## PUBLICATION 1 SERVICE DESCRIPTION FOR FLEXIBLE SSL 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.

"**Customer Information**" means the Customer information to which Users will have access through the Flexible SSL Service.

"**Device**" means the unit (e.g. smartphones/laptops/kiosks) from which a User may connect to the Flexible SSL service to access the Customer Information. Orange will identify and may modify from time to time the Devices that may be used with the Flexible SSL Service.

"**External Network Link**" means the network link, including the router, provided by Orange as part of the Flexible SSL Service, allowing to connect the SSL gateway to the internet.

"**Fault**" means a fault, failure, or malfunction in the Flexible SSL Service.

"**Fault Call**" means the notification made by Customer to the GCSC to report a Fault.

"**Firewall**" means a method to enhance network security.

"**GCSC**" means the Orange Global Customer Support Centers.

"**Incident**" means a security event, alert, or problem regarding the Flexible SSL Service detected by Orange.

"**Internal Network Link**" means t the network link, including the router, provided by Orange as part of the Flexible SSL Service, allowing to connect the SSL gateway to the customer's internal network using the Orange MPLS backbone.

"**Portal**" means he Flexible SSL Care Service web portal.

"**Proper Operational Condition**" means that the Flexible SSL service is functioning in accordance with the parameters of the Flexible SSL Service, as set forth in this Service Description and in the SRFs.

"**Security Rules Base**" means the ordered set of rules against which each connection is checked, which is configured in SSL Gateway. The Security Rules Base will be determined by Customer's security policy, as set forth in the SRF.

"**Service Request Form**" of "**SRF**" means the form that details Customer's specific Flexible SSL Service requirements.

"**Severity Level**" means the category assigned by the GCSC for Incidents and Faults.

"**SSL Gateway**" means the centrally managed server, including Software, provided by Orange as part of the Flexible SSL Service, on which the Security Rules Base is configured and to which Users connect to access the Customer Information.

### 1.2 Description of the Flexible SSL Service

The Flexible SSL Service provides Users with secure access to Customer Information from a Device using a web browser or dedicated software supported by the Service. The Service will be delivered by Orange in accordance with the Service Level Agreement for Flexible SSL Service. Users remotely connect to the SSL Gateway through the infrastructure provided by Orange Business Services as part of the Flexible SSL Service. The Flexible SSL Service includes:

- the SSL Gateway,
- the Firewall protecting the Flexible SSL architecture from internet,
- an External Network Link,
- an Internal Network Link.

The Security Rules Base implemented on the SSL Gateway allows different Users to access specific Customer Information. Depending on the Security Rules defined by the Customer using the Portal, the Users may experience either a clientless access and may be asked to use dedicated connectivity software provided by the SSL Gateway. If due to technical constraints, it is not possible to publish Customer Information in accordance with what has been defined in the Security Rules Bases, Orange reserves the right to amend the publication type and to implement "client based" connectivity instead of a clientless connectivity. Except as otherwise expressly provided in this Agreement, Orange will have no responsibility or liability for, or related to, the Customer Information, Devices, Internet browsers, authentication services, or other services not provided by Orange, but that may be used or accessed by Customer or Users in connection with the Flexible SSL Service. The service is only available as a fully hosted solution in Orange premises.

### 1.3 Service Request Form

1.3.1 **Customer Requirements.** Prior to commencement of the Flexible SSL Service, the Parties will complete the applicable SRF. Customer will provide all relevant technical specifications and documentation regarding its existing network, and Orange will reasonably assist Customer in completion of the SRF. Customer will ensure that all information contained in the completed SRF is accurate.

1.3.2 **Customer Security Contacts.** Customer will identify a primary security contact and two secondary security contacts in the SRF. Customer will ensure that all primary and secondary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week. Orange will respond only to Flexible SSL Service requests and Fault Calls issued by such contacts. All communications between the Parties will be in English, unless otherwise agreed to by the Parties.

