GENERAL CONDITIONS OF OPERATION
OF THE MOBILE ID SERVICE

Article 1 - FOREWORD

Orange has developed a solution called “Mobile ID”, which aims to make customer experiences on Service Providers’ websites simpler and more secure, through the reuse of information collected by Orange from its Internet and Orange mobile subscribers.
Subscription to the Mobile ID solution by the Partner assumes the full acceptance of these terms and conditions and their appendices.

Article 2 - DEFINITIONS

For the purposes of this Contract, the following terms shall have the following definitions:

“Eligibility API”:
Refers to the functionality, provided as an optional part of the FormID Service, the Match ID Service, the SIM Verify Service, the Number Verify Service and the Home Verify Service, that enables the Partner requesting it to see whether the End User is eligible or ineligible for the Mobile ID Service. The Partner may query the Eligibility API upstream of the Mobile ID Service use cases, provided that this does not itself constitute a Mobile ID Service use case. It is specified that no reason for ineligibility will be communicated to the Partner.

“Co-contractor” or “Partner”:
The legal person identified in Appendix H hereto, who by signing the aforesaid Appendix H becomes a co-contractor of Orange and unreservedly accepts these general conditions of operation of the Mobile ID Service by Orange under the conditions laid down in the Contract.

“Contract”: all the requirements set out in these General Conditions which are supplemented by the appendices numbered from A to J:

- Appendix A Mobile ID Service Description
- Appendix B Technical Conditions
- Appendix C Security Requirements for the Partner Network
- Appendix D Orange Security Requirements
- Appendix E Brands
- Appendix F Tariff Conditions
- Appendix G Form Identifying Service Providers
- Appendix H Partner Form
- Appendix I Security Questionnaires
- Appendix J Orange Customer Experiences

The terms of the Contract express the full agreement between the Parties relating to the subject-matter of the Contract. They shall prevail over any previous version and over any proposal or exchange of letters prior to signature, as well as any other stipulation contained in documents exchanged between the Parties and relating to the subject-matter of the Contract.

"End User Data": the data listed in Appendix A, Description of Services, that may be provided to the Partner and Service Providers under the Mobile ID Service of this Contract. Only the Data referred to on the Form duly validated by Orange shall be submitted by the Partner to the Service Provider referred to on the Form.

"Security Breach": any event compromising the Security of the Mobile ID Service or the End Users' Personal Data.

"Form": the document in Appendix G hereto, to be duly completed (including the Service Provider's customer experiences) and signed by the Partner and subject to prior validation by Orange prior to making the Mobile ID Service available by the Partner to the Service Provider.

"Application Programming Interface" or "API": the set of coded instructions that specify how Partner and Service Provider software must interact with the Mobile ID Service. These instructions are made available by Orange.

"MSISDN" or "Mobile Station International Subscriber Directory Number": the mobile phone number of the End User holding an Orange mobile subscription attached to the SIM card.

"Orange Digital ID Platform": the Orange-operated platform that allows the Mobile ID Service to be supplied to the Service Providers and to which the Partner can be interfaced using the API.

"Mobile ID Service" or "Orange Service" or "Service": the digital ID service using End User Data, which is provided by Orange to the Partner for the Service Providers' needs. This service consists of five use cases made available to the Service Providers at the request of the Partner as described in Appendix A, which are:

- the Form ID Services
- the Match ID Service
- the SIM Verify Service;
- the Home Verify Service
- the Number Verify Service

"Service Provider": the Partner's customers, online service publishers, whether from the public or private sector, or natural or legal persons wishing to make use of the Mobile ID Service.

"Mobile Device": the portable device (such as phone, smartphone or tablet) acquired or held by the End User.

"Orange Account Holder": the End User who has a non-professional Orange subscription in their name for their personal needs. Orange subscriptions are:

- mobile Orange subscriptions in metropolitan France;
- bundle subscriptions (Mobile + Internet) in metropolitan France;
- Internet subscriptions in metropolitan France.

"End User": an Orange customer who is subscribed to mobile and/or Internet services and who may opt for services provided by Service Providers approved under the Contract.

Article 3. SUBJECT-MATTER OF THE CONTRACT

3.1 This Agreement defines the conditions under which Orange provides the Partner with the Mobile ID Service consisting of the Form ID Service, the Match ID Service, the SIM Verify Service, the Home Verify Service and/or the Number Verify Service as described in Appendix A.

3.2 It is specified that the provision of the Mobile ID Service shall only take effect when Orange expressly validates the Form. (Appendix G)

3.3 Nothing in this Contract shall be deemed to confer any kind of exclusivity on either Party in the provision of similar or identical services of the other Party, nor shall it prevent a Party from dealing with third parties.

Article 4. RELIABILITY OF SHARED INFORMATION ON END USERS

The End User Data transmitted in connection with the delivery of the Mobile ID Service is the data declared by the Orange Account Holder as part of their Orange subscription. Therefore, Orange does not guarantee the accuracy of the data transmitted to the Partner and Service Providers.

Article 5. THE PARTNER'S ELIGIBILITY CRITERIA AND THE SERVICE PROVIDERS' APPROVAL PROCESS

5.1 Partner Eligibility Criteria

In order to qualify for the Mobile ID Service, the Partner must meet the following cumulative conditions:

- their Mobile ID contract has not been suspended or terminated in the last year following a breach of their contractual obligations;
- they have paid any amount they owe to Orange;
- they have not attempted fraud against Orange;
- they respect all of the Orange Group's ethical rules and compliance policies available on orange.com, especially those regarding anti-corruption, money laundering and economic sanctions.

The Partner undertakes to return the Partner Form provided in Appendix H, duly completed and signed in two copies, to Orange using the postal address for Orange / Pay Services and the following email address: pay.services@orange.com. The Partner undertakes to inform Orange of any changes to the information contained in the Partner Form in Appendix H.

In the event that the Counterparty, during the term of the Contract, no longer meets any of the conditions listed above, the Contract may be terminated by Orange under the conditions set out in Article 6.

5.2 Service Provider Approval Process

The Partner undertakes to respect the approval process described in this article for each Service Provider of which it is an aggregator.

The Partner must send its request to Orange by email. A request must be made for each Service Provider. This request shall include the following information:

- Service Provider Identification Form duly completed and signed by the Partner (Appendix G)
- Name of the proposed Service Provider;
- A copy or link to the terms of the proposed Service Provider's privacy policy;
- A copy of each customer experience actually implemented by the Service Provider, which will be appended to this Contract (Appendix J);
- The assurance that the contract between the Partner and the Service Provider requires that the Service Provider's terms of use and privacy policy be readily accessible to End Users and that no change is made to the Mobile ID Service by the Service Provider.

Orange will give its approval by returning the dated and signed Form by e-mail.

The Partner will be required to inform Orange of any change in the information contained in the request for the supply of the Mobile ID Service of a Service Provider.

Article 6. CONTRACT PERIOD AND TERMINATION

6.1 Contract Period

This Contract shall take effect as soon as Orange signs the Partner Form (Appendix H) duly completed and signed by the Partner for an open-ended period.

6.2 Contract Termination

6.2.1. Termination without cause

Each Party may terminate this contract at any time without cause, subject to a minimum of six (6) months' advance notice, starting on the date on which the notice is sent to the other Party by certified mail with return receipt confirmed by email.

6.2.2. Early Contract termination for breach by either Party

If either of the Parties violates one of its obligations under this Contract, the non-violating Party may duly and lawfully terminate it, after a formal notice with return receipt goes unanswered for a period of thirty (30) days, and without prejudice to any damages that may be claimed by the other Party.

Furthermore, each Party may also terminate the Contract, in accordance with Article 6.2.1 above, if the other Party does not comply at all times with the principles set out in Article 18, and if the defaulting Party has not remedied the non-compliance within thirty (30) days following the formal notice to the defaulting Party.

6.2.3. End of contractual relations

If the Contract is terminated for any cause, the Contract will continue to have its effects only to permit the recovery of amounts remaining due, as applicable, by either Party on the Contract's termination date.

The Parties undertake at that date to cease any use of the elements belonging to the other Party, including brands, trade names, logos, contents, and databases, and not to keep copies except for elements necessary for the recovery defined above.

The provisions relating to Guarantees, Liability, and Intellectual Property will continue to apply even after the termination of the Contract.

Article 7. TARIFF CONDITIONS

In return for the supply of Orange's Mobile ID Service, the tariff conditions charged to the Partner will be those set out in Appendix F to the Contract.

Payments made to Orange shall be made in accordance with the following procedure: payments shall be made by wire transfer. The transmission of Orange's IBAN is subject to a specific procedure for obvious security and anti-fraud reasons, as described below:

- the Partner shall provide Orange Pay Services with its electronic contact details (last name, first name, function, email address), which will be forwarded to the Finance and Treasury Department.
- the Payment Center will send an IBAN on behalf of Orange to the person named above.

