1.1 Web Content Protection Service

1.1.1 **Definitions.** All capitalized terms used but not defined herein will have the meanings given to such terms in the Service Description or Service Level Agreement for Business VPN Service, or 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.

"**Administrator**" means the Customer personnel who are responsible for the administration and monitoring of security, web usage, and related policies with regard to the WCP Service. The Administrator will be identified in the SRF.

"**Authorized Users**" will have the meaning defined in Clause 1.1.8.1 (Number of Users) of this Service Description.

"**Base User Population**" means the total number of Users specified in the first Order for the WCP Service.

"**HTTP**" means Hypertext Transfer Protocol.

"**HTTPS**" means Hyper Text Transfer Protocol Secure.

"**Incident**" means: (a) a fault, failure, or malfunction in the WCP Service that is reported by Customer to the GCSC, or (b) a security-related event, alert or problem with the WCP Service that is reported by Customer to the GCSC.

"**Internet User**" means a User of the WCP Service who accesses the Internet.

"**IT Infrastructure**" means Customer's information technology (IT), networks, and systems (including network elements such as LAN, proxies, etc.) that are used by Customer to provide the Internet Users with access to the Internet.

"**LDAPS**" means Secure Lightweight Directory Access Protocol.

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

"**Portal**" means the self-service web portal that an Administrator or a Super User may access in order to administer the WCP Service.

"**Required Consent**" means any license, consent, permit, authorization or approval that is necessary in order to give Orange the permission, right or license to access, use, or modify any hardware or software that Customer may provide to Orange in connection with the WCP Service without infringing the ownership, intellectual property (including patent and copyright) or licensing rights of the software licensor.

"**SAML**" means Security Assertion Markup Language.

"**Service Request Form**" or "**SRF**" means the form that details Customer's specific WCP Service technical requirements.

"**SSL**" means Secure Socket Layer.

"**Super User**" means an Administrator or other Customer-authorized personnel who are responsible for implementing, enforcing, and managing the Internet Users' compliance with the Customer security policy that is configured into the WCP Service.

"**URL**" means Uniform Resource Locator, which is the address that defines the route to a file on the World Wide Web or any other Internet facility.

"**WCP Nodes**" means the shared infrastructure platform used by Orange to deliver the WCP Service.

"**Web Content Protection Service**" or "**WCP Service**" means the Service described in this Service Description.

"**Web Filtering**" or "**WF**" means the process that filters web pages and attachments using URL categorization and content analysis.

1.1.2 **Overview.** The Specific Conditions for Network Services apply to the WCP Service. WCP Service only provides the features and functionalities set forth in this Service Description. WCP Service, which is an optional service feature of Business VPN Service, gives Customer the ability to set up security policy and filtering rules for Internet browsing. In order to subscribe to WCP Service, Customer must also order Business VPN Service and Business VPN Internet Service. For clarity, Business VPN Service and Business VPN Internet Service, which are described in separate Service Descriptions, are not included in the WCP Service.

1.1.3 **Customer Responsibilities**

1.1.3.1 **Customer Requirements.** The Parties will complete the applicable SRF. Customer will provide Orange all relevant technical specifications and documentation regarding its existing IT Infrastructure and will ensure that all information contained in the SRF is complete and accurate.

1.1.3.2 **Customer Security Contact.** In each SRF, Customer will identify a primary security contact, and this person will be designated as an Administrator. In addition, Customer will identify between 2 and 4 secondary security contacts, and these personnel will also be designated as Administrators and will belong to the Super User group. Customer will ensure that all Administrators (including those who are designated as primary and secondary security contacts) are available and can be contacted by Orange at all times. The Users will report all Incidents to the Administrators. The Administrators are responsible for calling the GCSC to report any Incidents. The GCSC will only respond to Incidents and service requests reported by an Administrator to the GCSC by telephone or via the Portal. All communications between the GCSC and the Administrators will be made in English, unless otherwise agreed in writing by both

Parties. Customer will notify Orange of any changes to the primary security contact in writing, on Customer's letterhead, and such notification must be signed by a senior manager in Customer's organization.

The primary security contact will ensure that: (a) all security contact information contained in the SRF are up-to-date, and (b) Orange is notified before and after any planned outages or configuration changes to Customer's IT Infrastructure or network-related services.