For Severity Level-1 and Severity Level-2 Incidents, Orange will notify Customer's security contacts of the Incident using the contact details provided in the SRF. For Severity Level-3 Incidents, Orange will send a message to the email addresses set forth in the SRF. All contacts by Orange will be made in English, unless otherwise agreed to by the Parties.

The primary security contact identified in the SRF will ensure that:

(a) All security contact information is maintained and current;

(b) Orange is notified before and after any planned outages or configuration changes to Customer's network or network services; and.

(c) All changes to Customer's primary security contact must be made in writing, on Customer's letterhead, and be signed by a senior manager in Customer's organization.

**1.4 Service Deployment**

1.4.1 **Lead Time Requirements.** The time to deploy the Service is measured only when Orange has received both a signed Order and a fully completed SRF. The time to deploy the Service is two weeks as of receipt by Orange of the two documents. The deployment will be delayed if Customer does not provide both documents or if the Customer requires changes to the specifications listed in the completed and accepted SRF.

1.4.2 **Configuration.** Orange will configure the SSL Gateway exclusively based upon specifications contained in the applicable SRF. Any configuration changes required due to inaccurate or revised specifications will be charged to and paid by Customer at the Hourly Labor Rate for such services, plus Expenses.

Following service opening, Orange will accept requests for changes to the configuration of the SSL Gateway only from the security contacts identified in the SRF. All such changes will have to be requested through the Flexible SSL Care Service web portal ("**Portal**").

1.4.3 **Installation.** The installation of the Flexible SSL Service consists in the connection of the Flexible SSL platform to the Customer's MPLS network. Considering the little impact of such connection, the Flexible SSL Gateway connection to the Customer's MPLS network will be conducted during Business Hours unless otherwise agreed to by the Parties. If Customer requests Orange to connect the Flexible SSL Gateway outside of Business Hours, Orange will advise Customer of any increased charges prior to commencement of the installation.

Orange will not be responsible for any delay in the connection of the SSL Gateway if such failure is due to any cause beyond its reasonable control, including the inability of Orange to get the relevant required technical information from the Customer.

1.4.4 **Server Upgrades.** Orange will provide version management of the operating system and various elements of the SSL Gateway Software, which may include upgrades to a new operating system level. Notwithstanding anything to the contrary contained herein, Orange has no obligation to provide all new releases of Software from the SSL Gateway hardware vendors and Software licensors, and Orange, in its sole discretion, will decide when upgrades take place.

If Orange needs to take a SSL Gateway off-line to implement Software updates or network enhancements, Orange will provide at least 7 days prior written notice of such events. When possible, Orange will work with Customer to minimize any impact this could have. When possible, Orange will implement SSL Gateway upgrades during Business Hours.

1.4.5 **Acceptance Testing.** Upon completion of the installation of the SSL Gateway, Orange will commence its own acceptance testing, which will confirm that all aspects of the Flexible SSL Service are operational in accordance with the terms of this Service Description and the parameters set forth in the SRF. Upon completion of this internal acceptance testing, Orange will send to the security contacts listed in the SRF a "Welcome mail" confirming that the Flexible SSL service is ready to be used and operational.

1.4.6 **Security Policy Changes Procedure.** Following installation and acceptance testing, Orange will accept requests for changes to the Security Rules Base only from the security contacts identified in the SRF. All such changes will have to be requested through the Portal. If Orange requires additional information to finalize the implementation of the change, Orange reserves the right to contact the primary security contact to agree to the appropriate actions, timeframes, and charges, if applicable. Any potential conflict in the Security Rules Base or any inadvertent reduction in the security effectiveness perceived by Orange will be brought to Customer's attention, and Orange will recommend alternative strategies.

Orange will require the following information for any changes to the Security Rules Base:

(a) Completed change control form in the Portal;

(b) Supporting details relevant to the specific change action, if applicable; and

(c) Contingency plans and contact details of Customer personnel performing acceptance testing for the changes to the Security Rules Base.

