

## PUBLICATION 1 DATA PROTECTION CLAUSES

### 1.1 Definitions

References herein to “**Data Controller**”, “**Data Processor**”, “**Data Subject**”, “**Processing**” and “**Personal Data**” will have the meanings as set out in (or to the nearest equivalent term in) the Data Protection Legislation.

“**Data Protection Legislation**” means the EU Regulation 2016/679 of April 27 2016 (the “**General Data Protection Regulation**” or “**GDPR**”), or secondary national laws, recommendations, guidelines or opinions with the force of law or any other applicable legislation relating to privacy or the protection of Personal Data in force, and as amended, from time to time.

### 1.2 Customer and Orange accept and acknowledge that in relation to the Services provided under the Agreement:

- (a) Customer, by specifying and procuring the Services, is a Data Controller in respect of the Personal Data of its employees and end-users which is collected or generated by Orange to provide its Services to Customer, on its instructions, and not for any other purpose; and
- (b) Orange, by providing the Services specified by Customer to Customer and its end-users, is a Data Processor in respect of any Personal Data of Customer’s employees and end-users that Orange processes in order to provide the Services, which is collected or generated by Orange to provide its Services to Customer, on its instructions, and not for any other purpose.

The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are set out generally in the Orange Privacy Policy for Customers and Prospects available on <https://www.orange-business.com/en/personal-data>, as may be updated from time to time (the “Orange Privacy Policy”), and more specifically in the Annex or Exhibit (as applicable) “Description of Processing of Personal Data by Orange Business Services as Processor for Customer – Article 28 of GDPR” attached to each Service Description.

- (c) Orange or its subcontractor, may also act as Data Controller of the Personal Data of Customer’s employees and end-users, when Orange, or its subcontractor, processes such Personal Data for its own purposes, independently of Customer’s requirements. The processing in respect of which Orange, or its subcontractor, acts as a Data Controller of Customer’s employees and end-users Personal Data are described in the Orange Privacy Policy. In addition, Orange may transfer Personal Data outside of the EU when processing Personal Data as Data Controller as explained in the Orange Privacy Policy.

### 1.3 Customer will ensure that it has given all necessary notices (which may include referring its employees and end users to the Orange Privacy Policy) and has all necessary appropriate consents in place to enable lawful transfers of the Personal Data for the duration and purposes of the Agreement and to enable Orange to lawfully provide the Services.

### 1.4 Customer and Orange each will comply with all applicable requirements of the Data Protection Legislation.

### 1.5 The obligations of Orange when acting as Data Processor, and of Customer as Data Controller, are as follows:

#### 1.5.1 Orange will comply with the reasonable written instructions of Customer in the Processing of the Personal Data provided that such instructions are lawful and are not contrary to other provisions of the Agreement and unless Orange is required by the Data Protection Legislation applicable to Orange to process Personal Data. Where Orange is relying on laws of a member of the European Union or European Union law as the basis for processing Personal Data, Orange shall promptly notify Customer of this before performing the processing so required unless Orange is prohibited by law from doing so.

#### 1.5.2 Notwithstanding anything to the contrary otherwise contained in the Agreement, Orange will implement appropriate technical and organizational security measures to protect the Personal Data against unauthorized or unlawful Processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data, appropriate to the harm that might result from the foregoing and the nature of the data to be protected, considering the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising, and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organizational measures adopted by it).

#### 1.5.3 Customer is responsible for the management of the requests of Data Subjects for the exercise of their rights under the Data Protection Legislation including, but not limited to access requests, explaining to Data Subjects how Personal Data will be processed, responding to queries or requests made by Data Subjects in connection with their Personal Data, data portability/rectification/ erasure requests, keeping Personal Data accurate and up to date and obtaining any necessary consents. Upon Customer’s written request and insofar as possible, reasonable, and proportionate, Orange will assist Customer, in: (a) responding to any request from a Data Subject and, at Customer’s cost. (b) Customer’s compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators. Orange’s assistance is conditioned upon Customer proving that Orange processes the Personal Data of the relevant Data Subject on Customer’s behalf. The persons authorized by

Customer to request Orange's assistance in respect of Data Subject requests are Customer's authorized user(s) of My Service Space, unless otherwise notified in writing by Customer.