1.1.3.3 **Acceptable Use Policies.** Customer is solely responsible for all Users' usage of the WCP Service and access to the Internet. Customer is also responsible for ensuring that all Users are aware of, and comply with any Customer acceptable use policy and the Orange Policy. Customer will defend, hold harmless and indemnify Orange against any and all Losses arising out of or related to any breach or alleged breach by Customer, Users, or Customer's permitted users (including Internet Users) of any Customer acceptable use policy or the Orange Policy. Customer will immediately notify Orange upon learning of any violation of the Orange Policy or any Customer acceptable use policy.

1.1.3.4 **Software and Equipment.** WCP Service includes Software that is licensed by a third party. Orange will, only for the Service Term of the Order for the WCP Service, either grant to Customer and the Users or obtain on Customer's behalf, non-exclusive, non-perpetual and non-transferable license to use the Software, in object form only, strictly for the purpose of allowing Customer and the Users to use the WCP Service. Customer authorizes Orange to procure the necessary license from the Software licensor (including entering into the end user license agreement with the Software licensor) on behalf of Customer and the Users. If the provisioning of the WCP Service requires Orange to use or modify any Customer-provided equipment (including, program, software, or hardware), then Customer will obtain and provide all Required Consent. Orange will be excused from performance of any of its obligations that may be affected by Customer's failure to promptly obtain and provide such Required Consent.

1.1.3.5 **Technical Integration**

1.1.3.5.1 Orange will work with Customer to determine the level of Orange effort needed to integrate and setup the WCP Service into the IT Infrastructure. Depending on the level of effort and the scope of the WCP Service implementation project, Orange may either provide Customer with a project plan that outlines the steps and activities that the Parties will undertake to implement the WCP Service, or send to Customer's technical contact or an Administrator an e-mail to explain the necessary technical changes that Customer needs to make to the IT Infrastructure in order to implement and use the WCP Service.

1.1.3.5.2 Customer will supply Orange with all technical data and all other information that Orange may reasonably request to allow Orange to supply the WCP Service.

1.1.3.6 **Internet Access.** The WCP Service does not include the provisioning by Orange of any Internet service or any equipment (e.g. modem) that may be necessary for Customer to access the Internet. If Customer requires Orange to provide Internet access, then Orange will provide the Internet access as a separate Orange service, and the Charges for the Internet access are separate from and in addition to the Charges for the WCP Service.

1.1.3.7 **Service Developments**

1.1.3.7.1 Orange may modify and update the features and functionality of the WCP Service. These updates may include any subsequent release or version of the WCP Service containing functional enhancements, extensions, error corrections, or fixes.

1.1.3.7.2 Scheduled Maintenance of the WCP Service will generally be carried out on Saturday or Sunday. If Orange needs to perform Scheduled Maintenance during other days, then it will do so between the hours of 8:00 pm CET and 8:00 am CET.

1.1.3.8 **Acceptance Testing.** Orange will start the Acceptance Test after the WCP Service is installed. The Acceptance Test will verify that the WCP Service is operational and is in compliance with the parameters set forth in the SRF. Orange will provide Customer with a Service Acceptance Form after the Acceptance Test is successfully completed. The Service Acceptance Form will identify the test performed by Orange. Notwithstanding anything to the contrary set forth in the Agreement, the WCP Service is deemed accepted by Customer on the date that Orange issued the Service Acceptance Form unless Customer informs Orange in writing of a material fault in the WCP Service no later than 5 Business Days after Customer's receipt of the Service Acceptance Form, and it is shown that Orange caused the material fault.

If Customer informs Orange during such 5-Business Day period that there is a material fault in the WCP Service and Orange caused the fault, then Orange will fix the fault and re-perform the Acceptance Test. For clarity, Orange is not responsible for correcting any fault caused by Customer, the IT Infrastructure, or any software or equipment provided by Customer.

1.1.3.9 **Service Availability.** Web Content Protection Service is not available in some countries such as Russia, Egypt, United Arab Emirates, Kuwait, Saudi Arabia, and Qatar. Orange will confirm the availability of the WCP Service in a certain country at the time Customer orders the WCP Service or upon request.

1.1.4 **WCP Packages & Features.** Customer can subscribe to standard WCP package, advanced WCP package, or premium WCP package, as described in Clause 1.1.4.2 (WCP Service Packages). Each WCP package includes the shared features described in Clause 1.1.4.1 (Shared Features).