These sums must be paid in Euros (€) and must reach Orange no later than forty-five days (45) following the invoice issue date.
Any unpaid amounts due at the scheduled time will automatically result in the payment of interest on arrears. It will be calculated on the basis of the amount due multiplied by the ECB's rate + 10%, the sum of which is divided by 26. This clause cannot compromise the debt's payability. These penalties shall accrue from the first day following the payment deadline until the Partner's actual payment is deemed effective on the day on which the Orange Bank Account is credited. The ECB's rate is the overnight rate of the day after the payment should have been made.

In addition, in the event of a late payment, a lump sum payment for recovery costs will also be applied in full to the Partner, starting on the first day of delay and without prior formal notice. The amount of this indemnity shall be equal to forty (40) euros as set by Article D 441-5 of the Commercial Code on the date of the first late day.

The Partner shall have a period of one (1) month from the date of issue of the invoice to express the duly substantiated reservations that he considers necessary to Orange. Beyond that time limit, the counterparty, if any, will no longer be able to contest the invoice, which will be considered as final.

Orange is duly authorized to offset any amount unpaid by the Partner with any amount owed by Orange to the Partner or belonging to the Partner and held by Orange.

The Eligibility API option is included in the price of the Mobile ID Service.

Article 8. PERSONAL DATA PROTECTION

8.1 Definitions

For the full understanding of the following terms, the terms “Controller," “Subcontractor," “Concerned Person," “Recipient," "Breach of Personal Data," and “Processing" will have the meaning defined in the "Applicable Data Protection Laws."

Similarly, the term "Personal Data" has the meaning given to it in these same Laws.

The term "Applicable Data Protection Laws" means:

- Regulation (EU) 2016/679 of the European Parliament and of the April 27, 2016 Council (General Data Protection Regulation) repealing Directive 95/46/EC;
- where appropriate, the texts adopted by the European Union and local laws which may apply to the Personal Data processed under the Contract.

8.2 General stipulations

The Parties undertake to comply with the legal and regulatory obligations relating to the protection of their personal data in the performance of the Contract.

The Parties acknowledge that Orange is the Controller of the processing of Orange customers’ Personal Data, implemented in the performance of the contract, and that the Partner acts as Subcontractor.

The nature and scope of the Processing, the Personal Data categories, and their retention period by the Partner for the Mobile ID service are described in Appendix A.

When processing the Personal Data transmitted by Orange, the Partner acts only on documented instructions and in the context of written authorizations received from Orange.

The Partner must notify Orange immediately if, in its opinion, an instruction constitutes a violation of applicable Data Protection Laws. They must notify Orange at the following email address: pay.services@orange.com

The Parties agree that the Personal Data provided by Orange to the Partner within the framework and for the purposes of this Contract shall remain Orange’s property. The Partner will never own and shall never act as if they own the Personal Data transmitted by Orange in connection with the performance of the Contract.

8.3 Specific stipulations

The use of the Form ID Service, the Match ID Service, the SIM Verify Service and the Home Verify Service is subject to the consent of the End User, which Orange is responsible for obtaining as Data Controller.

The End User's express consent will not be required as part of the Consent Option for the SIM Verify Service and for the Match ID Service if it is demonstrated that the Service Provider has a legitimate interest and this is approved by Orange and part of the Number Verify Service option. In these cases, the Partner must explain the justification for the Service Provider's legitimate interest in the Service Provider Identification Form as provided in Appendix G.

The Partner undertakes not to proceed with processing operations other than those defined in this Contract on Personal Data transmitted by Orange in connection with its execution.

If the Partner intends to make any changes that may affect the Processing of Personal Data, the Partner undertakes to notify Orange in advance, and not to implement such modifications without its prior written consent.

The Processing carried out under this Contract involves making a third party, the Service Provider, acting as the Data Controller, the Recipient of the data. The latter is then obliged to fulfil all the obligations towards the persons concerned or towards its compliance with the regulations.

It is the Partner's responsibility to contract with this Service Provider in order to provide for the legal and technical conditions under which the Service Provider may become a Recipient of the data described in Appendix A in accordance with the provisions of this Contract.

The Partner undertakes to indicate to Orange, in any contract concluded with a Service Provider, that the Orange pages proposed in some of the options and described in Appendix J (identification / connection / validation of consent) are not modifiable.

The Partner undertakes to declare to Orange, in any contract concluded with a Service Provider, the legal conditions (in particular the possible collection of consent) and technical conditions provided for in this Contract for the Processing in question.

In any contract with the Service Provider, the Partner shall specify that Orange does not guarantee the content, availability, accuracy or any other aspect of the information provided in the Mobile ID Service, which exclusively reproduces the information declared by the Orange Account Holder.

8.3.1. Confidentiality of Personal Data

The Partner undertakes to:

- not disclose any Personal Data to a Recipient other than an approved Service Provider, whether a private or public, physical or legal person, without Orange's prior consent;
- not disclose any personal data processed under this Contract to members of its staff who do not participate in the services provided under the Contract;
- ensure that all its staff members, subcontractors and providers providing services under this Contract know and comply with the rules relating to the confidentiality and protection of Personal Data and are subject to a specific obligation of confidentiality.

8.3.2. Security, Breach of Personal Data and Notification

The Partner must take the necessary technical and organizational security measures to protect Personal Data from accidental or unlawful destruction, accidental loss, modification, disclosure or unauthorized access to Personal Data in accordance with applicable Data Protection Laws.

The Partner must notify Orange immediately after having detected or been informed by the Service Provider of a Personal Data Breach, or any security breach resulting in the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of Personal Data transmitted, stored or otherwise processed, or unauthorized access to such Personal Data.

The notification will be sent to Orange at the following email address: cert@orange.com

The notification shall specify the nature of the Personal Data Breach and its likely and actual consequences on the People concerned, the nature of the measures already taken or those proposed to remedy the Breach, the people with whom additional information may be obtained, any unaffected subsidiaries or entities of Orange and the geographical areas concerned, and, if possible, an estimate of the number of People concerned who may have been affected by the breach in question and all the elements for identifying them.

The Partner undertakes to establish, with Orange, in the framework of cooperation between the Parties, regular updates consistent with the urgency and gravity of the situation.

If one or more Service Providers are affected by the situation, the Partner shall ensure that they are involved in any exchange.

It is incumbent only on Orange, as the Controller, to inform and notify the competent control authorities and, where appropriate, the person(s) concerned by the Breach of their Personal Data. The Partner shall not notify the competent authority in Orange's place.

8.3.3. Cooperation with Orange

The Partner undertakes to cooperate with Orange:

- by providing Orange with all documentation and information it might need in the event of a referral to a regulatory authority to demonstrate its compliance with applicable Data Protection Laws;

- in the management of requests from Persons Concerned for the exercise of their rights, in particular their rights of access, correction, deletion and/or opposition, or any other request relating to the protection of their Personal Data.

- Should the Person Concerned contact the Partner directly to exercise their rights, the Partner shall communicate to Orange the request received, within seventy-two (72) hours of receiving it. The Partner shall not respond to the request of a Person Concerned without Orange's approval.

  In the event that the Person Concerned contacts the Service Provider directly to exercise his/her rights regarding the processing carried out by Orange, the Service Provider shall communicate the request to the Partner who shall pass it on to Orange under the conditions presented above.

- in carrying out an impact assessment that Orange should conduct in order to assess the risks associated with the processing of Personal Data and to identify the measures to be taken to deal with these risks and the possible consultation of the supervisory authority;

- in the event of a control or investigation by a competent supervisory authority, the Parties undertake to cooperate reasonably with each other and with the supervisory authority.
  In the event that the control exercised by the competent authority concerns the Processing carried out on behalf of Orange and in its name, the Partner undertakes to inform Orange of that control immediately after having been notified by the supervisory authority itself, and not to commit itself on behalf of Orange or in its name.
  If Orange is controlled by a competent authority, in particular with regard to the Services provided by the Partner, the latter undertakes to cooperate with Orange and to provide Orange with any information it may need to demonstrate compliance with applicable Data Protection Laws.

8.3.4. Subsequent Subcontractors

The Partner cannot subcontract all or part of the Processing of Personal Data to any Recipient without Orange's prior written consent.

The Partner shall only call upon subsequent subcontractors providing sufficient safeguards for the implementation of appropriate technical and organizational measures to ensure Orange's compliance with applicable data protection laws, and undertakes to sign with its subsequent subcontractor a written contract imposing the same

data protection obligations as those provided for in this Contract, and including obligations relating to security, confidentiality, and cooperation in case of data breaches or international transfers of Personal Data;

The Partner shall provide Orange, upon request, with a certificate guaranteeing the implementation of the obligations relating to the protection of personal data by its subsequent subcontractor and a description of the processing carried out by the subsequent subcontractor, indicating, in particular, the purposes of the processing, the categories of data processed, the categories of people having access to the data, and the storage location(s) of the data;

If the subsequent subcontractor fails to comply with the data protection obligations, the Partner, as an original subcontractor, remains entirely responsible to Orange for the proper fulfillment of the obligations of its subsequent subcontractor.