### 1.5 Standard Service Features

When using the Flexible SSL Service, Users will access a Web portal sign-in page, where they will be required to identify the information requested for authentication (e.g. username and password). Different Users will be allowed to access, or will be denied access to, specific Customer Information based on the Security Rules Base implemented on the SSL Gateway. The Flexible SSL Service will also encrypt the traffic between the Device and the SSL Gateway and will support basic security features and authentication services that may be provided by Customer, as identified and as may be modified by Orange from time to time. Customer may download periodic reporting for the Flexible SSL Service from the Portal.

Orange also will provide up to 3 administrator software tokens with the standard Flexible SSL Service to get access to the Flexible SSL Care Service web portal ("**Portal**").

### 1.6 Optional Service Features

Orange may provide the following optional features, subject to additional Charges and the availability of the option.

1.6.1 **Pre-Production environment.** The Pre-Production environment is a temporary replication of Customer's production environment to do various tests (version upgrade, configuration changes, etc.) without impacting the production. Each time the option is ordered, the Pre-Production is available for a single month for 10 concurrent users only.

1.6.2 **Service Manager.** As for the other Orange services, the Service Manager is the Customer's primary point of contact within Orange. The Service Manager provides Customer with a monthly dashboard and reporting analysis and is responsible for the verification of the Service performance. SLA for the Service will only apply if the Customer has ordered a Service Manager.

### 1.7 Maintenance of the SSL Service

1.7.1 **Remedial Maintenance.** Orange will maintain the hardware portion of the Flexible SSL service in Proper Operational Condition. If a Fault is caused by a failure in any Flexible SSL service component, Orange will repair the Fault following receipt of a Fault Call or upon detection of the Incident by Orange, whichever occurs first.

The GCSC will classify all Fault Calls and Incidents as follows:

| | |
|---|---|
| **Severity 1** | Problems causing critical impact to the business function(s) or customer(s). Justifies immediate management attention and dedicated resources applying continuous efforts to resolve as soon as possible. |
| **Severity 2** | Problems causing degradation of service resulting in impact to business function of customer. Impact justifies priority attention and application of resources to resolve in a timely manner. |
| **Severity 3** | Problems causing low impact to the business function(s) and customer(s). Requires timely resolution to minimize future impacts. Resources should be allocated in accordance with normal managerial planning prioritization. |

1.7.2 **Remedial Maintenance Exclusions.** Orange will have no obligation to provide Remedial Maintenance Services for, nor will Orange be liable to Customer for damages for loss of the Flexible SSL Service or the SSL Gateway caused by any of the following (collectively "Limitations"):

(a) Damage to the SSL infrastructure caused by any Force Majeure Event, or any other casualty or loss;

(b) Any instability in the operation of the SSL Gateway that is caused by or related to the use of certain software, or by any other software provided by Customer or its designees, or by combinations of the SSL Gateway and software, even if such combination is specified on a duly accepted SRF.

(c) Fault calls and Remedial Maintenance Services rendered necessary by the above causes may be performed by Orange at Customer's request, and will be charged to and paid by Customer at the Hourly Labor Rate, plus Expenses.

Remedial Maintenance Services do not include:

(a) Maintenance of attachments or other devices not specified in the SRFs.

(b) Correction of software databases and/or programming errors or any errors or damages caused by or arising out of input or error, except as otherwise set forth in this Service Description.

### 1.8 Pricing

One-time and monthly recurring Charges apply to the Flexible SSL Gateway Service and to each optional feature. The monthly recurring Charges will vary depending on the number of concurrent Users of the Flexible SSL Gateway Service and on the number/type of declared applications.

### 1.9 Geographical and Legal Service Availability

Being based on SSL/TLS standards, this Service is embedding cryptographic software. Depending on the country the Users will connect from, the use or import of such materials may be subject to specific conditions. The Customer will verify whether it is legally allowed to use the service in his country.

### 1.10 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: Flexible SSL**

### 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.). | No |
| 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. | 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.). | 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.). | 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 |
| 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. | 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. | No | 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 |

### 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 FLEXIBLE SSL SERVICE**