1.1.4.1 **Shared Features.** WCP Service includes the shared features described in Clause 1.1.4.1.1 (Traffic Forwarding) through Clause 1.1.4.1.3 (Directory Connectivity).

1.1.4.1.1 **Traffic Forwarding.** The traffic forwarding feature handles web request via a connection between the Orange-managed CPE Router and a WCP Node. Internet traffic is forwarded according to whether Customer uses transparent Internet breakout, explicit Internet breakout, or transproxy Internet breakout.

1.1.4.1.2 **Initial Security Setup.** Orange security personnel will perform the initial security setup of the WCP Service using the Customer-provided security policy and other pertinent information specified in the SRF. If information is missing, the Orange security personnel will set up the WCP Service using the default configuration.

If a Customer request Orange to develop a security policy and Orange agrees to do so, then the development of such security policy will be provided via the Orange Professional Services. Such Professional Services are separate from the WCP Service, and all charges for Professional Services are in addition to the charges for the WCP Service.

1.1.4.1.3 **Directory Connectivity.** Orange will configure the directory connectivity feature during the implementation of the WCP Service, and Customer will assist and cooperate with Orange to activate the feature. The directory connectivity feature sets up an automatic interconnection between the WCP Service and Customer's LDAPS or SAML directory, and it allows Customer to interconnect up to two (2) active directories provided that the directories are in active mode. For clarity, the directory connectivity feature does not support active/passive architecture. Orange is not responsible or liable, and Customer assumes and is solely responsible, for any data leakage that may arise from the interconnection between the WCP Service and the LDAPS or SAML directory.

1.1.4.2 **WCP Service Packages.** Customer can order standard, advanced, or premium WCP Service package. The features included in each package are described in Clause 1.1.4.2.1 (Standard WCP Package) through Clause 1.1.4.2.3 (Premium WCP Package) below.

1.1.4.2.1 **Standard WCP Package.** Standard WCP Service package includes the following features:

(a) **User Management.** The user management feature allows an Administrator to manage the Internet Users or groups of Internet Users to ensure that each User only has one account for WCP Service. This feature only works if the directory connectivity shared feature described in Clause 1.1.4.1.3 (Directory Connectivity) is set up to support the User Management feature. Customer acknowledges and agrees that: (i) the WCP Service is priced on per-User basis, (ii) it is responsible for ensuring that each User only has one WCP Service account per User, (iii) Orange or its third party service provider may check the User activity to verify that each User only has one (1) account, and (iv) Orange may increase the Charges for WCP Service without notice if any User is found to have more than one (1) account.

(b) **In-line Anti-Virus and Anti-Spyware.** The in-line anti-virus and anti-spyware feature will scan unencrypted web pages and attachments via a shared security platform that detects malware threats.

(c) **Content Filtering.** The web filtering feature will filter the web pages and attachments; provided, however, Orange does not guarantee that the WCP Service will be able to filter all web pages or attachments. URLs are categorized by reference to a number of predefined categories, as specified in the Portal.

The Administrator is responsible for: (i) configuring the web filtering tool to create access restriction policies based on categories and types of content, and (ii) applying the restriction policies to certain Internet Users or groups of Internet Users. The web filtering feature also lets an Administrator implement additional filters such as "blocked" list and "allowed" list. The Administrator may configure the web filtering tool so that certain web sites are not filtered.

Encrypted traffic such as HTTPS traffic or SSL traffic cannot be filtered, and the encrypted traffic will be allowed to pass through. The web filtering feature will only filter web pages that the Administrator has chosen to filter using the Portal.

An Internet User who tries to access a web page or attachment that is blocked by the web filtering's access restriction policies will receive an automatic alert web page informing such User that access is denied. The Administrator can also set up the WCP Service to notify the Administrator via email of the denial of access incidents.

1.1.4.2.2 **Advanced WCP Package.** The advanced WCP Service package includes the features described in Clause 1.1.4.2.1 (Standard WCP Service Package), plus the following features:

(a) **Browser Control.** Browser Control lets the Administrator limit the Internet Users' choice of Internet browsers according to the list of permitted browsers that Administrator configured on the Portal. For example, the Administrator can block the Internet Users from using older browser versions (e.g. blocking the Internet Users from using Microsoft Internet Explorer 5 and allowing them to only use Microsoft Internet Explorer 6). The Administrator is responsible for implementing the appropriate Browser Control configuration and for maintaining such configuration. After the Browser Control configuration is set up, the WCP Service will verify whether a web browser is on the list of permitted browsers. The Browser Control cannot filter browser versions that are not on the list of permitted browsers. Subject to prior approval of Orange in order to avoid any configuration problem, the filtering of new browser version based on the browser's user agent may be possible.