8.3.5. Transfer of Data Outside the European Union (EU)

If the Partner is located in a country not recognized by the European Commission as providing adequate protection, or is likely to transfer Personal Data transmitted by Orange to a Service Provider located in a country not offering such protection, it undertakes to comply with the formalities laid down in the applicable Data Protection Laws to regulate data transfers outside the European Union.

Personal data cannot be transferred to a third country outside the European Economic Area without Orange's prior written consent.

Orange authorizes the Partner to sign on its behalf and for its account the Standard Contractual Clauses of the European Commission, or any other instrument governing the transfer of Personal Data outside the European Union, and/or to have them signed by the Service Providers.

8.3.6. Audit

Orange reserves the right to verify compliance with the obligations and guarantees stipulated in this contract and, in particular, to request that the Partner submit its data processing capabilities, data files and documentation required for processing to an audit.

This audit shall be conducted in accordance with the procedure and modalities described in Article 5 of Appendix D (Orange Security Requirements) to this Contract.

8.3.7. Fate of Personal Data After Processing

The Partner undertakes to comply with the retention times set for the Data transmitted to it by Orange for the purposes of this Contract.

In addition, the Partner undertakes to delete all documents and files containing Personal Data after the end of the Processing provided under this Contract without delay and without further formalities and not to retain any copy of the Personal Data.

The Partner shall provide Orange, upon request, with a Personal Data Deletion Certificate.
Failure by the Partner to comply with the provisions of this Article will result in termination of the Contract under the conditions specified in Article 6. Orange will also have the right to request an injunction or other provisional remedy for any actual or potential breach of this Article, without prejudice to any other rights and remedies that Orange may have.

Article 9. INTELLECTUAL PROPERTY RIGHTS

The Partner, on the one hand, and Orange, on the other hand, will retain ownership of their own existing solutions and all associated Intellectual Property Rights (including Partner APIs, and Orange APIs related to Orange). It is expressly agreed between the Parties that no title or property relating to the history of the Parties or any associated Intellectual Property Rights shall be transferred to the other Party under this Contract.

Orange S.A. grants the Partner limited rights to Orange Services and Orange APIs.

Orange Services and Orange APIs are and shall remain the exclusive property of Orange. Orange shall grant to the Partner, for the Duration of this Contract, a global, non-exclusive, non-transferable, royalty-free license authorizing agents, representatives, Authorized Subcontractors and Service Providers of the Partner, solely in connection with the provision of the Services Subject to this Contract, to use Orange Services and Orange APIs.

The Partner grants Orange Limited Rights to the APIs of the Partner and of the Service Providers.

The APIs of the Partner and of the Service Providers are and shall remain the exclusive property of the Partner and Service Providers, respectively. The Partner shall grant Orange, for the Duration of this Contract, a worldwide, non-exclusive, non-transferable, royalty-free license authorizing agents, representatives, and subcontractors of Orange, only in connection with the supply of the Mobile ID service subject to this Contract, to use the Partner's APIs.

Article 10. TRADEMARK LICENSES

10.1Orange Brand License

Orange grants the Partner a personal, royalty-free, non-exclusive, non sub-licensable, non-transferable license to use Orange's brand, trademarks, trade names and logos as described in Appendix E ("Orange Brand"), only for the purpose of marketing and promoting Orange Services during the duration of the Contract. No other use of the Orange Brand is authorized under this Contract. Any use of the Orange Brand in any marketing or other medium must be consistent with Orange’s brands, as incorporated in Appendix E, and such use requires prior written approval from Orange.

10.2Partner Brand License

The Partner grants Orange a personal, royalty-free, non-exclusive, non-sublicensable, non-transferable usage license to the Partner's brand, trademarks, trade names and logos, as described in Appendix E (“Partner Brand”), for the sole purpose of marketing and promoting the Mobile ID Service for the Duration of the Contract. No other use of the Partner's brand is authorized under this Contract.

10.3Reputation associated with the Orange Brand and the Partner’s Brand

Each Party agrees to carry out its sales, marketing and distribution activities in such a way as to avoid any action likely to diminish or compromise the reputation, name, image, value and reputation of the other Party's brand (Orange Brand for the Partner and the Partner's Brand for Orange).

Article 11. SECURITY REQUIREMENTS

The Partner must comply with the security requirements described in Appendices C and D.

Each Party undertakes to ensure that access to its API is secure to prevent unauthorized access by third parties or unauthorized users at any time.

Article 12. INDEMNITIES

Subject to Article 13, a Party (the “Indemnifying Party") shall defend, indemnify and release the other Party (the “Indemnified Party”), as well as the respective directors, officers, staff members and agents of the Indemnified Party, from and against any claims, costs, losses, judgments and expenses (including reasonable attorney’s fees) resulting from or in relation to a third-party claim resulting from a real breach of the declarations or guarantees of that Party listed in this Contract. The Indemnifying Party's obligations are subject to the conditions under which a) the Indemnified Party notifies the Indemnifying Party in writing within a reasonable timeframe after the Indemnified Party has been notified of a claim; b) the Indemnifying Party shall have exclusive control over the defense of the claim (except where a Indemnified Party chooses to do so, it may participate on an equal footing in defense at its own expense) and all related monetary settlement negotiations (with the understanding that any non-monetary terms, including any licensing terms, or any settlement terms for a claim directly affecting the Indemnified Party shall be approved in writing by the Indemnified Party), and (c) the Indemnified Party shall provide the Indemnifying Party with the assistance, information and authorizations necessary for the Indemnifying Party to fulfill its obligations under this Article 12; provided that the Indemnified Party is not obligated to admit liability under any circumstances. The obligations of the Parties set out in this Article 12 shall survive the termination of this Contract for a period of four (4) years.

Article 13. LIABILITY

13.1Exclusion of Indirect Damages

None of the Parties shall be liable for any loss of profits, income, business or customers, or any indirect, incidental, consequential, punitive or special costs, damages or expenses of any kind arising from, or in any way related to, the Contract, or the breach thereof, irrespective of the legal theory on which any claim for such damage is based.

13.2 Limitation of Liability

The overall liability of:

(i) Orange towards the Partner shall not exceed the cumulative amount paid by the Partner to Orange or received by Orange from the Partner in the year preceding the date on which the claim or dispute occurred; and

(ii) The Partner towards Orange shall not exceed the cumulative amount paid by the Partner to Orange in the year preceding the date on which the claim or dispute occurred.

13.3Exceptions

13.3.1. Article 13.2 shall not apply to either Party:

a. concerning their confidentiality obligations (Article 15),
b. concerning their obligations relating to Brand Licenses (Article 10),
c. in the event of death or injury caused by negligence,
d. in the event of deliberate conduct and/or gross negligence,
e. in the case of liability for fraud caused by the actions or omissions of that Party,
f. in the case of liability that cannot be excluded by law,
g. under Article 8.

13.3.2. In the event of a breach of Article 8, and provided that the damage suffered by Orange has been caused directly and materially by the Partner, the sole responsibility of the Partner and the exclusive remedy of Orange for a breach of Article 8 shall not exceed the maximum amount of seven hundred and fifty thousand euros (€750,000) or 300% of the agreed amount paid by the Partner to Orange or received by Orange from the Partner in the year preceding the date on which the claim or dispute occurred (hereinafter referred to as the “Specific Ceiling”).

Under no circumstances shall the annual Specific Ceiling, for a consecutive period of 12 months from the date of entry into force, exceed the total amount of five million euros (€5,000,000).

The Partner agrees to reimburse Orange for the actual and reasonable costs incurred by Orange to respond to and mitigate the damage caused by any security breach caused by the Partner, including all notice costs ("Compensatory Indemnities"). The Partner's obligations with respect to the payment of Compensatory Indemnities, the settlement to which the Partner consents, or the legal fees and defense costs of Orange are subject to the Specific Ceiling.

Article 14. FORCE MAJEURE

A Party (the “Affected Party”) shall not be considered to be in violation of this Contract, nor shall it be liable for any breach or delay in the performance of the obligations stipulated therein, if and to the extent that such breach or delay results from a Case of Force Majeure, as defined in the paragraph below.

For the purposes of this Contract, a “Case of Force Majeure" is considered to be an event such as fire, water damage, natural disaster, storm, flood, earthquake or attack; war or armed conflict, military operation; civil war, riot or public disorder; an act of terrorism; an explosion; a general disruption of work such as a general strike; a blocking of means of transport or telecommunications; any legal or regulatory restriction imposed or any decision taken by a public authority not attributable to a Party, such as an embargo, or any other event or circumstance beyond the reasonable control of that Party which could not reasonably have been foreseen or prevented.

