviews of the countermeasure scenarios. Orange will perform such deletion within seven (7) Business Days of receiving the request from Customer.
- For modification or addition of applications or IP addresses, a review of the countermeasure scenarios may be required, without additional Charges. Subject to the extent of change required, the implementation may take up to six (6) weeks from the time of the request.

1.4 Service Requirements

1.4.1 Provision of information. Customer shall provide to Orange:

- all relevant technical specifications and documentation regarding its existing IT infrastructure; and
- a list of identified security contact persons who may request support through CyberSOC or the Web Portal and to whom any DDoS attack incidents will be reported.

1.4.2 Coordination. Customer shall cooperate with Orange to:

- perform a situation analysis to identify and evaluate Customer's existing IT infrastructure in order to assess what needs to be changed or adjusted for Customer to receive the Service;
- identify the suitable level of protection needed for areas in the Customer's IT infrastructure that are vulnerable to DDoS attacks;
- determine the threshold activities to trigger a DDoS Alert and countermeasures activation;
- define the characteristics of DDoS attacks against which the appropriate countermeasures will be applied;
- analyze the Baseline and adjust as necessary the threshold of alert and countermeasure activation in order to improve the false positives rate thereby reducing the rejection of legitimate traffic in a traffic rerouting exercise;
- conduct validation tests on the identified countermeasures before commencement of the Service to technically stimulate the setup of the Baselines; and
- perform, whenever requested by Orange, certain basic checks intended to help speed up the diagnosis of any malfunction of Customer's IT infrastructure.

1.5 Conditions and Limitations of Service

1.5.1 The Service does not include any Internet access connection(s) or any equipment necessary for Customer to make such connection. Any Internet access service provided by Orange to Customer will be described in a separate Service Description, which is subject to separate Charges.

1.5.2 Orange reserves the right to modify and update the features and functionality of the Service. These updates may include any subsequent release or version of the Service containing functional enhancements, extensions, error corrections, or fixes. Updates will not automatically include any release, option, or future product which may be sold separately or which is not included under the applicable Defense Model.

Where practicable, Orange will give Customer prior written notice of any material modification or update, and will reasonably ensure that any modifications or updates do not materially degrade the performance of the Service or Customer's use of the Service or require Customer to incur any additional cost to continue its use of the Service. Orange will use reasonable efforts to implement all such modifications or updates in a manner that minimizes the impact on the use of the Service.

1.5.3 The Service will enable Customer to continue having access to Internet service during a DDoS attack. However, Orange does not guarantee that there will be no degradation in the performance of the Internet service.

1.5.4 Customer acknowledges that legitimate traffic may be dropped if the Protection Perimeter set is too aggressively. Orange does not guarantee a zero false positive rate, and Orange shall not be held liable for any such legitimate traffic drop.

1.5.5 Traffic rerouting at the time of a DDoS attack may cause Customer to get a suboptimal traffic path.

1.5.6 For the Cleanpipe Defense Model, the countermeasures can only handle DDoS attacks up to 100 Gbps of attacks on layer-4 over Transmission Control Protocol ("**TCP**") and 50 Gbps of attacks on layer-7 over TCP. There is no limit for volumetric attacks over User Datagram Protocol ("**UDP**").

1.6 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: DDoS Protection Cleanpipe

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.).	No
Organization (organizing personal data in a software program, etc.).	No
Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.).	No
Modification (modifying the content or the way the personal data are structured, etc.).	No
Consultation (looking at personal data that we have stored in our files or software programs, etc.).	No
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.	No
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.).	No
Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.).	No
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).	No
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.	Yes

ExA.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	
Incident Management.	No	
Quality of Service.	Yes	
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.	Yes	For the duration of the hosting service ordered by Customer.
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

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.

END OF SERVICE DESCRIPTION FOR DDOS PROTECTION CLEANPIPE BY ORANGE SERVICE