(b) **SSL Inspection.** The SLL Inspection feature allows the Administrator to decipher SSL flows and detect the security threats.

(c) **Advanced Threat Protection.** The Advanced Threat Protection feature complements the antivirus feature described in Clause 1.1.4.2.1(b) (In-line Anti-Virus and Anti-Spyware) by offering protection against botnets, phishing, or malware hidden contents (in ActiveX, Ajax, Flash, and JavaScript).

(d) **Cloud Application Control.** The Cloud Application Control feature allows the Administrator to control the usage of some applications, browsers, macros, and messages. For example, Cloud Application Control allows the Administrator to block instant messaging from webmail (e.g. blocking Google Talk instant messaging service that is integrated into Gmail) and certain applications (e.g. blocking Facebook Games from Facebook). Applications that are not included in the Cloud Application Control blacklist will not be filtered.

(e) **Bandwidth Management.** The Bandwidth Management feature gives the Administrator bandwidth control based on cloud applications, specific websites, and the type of traffic or file size being transferred. The bandwidth control module can control the maximum, minimum, and concurrent sessions bandwidth allocated for large file download, streaming, web conferencing, and VoIP) either globally or per Location.

1.1.4.2.3 **Premium WCP Package.** The premium WCP Service package includes the features described in Clause 1.1.4.2.1 (Standard WCP Service Package) and Clause 1.1.4.2.2 (Advanced WCP Package), plus the Data Loss Protection feature. The Data Loss Protection feature allows the Administrator to determine and control the exit of sensitive enterprise contents (data type, keywords, expressions, etc.) using HTTP or HTTPS.

1.1.4.3 **Optional WCP Features**

1.1.4.3.1 **12-Month Log Retention.** The WCP Service will retain Internet User logs of traffic metadata, Internet User and company binary identifiers, and other traffic information (e.g. if an Internet User sends email through Gmail, the WCP Service only logs information about the transaction; it does not log the email content) for 6 months regardless of whether Customer has ordered standard, advanced or premium WCP package, and Customer hereby gives Orange permission to collect, retain and discard such Internet User logs. To the extent applicable laws require the Internet Users to be notified of the collection, retention or deletion of Internet User logs, then Customer is solely responsible for notifying the Internet Users and (if necessary or required by applicable laws) for obtaining the consent of the Internet Users. After the 6-month period, the oldest logs will be overwritten by new entries. As an optional service feature and subject to an additional Charge, Orange can extend the log retention period from 6 months to 12 months. In all cases, Customer is solely responsible for the retention of all URL in accordance with applicable laws.

1.1.4.3.2 **Security Change Management.** Subject to additional Charges, Customer can engage an Orange security consultant to implement security policy changes and filtering rules into the Portal.

1.1.5 **Self Service Web Portal & Support**

1.1.5.1 **Self Service Web Portal.** Customer will specify in the SRF the specific Administrators and Super Users who are to be given access to the Portal. The Portal is an HTTPS website and the authorized users must enter a valid password in order to access the Portal. If one or more Administrators or Super Users share a Portal access account, then Customer can give each Administrator or Super User a unique login credential, and Customer can also determine the scope of the access privileges given to each Administrator or Super User (e.g. read-write access right or read-only access right).

1.1.5.2 **Portal Functionality.** Depending on the WCP Service package that Customer has purchased (e.g. standard, advanced or premium package, as described in Clause 1.1.4, WCP Service Packages) and the scope of the Administrator's or Super User's Portal access right, the Portal lets the Administrator or Super User:

- view available statistics of all malware and web contents blocked by the WCP Service;
- create Internet access restrictions;
- customize browser alert pages seen when access to a web site or file is denied;
- update the administration details for real-time e-mail alerts;
- configure the reporting and auditing system;
- view available automated reports such as overall Internet traffic, bandwidth utilization, and blocked URLs, and web malware;
- schedule regular reporting of certain activities performed by the WCP Service features described in Clause 1.1.4 (WCP Service Packages);
- subject to Orange validation, set up distribution (via email) of certain reports to identified Internet Users;
- configure the Portal to create a log of changes to the administration rights, WCP Service configuration, filtering rules, and security policy so long as the Administrator or Super User has a read-write access to the Portal; and
- set up the Portal to create a log of web pages blocked by the filtering policy or to exclude certain personally identifiable information (e.g. username and IP address) from the log.