In a Case of Force Majeure, the Affected Party shall:

a. as soon as reasonably possible after the start of a Case of Force Majeure, notify the other Party in writing of the date of occurrence of the Case of Force Majeure and the effects on its ability to fulfill its obligations under this Contract;
b. do whatever is reasonably possible to continue to fulfill its obligations under the Contract, or to mitigate the impact of its non-execution notwithstanding the Case of Force Majeure; and
c. as soon as reasonably possible after the end of the Case of Force Majeure, notify the other Party in writing that the Case of Force Majeure is over and recommit to its obligations under this Contract.

If the Party's failure to comply fully with its obligations under this Contract following a Case of Force Majeure continues for more than sixty (60) days, the unaffected Party shall be entitled to terminate the Contract with immediate effect.

Article 15. CONFIDENTIALITY

15.1 In accordance with this Contract, the following information shall be considered “Confidential Information”: this Contract, the End User Data (including Personal Data), technical, commercial, strategic, financial and economic data, data related to research, to the technical specifications, to software, to components and to products of Orange and of the Partner, on any verbal, visual or written medium, and communicated to the other Party during the negotiations or execution of this Contract.

15.2 Unless otherwise specified in the Contract, a Party receiving ("Receiving Party") Confidential Information from the Other Party (the “Disclosing Party") must:

a. only use Confidential Information received from the Disclosing Party in the performance of the Contract; and
b. keep confidential and not use or disclose directly or indirectly to another party or entity, except to the extent provided herein, Confidential Information received from the Disclosing Party using the same degree of diligence (but while respecting commercial practices), which the Receiving Party would use to protect its own Confidential Information. The Receiving Party will only disclose Confidential Information to its representatives who need it and are bound by confidentiality obligations, and only to the extent necessary to fulfill their obligations under this Contract. The Receiving Party requires its representatives to comply with the provisions of this article to the same extent that it does. A party or person receiving Confidential Information will be responsible for any disclosure of this information by any representative to whom it discloses such information.

The Receiving Party must return or destroy all Confidential Information received from the Disclosing Party, including copies made by the Receiving Party, within thirty (30) days after receipt of a written request from the Disclosing Party to the Receiving Party, except for (a) Confidential Information which the Receiving Party reasonably needs to fulfill its obligations under the Contract and (b) a copy for archival purposes only.

To the extent that the Partner receives End User Data from Orange about the End User, the Partner must comply with the security requirements set out in Appendices C and D.

15.3 Unless otherwise agreed upon, the obligations of this Article shall not apply to information which:

a. was, at the time of receipt, already in the possession of or known to the Party, free from any obligation of confidentiality or restriction on use;
b. is or becomes publicly available or accessible by any lawful act of the Receiving Party or the directors, officers, staff members, agents or subcontractors of the Receiving Party;
c. is legitimately received from a third party having no direct or indirect obligation of confidentiality or restriction on use toward the Disclosing Party about such information;
d. is developed independently by the Receiving Party;
e. is approved for disclosure or use with the written permission of the Disclosing Party (including in this Contract); or
f. shall be disclosed by the Receiving Party under any applicable law, rules, regulations or public order, any decree or official publication, or any authority, provided that the Receiving Party has made commercially reasonable efforts to give sufficient notice to the Disclosing Party (where reasonably possible prior to disclosure) in order to enable it to seek protective solutions, and the Receiving Party shall also make reasonable efforts to ensure the confidentiality of the Confidential Information disclosed.

15.4 The Disclosing Party shall retain all rights, titles and interests to any Confidential Information that it discloses to the Receiving Party. Except as expressly provided in this Contract, no license shall be granted by this Contract concerning Confidential Information (including in the form of a patent, brand or copyright), it being also understood that no such license is implied solely by the disclosure of Confidential Information.

15.5 This confidentiality obligation will remain in force for the duration of the Contract and for a period of one (1) year following the expiration or termination of this Contract.

Article 16. GENERAL STIPULATIONS

16.1Specific stipulations

It is understood that the cooperation between the Parties shall under no circumstances be regarded as establishing either a partnership or a participating company between them or any other situation involving any reciprocal representation or solidarity to their respective creditors. Neither Party has the authority to conclude a contract on behalf of the other Party. Accordingly, the Parties have decided that their collaboration is only governed by the terms of the Contract.

16.2Intuitu personae/substitution

Since the Contract is concluded intuitu personae and, in particular, on the basis of the experience, expertise and knowledge of each Party, it may under no circumstances be subject to any partial or total assignment by either Party without the prior written consent of the other Party, which shall not be unduly refused, conditioned or delayed; however, either Party may assign this Contract, with prior notice, but without the consent of any entity which, directly or indirectly, controls or is controlled by a Party or exercises joint control over this latter. Each Party agrees to promptly respond to any request for a transfer authorization hereunder, and processes the request within two (2) weeks of receipt. Subject to the foregoing, this Contract shall be binding on all successors, assignees or receivers of the respective Parties hereto.

Neither the assignment of the Contract or a right by a Party under this Contract, including by assignment of guarantee, nor the granting of any guarantee by a Party in respect of the Contract or the rights of a Party under the Contract or resulting from the Contract, shall affect the rights of the other Party under applicable law, including the rights of compensation and recovery, as if such transfer or the granting of the guarantee had not taken place. No assignee or guaranteed party shall have any rights superior to those of a Party itself under this Contract, and any defense, compensation, recovery or claim of a Party against the other Party shall take precedence over the rights of an assignee or a guaranteed party of that Party irrespective of whether such defense, compensation, recovery or claim was made before or after a Party received notification of the assignment or security.

16.3Amendment(s) to the contract

If the Contract is amended by Orange, Orange undertakes to inform the Partner at least two (2) months prior to the entry into force of the amendments. On this occasion, should the Partner disagree, they may duly terminate the Contract with thirty (30) days' notice sent by registered letter with return receipt. Termination does not entitle the Partner to any compensation. If the Partner has not terminated by the date on which the amendments come into force, the Partner is deemed to have accepted the amendment.

16.4Absence of third-party beneficiary

Except as expressly provided herein, the Contract shall be concluded solely for the benefit of the Parties and, unless expressly stated otherwise, no other natural or legal person shall benefit directly or indirectly or have any interest in taking action or initiating any claim, direct or indirect, under this Contract.

16.5Partial non-validity

If one or more provisions of the Contract are held invalid or declared as such pursuant to a law or regulation, or following a final decision of a competent court, the other provisions shall retain their full force and scope, unless the invalid provision(s) are of a substantial nature and their disappearance jeopardizes the contractual balance. In any event, the Parties shall make every effort to substitute a valid stipulation in accordance with the spirit of the original text.

16.6Waiver

Any waiver, whatever its length, of the right to claim a total or partial breach of any of the terms of the Contract cannot constitute an amendment or deletion of said clause or a waiver of the right to claim previous, concomitant or subsequent breaches of the same or other clauses. Such a waiver shall only have effect if it is expressed in writing by the person duly authorized to that effect.

16.7Domicile

For the purposes of this Contract and its consequences, the Parties shall elect domicile in their respective registered offices.

16.8Titles

In the event of differences in interpretation between any titles and the terms of the clauses they represent, titles will be declared non-existent.

Article 17. DISPUTE SETTLEMENT PROCESS

If a dispute relating to this Contract arises between the Parties (the "Dispute"), the Parties shall follow the dispute settlement procedure provided in this Article:

a. Each Party shall notify the other Party in writing of the occurrence of the Dispute, setting out the nature of the facts and full details ("Notification of the Dispute"). Upon Notification of the Dispute by one Party to another, the Parties agree to organize first, within thirty (30) days from receipt of the Notification of the Dispute, two (2) meetings between the contacts, who will attempt in good faith to resolve the Dispute amicably;
b. If, for any reason, the contacts fail to resolve the Dispute within thirty (30) days from the date of receipt of the Notification of the Dispute, the Dispute shall be submitted to the authorized management executives of each Party for the purpose of resolving it amicably within sixty (60) days; and
c. If, for any reason, the two management executives fail to resolve the Dispute within the sixty (60) days referred to in paragraph (b) above, the Parties may bring legal proceedings pursuant to Article 18.2.

This dispute-settlement process shall not be construed as preventing either Party from terminating the Contract for any reason valid under any article permitting such termination.

Article 18. APPLICABLE LAW AND COMPETENT JURISDICTION

18.1 This Contract signed below shall be submitted and interpreted in accordance with French law.

18.2 In the event of a dispute arising in connection with the Contract, either in terms of its interpretation or its performance, and in the absence of an amicable agreement between the Parties, the Tribunal de Grande Instance de Paris [High Court of Paris], notwithstanding multiple defendants or the introduction of third parties, shall be granted express jurisdiction, even in the case of interim measures, summary proceedings or by request.