- 1.5.4 Customer is informed that portions of the Agreement may be performed (which may include sub-processing Personal Data) by Orange's Affiliates or subcontractors, some of whom may be based outside the European Economic Area (EEA). Orange is responsible for the sub-processing and performance of all of its Affiliates and subcontractors in accordance with the requirements of the applicable Data Protection Legislation and shall ensure that such sub-processing shall be on terms substantially equivalent to these Data Protection Clauses. The list of Affiliates and subcontractors is made available as set out in the Annex or Exhibit (as applicable) "Description of Processing of Personal Data by Orange Business Services as Processor for Customer – Article 28 of GDPR" attached to each Service Description and is approved by Customer as at the Effective Date. Orange shall inform Customer of any additional or replacement Orange Affiliates or subcontractors, which will be deemed approved by Customer, unless Customer objects to such changes within fifteen (15) days of having been informed thereof. Any objection shall be made in writing to Orange and include: (a) the detailed reasons for Customer's objection; and (b) Customer's alternative proposal. Orange will consider Customer's objection and proposal and in its sole discretion, inform Customer of its decision. If Orange decides to proceed with its proposed change and Customer still objects, Orange shall provide at least one alternative proposal (not necessarily Customer's alternative proposal) including additional costs. Customer may request Orange to implement such alternative proposal of Orange at Customer's sole expense.
- 1.5.5 Orange will ensure that its employees, Affiliates, subcontractors and each of their employees, workers, and independent contractors providing Services under the Agreement will keep the Personal Data confidential.
- 1.5.6 Customer expressly agrees that Orange may transfer the Personal Data to its subcontractors and Affiliates, subject to Clause 1.5.4 and Clause 1.5.7 of these Data Protection Clauses.
- 1.5.7 Customer hereby provides its prior written consent for Orange to transfer Personal Data outside the EEA (or outside of another region or country from which the Data Protection Legislation restricts transfers of Personal Data) provided that:
- (a) Customer or Orange has provided appropriate safeguards in relation to the transfer;
  - (b) affected Data Subjects have enforceable rights and effective legal remedies;
  - (c) Orange complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
  - (d) Orange complies with reasonable written instructions notified to it in advance by Customer with respect to the processing of the Personal Data.
- If applicable to the Service, Customer grants a specific mandate to Orange to execute, in the name and on behalf of Customer, with its Affiliates and subcontractors the standard contractual clauses for the transfer of Personal Data to processors established in third countries as set out in the European Commission decision of February 5 2010 (C (2010) 593), so that such Personal Data are covered by an adequate level of protection.
- 1.5.8 During the Term of the Agreement, Orange will maintain records and information to demonstrate its compliance with these Data Protection Clauses and will:
- (a) on thirty (30) days prior written notice provide to Customer reasonably and readily available information to demonstrate its compliance, always provided that Orange shall not provide any information which relates to Data Subjects for which Customer is not the Data Controller; and
  - (b) except as otherwise provided in the Agreement, on sixty (60) days prior written notice agree to schedule audits that Customer may conduct, provided that:
    - (i) audits are subject to Orange's data protection and security policies and processes and any other measures needed to protect the confidentiality of Orange's customers or Data Subject's privacy and are at Customer's cost;
    - (ii) Customer shall undertake no more than one audit in any rolling twelve month period;
    - (iii) Orange may schedule an audit on a mutually agreed date;
    - (iv) any audit shall be conducted during Orange's normal business hours and shall not exceed two days;
    - (v) prior to any audit, Customer will provide details of its audit plan to the Orange Global Security Organization and the Orange Global Data Protection Officer (DPO) for their review and approval (which will not be unreasonably withheld). The scope of the data protection audit will be mutually defined and agreed to in writing by both Parties and must be approved by the Orange Global Security Organization and the DPO. The approved audit plan will be documented and shall describe in detail the scope of the audit and the complete names and functions of the auditors and other Customer personnel (collectively, the "Customer Audit Team") who may require access to the Orange assets. The Customer Audit Team must follow the approved audit plan and shall not make any changes without a written approval of the Orange Global Security Organization and the DPO.
    - (vi) The Customer Audit Team will not disrupt Orange operations and business activities in any way.
    - (vii) The selection of Customer's external auditors will be mutually agreed between Orange and Customer.

- (viii) Orange will use commercially reasonable efforts to assist Customer in the audit so long as it does not:
  - (1) impose undue administrative or financial burden upon Orange,
  - (2) cause Orange to incur additional costs or expenses (e.g. requiring Orange personnel to travel to meet with the Customer Audit Team),
  - (3) disrupt Orange business operations or the performance of any Services or the services that Orange provides to other Orange customers.
- (ix) For the protection and security of Orange personnel, customers, service providers, facilities, business operations and business records, the Customer Audit Team shall not record, copy, film, photograph, or remove (each as applicable) from Orange premises any materials, records, reports, documentations, personnel, or any portion of the facilities without the prior written consent of Orange. A breach of this covenant shall be deemed a material breach of the Agreement, and Orange may:
  - (1) demand that Customer immediately return to Orange any materials, records, reports, documentations, film, photograph (or any copy or record thereof), and
  - (2) take any legal remedies available under the Agreement or at law or in equity.
- (x) Orange personnel may accompany the Customer Audit Team to the audit sites. The Customer Audit Team shall comply with verbal or written instructions from Orange regarding access to Orange facilities and to the different areas within the facilities. The Customer Audit Team shall also comply with Orange security, health and safety and such other applicable policies and procedures.
- (xi) Within ten (10) business days following the end of the audit, Customer shall provide Orange with a copy of the audit report at no cost to Orange.

In the event of any conflict between the terms of this Clause 1.5.8 and the terms of the Agreement with respect to audits, the terms of the Agreement will control.

- 1.5.9 Orange will notify Customer without undue delay when it becomes aware of a Personal Data breach. The notification will be made by encrypted email (using PKI Certificates, or ZED Container, or ZIP file password protected).
- 1.5.10 At Customer's request, which must be contained in the termination of service letter, Orange will delete or return to Customer all the documents and files containing Personal Data after the end of the provision of services relating to processing, and shall not retain any copy of the data, unless required to do so by applicable law.
- 1.5.11 Where Customer acts as Data Controller, Customer is responsible for and will comply with all obligations imposed on Data Controllers by applicable Data Protection Legislation and for ensuring that the use of the Services by Customer and its end-users does not result in a breach of such obligations.
- 1.6 Where Orange as Data Controller, Orange is responsible to answer requests of Data Subjects for the exercise of their rights under the Data Protection Legislation, Customer will provide all assistance requested by Orange to confirm the identity of the Data Subject and the validity of the request.

## END OF DATA PROTECTION CLAUSES