1.1.6 **Customer Support**

1.1.6.1 **Service Request and Incident Reporting.** The Administrator will submit all service requests for administrative support (e.g. helping an Administrator activate the WCP Service features described in Clause 1.1.4) concerning the WCP Service via the Portal. However, in case the WCP Service is out of service or if the nature of service request cannot be processed via the Portal, the Administrator will contact the GCSC to request assistance. The GCSC will log and manage all service requests made by an Administrator; provide the Administrator (by email or telephone) a

service request case number; and escalate (if needed) the service request to other Orange fix agents or support team for resolution.

Customer is responsible for reporting to the GCSC any problem with the WCP Service. Upon request, Customer will provide the GCSC agents with information (e.g. log files, configuration files, error messages, etc.) necessary for Orange to fulfill the service request or resolve the reported WCP Service problem.

1.1.6.2 **Customer Responsibility.** Customer will follow the Orange instructions concerning the installation, operation and the use of the WCP Service and the implementation of corrective actions. Orange is not responsible for Service failure if Customer does not carry out a corrective action recommended by Orange.

The GCSC may close the service request ticket if Customer does not provide the GCSC with the requested information within a reasonable period of time.

GCSC customer support does not cover: (a) the provisioning of a service, feature or functionality that is outside the scope of the WCP Service described in this Service Description, (b) resolution of problems not caused by Orange (e.g. a fault in IT Infrastructure), and (c) resolution of problems that cannot be reproduced by the Orange incident management team.

1.1.7 **Order**

1.1.7.1 **Minimum Service Term.** Each Order for WCP Service must have at least a 12-month "Order Term". The Order Term will start from the date that the Acceptance Test described in Clause 1.1.3.8 (Acceptance Testing) is successfully completed.

1.1.7.2 **Early Service Termination.** Notwithstanding anything to the contrary set forth in the Agreement, if Customer terminates the Service Term for convenience before the end of the Service Term, then it must give Orange at least 90 days' written notice using the Orange-prescribed Order termination form and pay Orange the following early termination Charges:

1.1.7.2.1 If the Service Term (as indicated on the Order) is 12 months, then Customer will pay Orange: (a) all unpaid Charges for the WCP Service that Orange provided up to the actual disconnection of the WCP Service; and (b) all Charges associated with the unused portion of the Service Term.

1.1.7.2.2 If the Service Term (as indicated on the Order) is more than 12 months, and Customer terminates the Service Term before the end of the Service Term, then it will pay to Orange: (a) all unpaid Charges for the WCP Service that Orange provided up to the actual disconnection of the WCP Service; (b) all Charges associated with the unused portion of the first 12-month period of the Service Term; (c) 50% of all Charges associated with the remaining portion of the Service Term; and (d) all charges and fees that Orange may be liable to pay to any third party.

1.1.7.3 **Change Orders**

1.1.7.3.1 Except as set forth in this Clause 1.1.7.3, during the Order Term, the only changes to the Order that Customer may request (via an Orange-prescribed change order form) without being required to add a 12-month period to the current Order Term are to add new Users to the WCP Service or to upgrade the WCP Service package (e.g. upgrading from WCP Service standard package to WCP Service advanced package).

1.1.7.3.2 If Customer requests a WCP Service package downgrade (e.g. downgrading from WCP Service advanced package to WCP Service standard package) during the Order Term or Extended Term, or if Customer reduces the total number of Users before the end of the first 12-month period of the Order Term, then such service package downgrade or reduction in number of Users will constitute an early termination by Customer of the Order for WCP Service for Customer's convenience. In either event, Customer: (a) must give Orange at least 90 days advance written notice of the package downgrade or User reduction and such prior notice is in lieu of the early Service termination prior notice requirement specified in the General Conditions, (b) will pay Orange all early Service termination charges specified in Clause 1.1.7.2 (Early Service Termination) in connection with the early termination of the Order, (c) sign and submit to Orange the Orange-prescribed change order or order termination/cancellation form, and (d) must sign and submit to Orange a new Order for WCP Service in connection with the package downgrade or User reduction, and such new Order must have at least a 12-month Order Term. For clarity, the conditions specified in parts (b), (c), and (d) of this Clause 1.1.7.3.2 must be satisfied in order for the package downgrade or User reduction to take effect and for Orange to change the Charges for the WCP Service to correspond to the package downgrade or User reduction, as the case may be.