Article 19. NOTIFICATION

Any notification, request, order or other communication required or authorized pursuant to or in connection with this Contract shall be communicated in writing, in French, and duly signed by the Party which makes them, and shall be addressed to the other Party as follows: to the persons and addresses listed below, or to any other person and address of which the other Party may occasionally be notified in writing for these purposes, and shall be sent by registered letter with return receipt, or hand-delivered in exchange for a return receipt signed and dated by the recipient:

- For Orange

  With a copy to: pay.services@orange.com

- For the Partner: to the contacts listed on the Partner Form

Appendix A Mobile ID SERVICE DESCRIPTION

1. General stipulations on the protection of personal data for the Mobile Id service

The nature and scope of the Processing, the Personal Data categories, and their retention period by the Partner for the Mobile ID service are described in the table below:

Processing	Categories of personal data processed	Retention period
Form ID: Automatic population of online forms using Orange's Customer Data	- Orange unique technical identification number - Full name: First and last name; - Address: Street number, town or city, postal code, country; - Contact email address; - Contact telephone number - Date of birth, gender - Orange mobile telephone number - Date on which data was last updated	No retention by the Partner of personal data transmitted by Orange
Match ID: Verification of Personal Identification Data for End Users on Service Provider sites using Orange's Customer Database	- Orange unique technical identification number - Full name: First and last name - Address: Street number, town or city, postal code, country; - Contact email address; - Contact telephone number - Date of birth, gender - Orange mobile telephone number - Date on which data was last updated	No retention by the Partner of personal data transmitted by Orange
Sim Verify: Verification of how long the SIM card has been registered	Provision of activation date	No retention by the Partner of personal data transmitted by Orange
Sim Verify: Verification of how long the SIM card has been registered	YES/NO answer to a question about how long the SIM card has been registered	No retention by the Partner of personal data transmitted by Orange
Home Verify: Provision of a duplicate Orange bill as proof of address	Bill (first two pages only)	No retention by the Partner of personal data transmitted by Orange
Number Verify: Verification that the mobile phone number of the End User holding an Orange mobile subscription declared to the Service Provider is identical	YES/NO answer to the question is the declared MSISDN identical to the MSISDN used	No retention by the Partner of personal data transmitted by Orange

to the mobile phone number used		

1. Specific conditions of the Form ID Service

1.1. **Objective**: Increase customer registrations by removing barriers through the automatic population of customer account creation and activation fields with Service Providers.

1.2. **Method**: The End User will first be identified and authenticated. The End User Data will then be used to populate the pages on the Service Provider's website or application.

1.3. **End User Consent**: This Service requires prior and express authorization from the End User for Orange to share the aforesaid End User Data with the Partner.

a. The End User must be presented with an express consent option (See Appendix J: "Orange Customer Experiences").

b. The Consent Option will be presented to End Users within the End User interface.

c. No Personal Data shall be provided to the Partner until the following conditions are met:

d. the End User must have given prior consent in the Customer Experience;

e. the End User who intends to use the approved Service Provider service has been identified and validated as the Holder of the Orange account; and

f. Orange has the files containing the End User Data and will store the End User's express consent.

1.4. End User Data transmitted:

Subject to the Consent of the End User as part of the Consent Option and the choices made by the Partner in the Form for each Service Provider, Orange will provide the Partner with the following End User Data attributes:

- Orange unique technical identification number
- Full name: First and last name;
- Address: Street number, town or city, postal code, country;
- Contact email address;
- Contact telephone number
- Date of birth, gender
- Orange mobile telephone number
- Date on which data was last updated

1.5. **Use and Retention of End User Data**:

The Partner cannot retain End User Data obtained from Orange. However, Service Providers may retain End User Data obtained from the Partner under the terms agreed upon with the Service Providers concerned. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

1.6. **API calls**: See Appendix B: "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.

- If the End User is eligible for this use case, the Service Provider invites the End User to use the Automatic Form Population Service. If the End User agrees, the Consent Option will be displayed to them.
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.
- Optionally and at the Partner's request, Orange will provide the URL SMS (Orange SMS) functionality, which involves sending an SMS that contains a URL directing the End User to the Orange consent page. The sole purpose of this functionality is to transmit the URL for redirection to the Orange consent page.

2. Specific conditions of the Match ID Service in the general case

2.1. **Objective**: Reduce fraudulent identifications by the Service Provider of the data declared by an End User on the Service Provider's website using End User Data.

2.2. **Method**: The Partner will compare the End User data (such as name and address) transmitted by the Service Provider with the data from the Orange Account Holder kept by Orange, subject to availability. Once the data is compared, the Partner will return a matching result to the Service Provider. The Service Provider alone shall decide on the conclusions regarding the correspondence of the data for its business activity. End User Data will not be shared with the Service Provider, but only approved with a correspondence response transmitted by the Partner to the Service Provider.

2.3. **End User Consent**: This Service requires prior and express authorization from the End User for Orange to share the aforesaid End User Data with the Partner.

2.3.1. The End User must be presented with an express consent option (See Appendix J: "Orange Customer Experiences").

2.3.2. The Consent Option will be presented to End Users within the End User Interface.

2.3.3. No Personal Data shall be provided to the Partner until the following conditions are met:

- the End User must have given prior consent in the Customer Experience;
- the End User who intends to use the approved Service Provider service has been identified and validated as the Holder of the Orange account; and
- Orange has the files containing the End User Data and will store the End User's express consent.

2.4. **Returned data:** Using End User Data, the Partner shall return the attribute level result for the data:

- Orange unique technical identification number
- Full name: First and last name;
- Address: Street number, town or city, postal code, country;
- Contact email address;
- Contact telephone number
- Date of birth, gender
- Orange mobile telephone number
- Date on which data was last updated

2.5. Use and Retention of End User Data:

The Partner cannot retain End User Data obtained from Orange. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

2.6. **API calls**: See Appendix B "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.
- If the End User is eligible for this use case, the Service Provider invites the End User to use the Personal Identification Data Verification Service. If the End User agrees, the Consent Option will be displayed to them.
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.
- Optionally and at the Partner's request, Orange will provide the URL SMS (Orange SMS) functionality, which involves sending an SMS that contains a URL directing the End User to the Orange consent page. The sole purpose of this functionality is to transmit the URL for redirection to the Orange consent page.

3. Specific conditions of the Match ID Service in the particular case of legitimate interest

3.1. **Objective**: To reduce fraudulent identifications by the Service Provider and the risks of fraud related to the impersonation of data declared by an End User on the Service Provider's website or mobile application using End User Data.

3.2. **Method**: The Partner will compare the End User data (such as name and address) transmitted by the Service Provider with the data from the Orange Account Holder kept by Orange, subject to availability. Once the data is compared, the Partner will return a matching result to the Service Provider. The Service Provider alone shall decide on the conclusions regarding the correspondence of the data for its business activity. End User Data will not be shared with the Service Provider, but only approved with a correspondence response transmitted by the Partner to the Service Provider.

3.3. **Implementation conditions:** In the specific case where the Match ID Service is part of the legitimate interest demonstrated by the Service Provider and approved by Orange, this service will not involve the prior and express consent of the End User in the User's option. The justification for this processing must be documented to Orange by the Partner. If necessary, the Service Provider will inform the End User, by any means in accordance with the regulations, that this Personal Identification Data may need to be verified with Orange.

3.4. **Returned data:** Using End User Data, the Partner shall return the attribute level result for the data:

- Orange unique technical identification number
- Full name: First and last name;
- Address: Street number, town or city, postal code, country;
- Contact email address;
- Contact telephone number
- Date of birth, gender

- Orange mobile telephone number
- Date on which data was last updated

3.5. Use and Retention of End User Data:

The Partner cannot retain End User Data obtained from Orange. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

3.6. **API calls**: See Appendix B "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.
- If the End User is eligible for this use case, the Service Provider invites the End User to use the Personal Identification Data Verification Service.
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.

4. Specific conditions of the SIM VERIFY service

4.1. **Objective**: Reduce fraudulent identifications to the Service Provider by providing information about the on the recency of the End User's current SIM card.

4.2. **Method**: Two ways of providing of information relating to the recency of the SIM card are offered to the Service Provider: the transmission of the date of activation of the SIM card or a YES/NO answer to a question about the age of the SIM card.

4.3. **Implementation conditions:** This Service does not imply the prior and express consent of the End User in the User's option as this is only offered when the legitimate interest is demonstrated by the Service Provider and approved by Orange. The justification for this processing must be documented to Orange by the Partner. If necessary, the Service Provider will inform the End User, by any means in accordance with the regulations, that the number declared may need to be verified with Orange

4.4. **End User Data transmitted**:

Orange will provide the Partner with the following End User Data: the activation date of the SIM card in use or a YES/NO answer to a question about the age of the SIM card.

In addition to the definition of "Orange Account Holder" (Article 2 DEFINITIONS), the Sim Verify Service is also aimed at prepay customers or customers who have signed up for a mobile package for the VSE sector.

4.5. Use and Retention of End User Data:

The Partner cannot retain End User Data obtained from Orange. However, Service Providers may retain End User Data obtained from the Partner under the terms agreed upon with the Service Providers concerned. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

4.6. **API calls:** See Appendix B "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.
- If the End User's account is eligible for the use case, Orange will provide the Partner with the following End User Data: the activation date of the SIM card in use or a YES/NO answer to a question about the age of the SIM card.
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.

5. Specific conditions of the Home Verify service

5.1. **Objective**: Facilitate customer registrations by providing the operator bill pertaining to the End User's mobile or Internet subscription by way of proof of address.

5.2. **Method**: The End User will first be identified and authenticated. The End User Data will then be used as proof of address.

5.3. **End User Consent**: This Service requires prior and express authorization from the End User for Orange to share the aforesaid End User Data with the Partner.

5.3.1. The End User must be presented with an express consent option (See Appendix J: "Orange Customer Experiences").

5.3.2. The Consent Option will be presented to End Users within the End User interface.

5.3.3. No Personal Data shall be provided to the Partner until the following conditions are met:

- the End User must have given prior consent in the Consent Option;
- the End User who intends to use the approved Service Provider service has been identified and validated as the Holder of the Orange account; and
- Orange has the files containing the End User Data and will store the End User's express consent.

5.4. **End User Data transmitted**:

Subject to obtaining the End User's consent as part of the Consent Option and the choices made by the Partner on the Form for each Service Provider, Orange will provide the Partner with the following End User Data: the first two pages of the latest bill for the mobile or Internet subscription.

5.5. **Use and Retention of End User Data**:

The Partner cannot retain End User Data obtained from Orange. However, Service Providers may retain End User Data obtained from the Partner under the terms agreed upon with the Service Providers concerned. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

5.6. **API calls**: See Appendix B "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.
- If the End User is eligible for this use case, the Service Provider invites the End User to use the Home Verify Service. If the End User agrees, the Consent Option will be displayed to them.
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.

- Optionally and at the Partner's request, Orange will provide the URL SMS (Orange SMS) functionality, which involves sending an SMS that contains a URL directing the End User to the Orange consent page. The sole purpose of this functionality is to transmit the URL for redirection to the Orange consent page.

6. Specific conditions of the NUMBER VERIFY service

6.1. **Objective:** The purpose of the service is to provide Service Providers with real-time confirmation that the mobile phone number (MSISDN) that an End User claims to be using is the same as the mobile terminal that he/she is actually using at the time of the request. The service thus makes it possible to meet the needs of line authentication and verification of the veracity of the declared MSISDN.

6.2. **Method:** Upon request, the service provides a method of mobile line authentication by allowing validation of an End User's mobile number when using an online service on his/her mobile terminal connected to the 3G/4G/5G mobile network.

6.3. **Implementation conditions:** This Service does not imply the prior and express consent of the End User in the User's option as this is only offered when the legitimate interest is demonstrated by the Service Provider and approved by Orange. The justification for this processing must be documented to Orange by the Partner. If necessary, the Service Provider will inform the End User, by any means in accordance with the regulations, that the number declared may need to be verified with Orange

6.4. **End User Data transmitted**: Only a YES/NO answer will be provided to the question: "Is the declared MSISDN identical to the MSISDN used?" In addition to the definition of "Orange Account Holder" (Article 2 DEFINITIONS), the Number Verify Service is also aimed at prepay customers or customers who have signed up for a mobile package for the VSE sector.

6.5. Use and Retention of End User Data:

The Partner cannot retain End User Data obtained from Orange. However, Service Providers may retain End User Data obtained from the Partner under the terms agreed upon with the Service Providers concerned. In addition, the Partner may retain information relating to transfers (other than Personal Data) for record-keeping, financial reporting and audits for its own account.

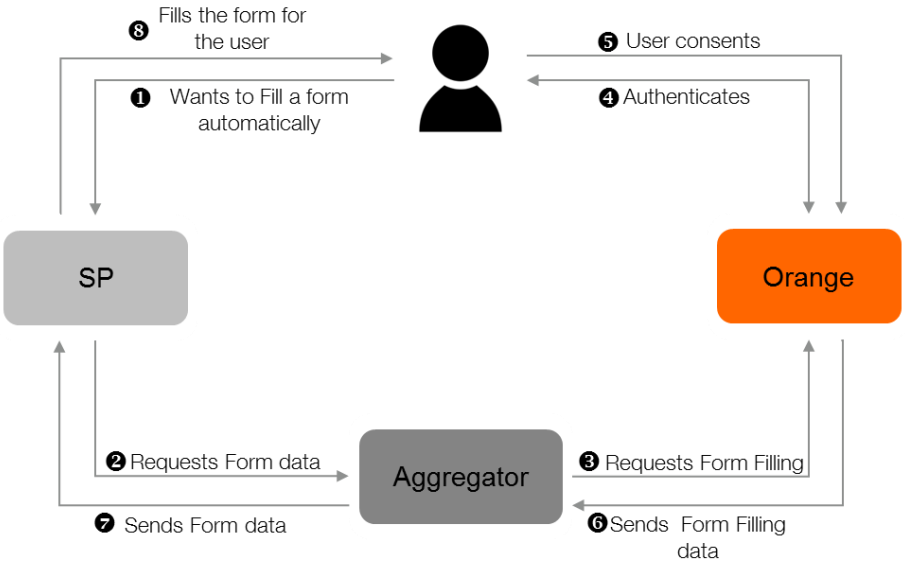
6.6. **API calls**: See Appendix B "Technical Conditions" for details on API.

- Verify the End User if the End User information is available to the Service Provider or if the End User account is eligible for the use case.
- If the End User's account is eligible for the use case, only a YES/NO answer will be provided to the question: "Is the declared MSISDN identical to the MSISDN used?"
- Optionally and at the Partner's request, Orange will activate the Eligibility API functionality.