1.1.7.3.3 If Customer reduces the total number of Users after the end of the first 12-month period of the Order Term, and so long as the aggregate total of all Users dis-enrolled and Users to be dis-enrolled from the WCP Service during the Order Term and any Extended Term is less than 10% of the Base User Population, then Customer does not need to extend the Service Term of the existing Order for WCP Service for an additional 12-month period. However, if the aggregate total of all Users dis-enrolled and Users to be dis-enrolled from the WCP Service during the Order Term and any Extended Term is equal to or more than 10% of the Base User Population, then: (a) such reduction in number of Users will constitute an early termination by Customer of the Order for WCP Service for its convenience pursuant to Clause 1.1.7.2 (Early Service Termination), in which case Customer will comply with all of its obligations specified under Clause 1.1.7.2. For clarity, the total number of Users to be removed from the WCP Service and the total number of Users that have been previously removed from the WCP Service will be added together to determine whether the cumulative total of dis-enrolled Users is less than, equal to, or more than 10% of the Base User Population.

1.1.8 **Pricing.** The Charges for WCP Service are based on the total number of Users, the type of WCP Service package (i.e. standard package, advanced package, and premium package), Internet bandwidth surcharge, and the optional features selected by Customer.

1.1.8.1 **Number of Users.** The monthly recurring Charges for WCP Service are dependent upon the total number of Users specified on the Order or Charges Schedule, as the case may be (such Users hereinafter referred to as "**Authorized Users**"). If the actual total number of Users (as determined by Orange) is more than the total number of Authorized Users (the excess Users hereinafter referred to as "**Unauthorized Users**"), then Customer must, immediately after being notified (including notification via email or the Portal) by Orange of such event, either:

(a) submit an Order for WCP Service in connection with the Unauthorized Users, for the remainder of the initial Order Term; or

(b) change the existing Order for WCP Service in accordance with Clause 1.1.7.3 (Change Orders).

If Customer does not comply with either part (a) or part (b) of this Clause 1.1.8.1 (Number of Users), then Orange may exercise one or both of the following remedies upon 30 days' notice (including notification given to Customer via email or through the Portal):

(c) suspend the WCP Service without further notice; or

(d) invoice Customer, retroactive to the date that Orange discovered the Unauthorized Users, the Charges for WCP Service corresponding to the Unauthorized Users, and such Charges will be calculated according to the following formula: [total number of monthly recurring Charges for WCP Service ÷ total Authorized Users] × total number of Unauthorized Users.

1.1.8.2 **Bandwidth Surcharge.** In addition to the Charges described in the foregoing Clause 1.1.8.1 (Number of Users), Orange will also invoice Customer, and Customer will pay Orange, monthly recurring bandwidth surcharge fees on a per User basis depending on the country or geographic region where the Users are located. The per-User monthly recurring bandwidth surcharge fee will be specified on the Order or Charges Schedule.

Table 1: WCP Service Packages

Packages	**Feature Name**				
Shared Features	Traffic Forwarding	Initial Security Configuration	Directory Connectivity		
Standard	User Management	Inline Anti-Virus & Anti-spyware	Content Filtering		
Advanced (+ Standard Features)	Browser Control	SSL Inspection	Advanced Threat Protection	Cloud Application Control	Bandwidth Management
Premium (+ Standard & Advanced Features)	Data Loss Protection				
Options	Security Change Management	1 year reporting extension	Consulting services		

1.1.9 **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 the Web Content Protection 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: Web Content Protection - International

ExA.1 Processing Activities

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

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

Categories of Personal Data Identifiable by Orange	
Categories of Personal data identifiable by Orange.	Yes
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).	No
Location Data (geographic location, device location).	Yes
Customer Relationship Management data (billing information, customer service data, ticketing info, telephone recordings, etc.).	No
Financial data (bank account details, payment information).	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.	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.	Yes	For the duration requested by Customer.
Hosting.	No	
Other. [if yes please describe]	No	

ExA.4 Purposes of Processing

Provision of the service to Customer.

ExA.5 Categories of Data Subject

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

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.