Appendix B - TECHNICAL CONDITIONS

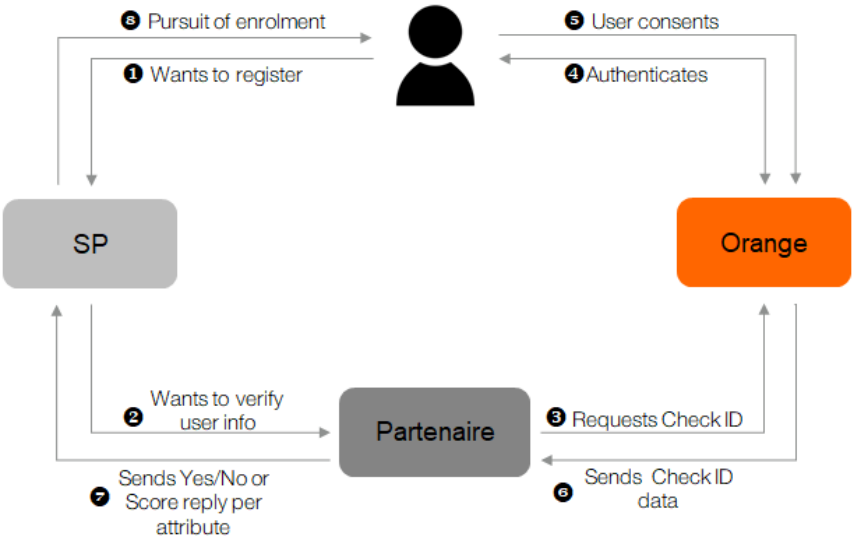
A- TECHNICAL FLOWS

1. Form ID Service

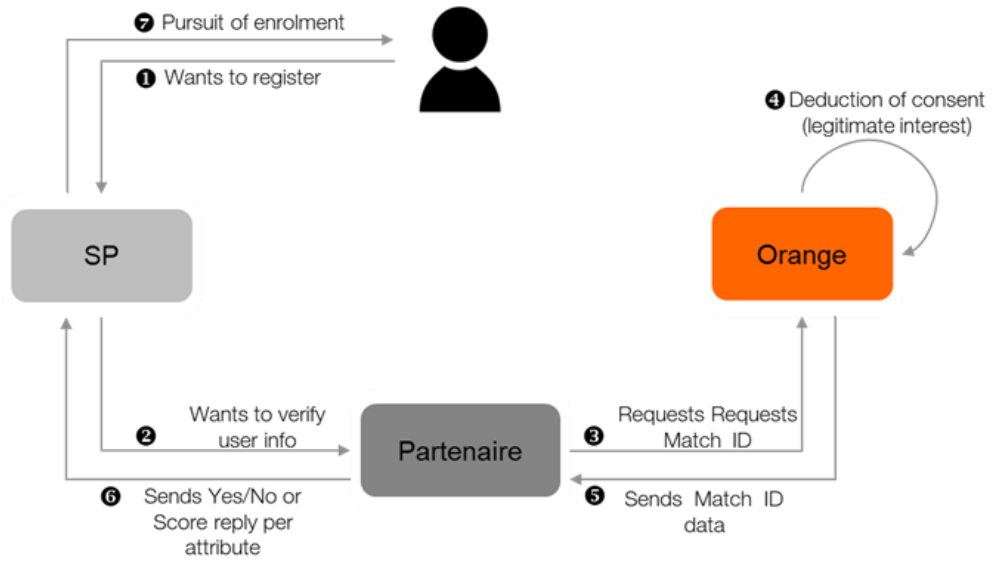


2. Match ID Service

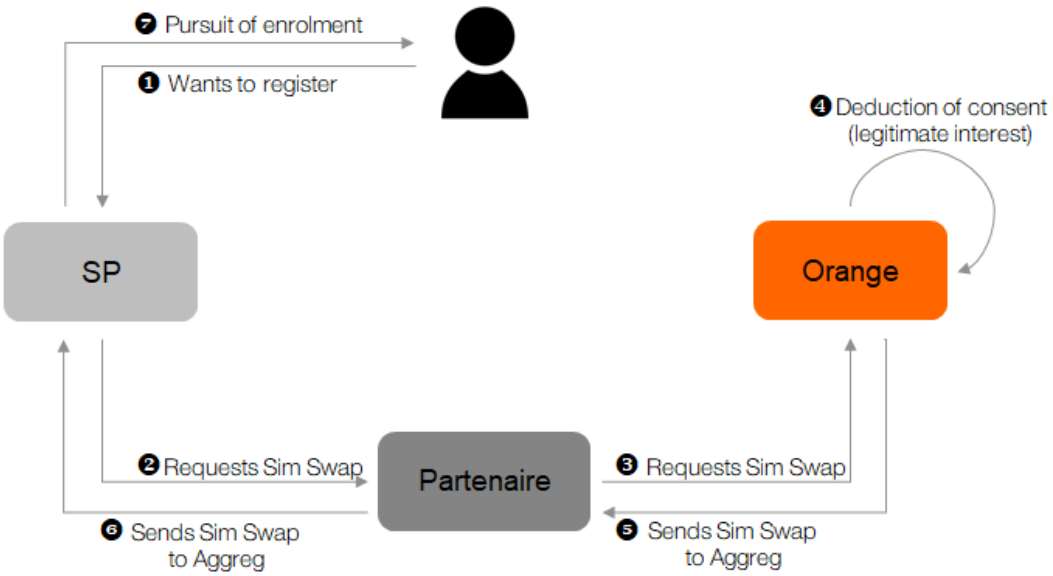
a) With express consent



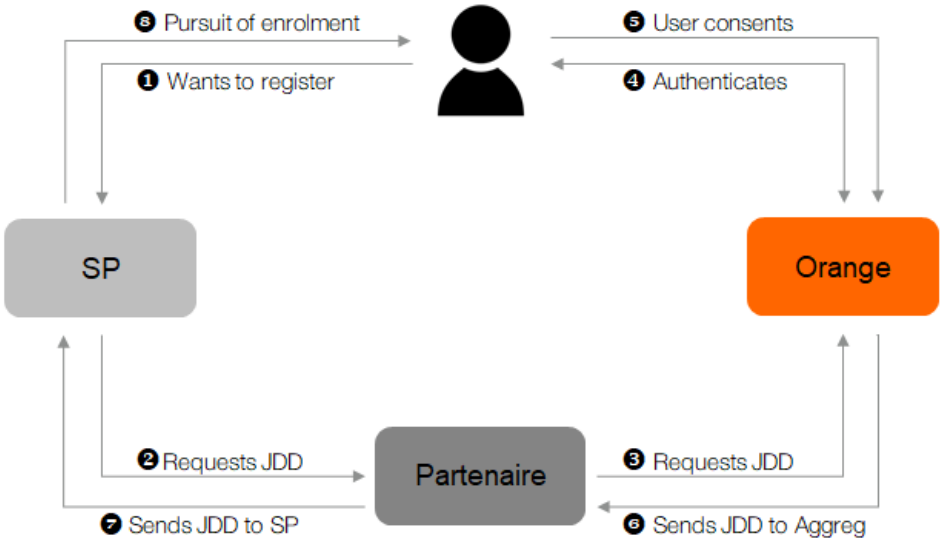
b) Without express consent – if a legitimate interest has been demonstrated



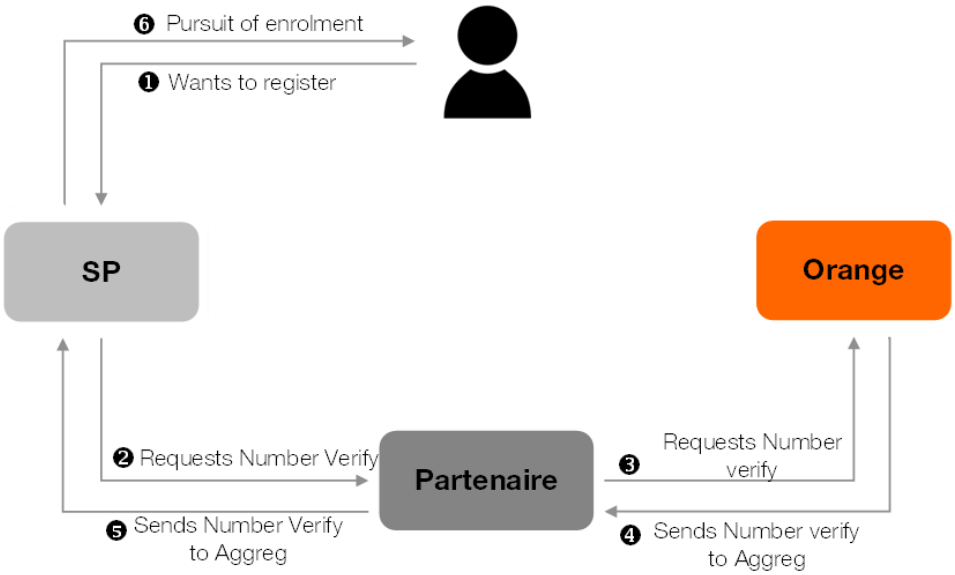
3. SIM Verify Service



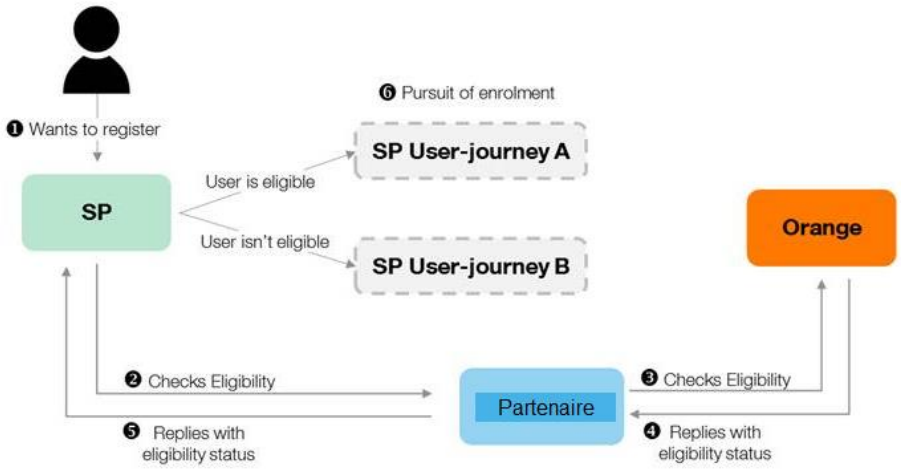
4. Home Verify Service



5. Number Verify Service



6. Eligibility API option



B- REQUIREMENTS FOR DATA FROM THE PARTNER

The fields below will be sent to Orange by the Partner under the Orange APIs as appropriate.

1. RequestId - registration of the transaction transmitted by the Service Provider to the Partner.
2. AgreggatorTransactionId - randomly generated number so that the Partner can track the transaction.
3. Service Provider name - to ascertain whom the identifiers were transferred to.
4. MSISDN - to confirm the subscriber who has been authenticated.
5. ConsentID - code for obtaining authorization from the User.
6. Date/Time - time stamp of the request (or response) transaction.
7. StatusCode - success/failure.
8. ReasonCode - if necessary, reason for the transaction's failure (non-existent, user auth. failure, etc.).

C. SERVICE QUALITY AND MAINTENANCE

Data recovery response time <1 sec. in 95% of cases.
Incident availability time: 95%
Disaster availability time: 96%

C: Standard	Level 2	Guaranteed operation 12x5	Availability
	Impact	RIO incident = 1 day	Incident 95% annual
	Sensitive	RTO damage = 5 days	Damage 96% annual
SLA Bronze		RPO damage = 1 day	
		No redundancy	

RTO recovery time objective
RTO is an objective. To meet it, many organizations define model solutions based on the recovery times expected.
RPO Recovery point objective
The RTO is considered in conjunction with the recovery point objective (RPO) which quantifies the recovery capacity upon saving the resource. The two aspects in combination make it possible to determine the total downtime of a resource following a major incident.

To contact the support channel, send an email to the following addresses:

orangeid.ext-support@orange.com

Appendix C – SECURITY REQUIREMENTS FOR THE PARTNER NETWORK

1. DEFINITIONS

The terms defined in this Section have the meanings below as they appear in Appendix C, unless the context in which they are used requires a different meaning or a different definition is indicated for a particular Section or provision.

1.1. **“Confidential Information”** means: Orange customer data and proprietary network information, data relating to systems, networks, Orange services and security checks implemented on these systems and networks, data relating to Orange staff, proprietary Orange and/or commercial secret information, and other confidential information or data or proprietary data in accordance with the terms of this Contract.

1.2. **"Industrial Standard”** means: accepted set of best practices (1) used or adopted by a substantial number of companies engaged in a similar type of business ("comparable companies") to manage similar types of information, (2) prescribed for use by a body or group of applicable industrial standards or (3) established by experts who are recognized in the field as acceptable and reasonable.

1.3. **"Penetration Test"** means: part of the Risk Assessment Process in which one or more qualified, experienced and trained individuals, known as "ethical pirates," engage in a coordinated and planned attack of computer systems and networks to uncover potential vulnerabilities and ensure that logical controls can resist deliberate attempts to circumvent them.

1.4. **"Program"** means: processes and procedures that are documented and implemented to achieve common objectives and monitor this achievement, which may be updated from time to time.

1.5. **"Risk Assessment Process” and “Risk Assessment"** mean: a process that is documented and implemented for identifying system security risks and determining the likelihood of occurrence and the resulting impact, and identifying additional protections or changes that would appropriately eliminate and/or mitigate this impact.

1.6. **"Risk Management Program"** means: a process that is documented and implemented to identify, control and mitigate risks that are inherent to the information system. It includes the process of assessing the qualitative and/or quantitative risks of the industrial standard, the cost-benefit analysis, and the selection, implementation, testing and evaluation of protections, including a determination of the steps necessary to meet the four objectives of Security Assurance.

1.7. **“Security Assurance”** means: evidence that the four security objectives (integrity, availability, confidentiality and compatibility) are adequately met by a specific information system. "Properly met” means (1) a feature that performs sufficiently, (2) sufficient protection against unintentional errors (users or software), and (3) sufficient resistance to intentional penetration or circumvention.

1.8. **"Threat Source"** means: (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) situation and method that may inadvertently cause a vulnerability.

1.9. **"Threat Analysis"** means: review and documentation of sources of threat against system vulnerabilities to identify potential threats to a specific information system in a particular operational environment.

1.10. **"Vulnerability"** means: a defect or weakness in functionality, design, implementation, internal controls of the information system or security procedures that can be applied (triggered accidentally or intentionally) and cause a security vulnerability or breach of the system's security policy.

2. GENERAL REQUIREMENTS

2.1. This document, "Security Requirements" ("Document"), applies to the Partner's performance when personally identifiable information relating to Orange end users is provided to the Partner, including, but not limited to, the development, offer, use and/or maintenance of any service, software or other product thereunder, and all editions, versions, updates, improvements and related changes ("software" or "hardware" as applicable).

2.2. The Partner shall implement and maintain administrative, physical and technical security checks of the industrial standard that are sufficient in their nature and scope to protect (1) the confidentiality, integrity and availability of personally identifiable information as well as (2) the availability and integrity of the Orange service, network and operations.

2.3. The Partner shall complete the administrative, physical and technical security checks described in this document.

3. USE OF INFORMATION

3.1. The Partner guarantees that personal data will only be used to combat fraud, identify a mobile phone, complete a form and provide access to data for its customers or other needs specified in this Contract.

3.2. The Partner will take appropriate measures to secure personal data during transit and storage by means of protective mechanisms in accordance with industrial standards (such as encryption). This protection will include all forms of portable media (such as flash drive/USB, laptop, CD, DVD, Blu-ray, portable hard drive, cellular phone/smartphone, MP3 player, etc.).

4. INFORMATION SECURITY POLICIES AND PROGRAM

The Partner shall implement and maintain a Risk Management Program in accordance with the following industry standards including, but not limited to:

4.1. The Partner shall have a security policy describing the security and confidentiality controls implemented in its operations to satisfy this Document ("Information Security Policy"). The Partner shall establish a Risk Management Program to implement its Information Security Policy including, but not limited to:

4.1.1. A risk assessment process that ensures that the partner's operating environments, development environment, systems, applications, networks and procedures are regularly assessed to identify and address security vulnerabilities.

4.1.2. A program for detecting intrusions and security breaches, and preventing and responding to incidents.

4.1.3. A program to manage the system, network and application configuration.

4.1.4. A program for implementing and administering logical access control(s) to the data, systems and network.

4.1.5. A program for implementing and administering physical access control(s) to the premises and data.

4.2. The Partner shall have the Risk Management Program monitored by an internal or external auditor at least once a year to assess compliance with the requirements inherent in its Information Security Policy.

5. DEVELOPMENT CYCLE

5.1. The Partner's controls associated with the development, pre-production testing and delivery of any software or equipment, whatever it may be, will include, but not be limited to, an obligation to:

5.1.1. Implement security controls of the industrial standard for its operating environment, systems, networks and all premises in which the software is developed and/or hosted.

5.1.2. Develop, implement and comply with the best security coding practices of the industrial standard.

5.1.3. Establish processes with, where appropriate, the use of source code scanners, performance testing tools for operating system security, web application scanners or other tools or techniques, or even information acquired through industry standardization bodies to assess vulnerabilities in software or hardware security before starting production.

5.1.4. Follow industrial standard practices to mitigate and protect against all known and reasonably foreseeable security vulnerabilities, including: (1) unauthorized access, (2) unauthorized changes in systemic configurations or data, (3) interruption, degradation, or denial of service, (4) unauthorized escalation to a user privilege, (5) service theft, and (6) unauthorized disclosure of confidential information.

5.2. The Partner must ensure that all entities and configurations remain operational following any updates, modification or upgrades to software and hardware, unless Orange has given its prior written authorization.

6. SECURITY ASSURANCE

The Partner shall maintain a Risk Assessment Process showing the Partner's Software and Hardware Security Assurance. This process shall include:

6.1. The Partner's obligation to organize and conduct a Risk Assessment of its software and hardware through a third-party security test provider. The Partner shall repeat the Risk Assessment at the beginning of (1) each major release launch or (2) for any software or equipment deployed in the Orange Network or hosted by the Partner. This Risk Assessment shall include:

6.1.1. analysis of threats to software or hardware,

6.1.2. software or hardware penetration test,

6.1.3. risk assessment for administrative, technical, logical and physical security controls in the operating environment, systems, networks and premises where the software or equipment is hosted, if they are hosted by the Partner.

6.2. The Partner must address all high- or medium-risk vulnerabilities identified in the Risk Assessment before starting production.

6.3. Orange may request an electronic copy of the field of work from the third party above tasked with testing the security assurance (Section 6.1).

7. SECURITY BREACH AND INCIDENT RESPONSE

7.1. The Partner shall establish and maintain documented escalation processes for all security breaches and responses to incidents, with procedures for notifying Orange within twenty-four (24) hours after a breach involving personally-identifiable information communicated by Orange.

7.2. The Partner shall cooperate and provide information if requested by Orange or any consultant, contractor, lawyer or other third party authorized by Orange to investigate a security breach in the Partner's operating environment.

7.3. In the event of a security breach affecting Orange, the Partner must send Orange, within forty-eight (48) hours after its discovery, a post mortem report with (1) identification of all the potentially compromised Orange information, (2) actions by the Partner to mitigate the damage caused, and (3) protection to prevent the recurrence of said breach.

8. RIGHT TO RISK ASSESSMENT

8.1. Orange reserves the right to perform a Risk Assessment on the Partner's software and hardware. The risk assessment may, at the discretion of Orange, take place once a year or after each software and/or hardware launch and include, but is not limited to, vulnerability assessments and penetration tests of: (1) software and hardware, (2) underlying infrastructure and operating environment in which software and/or equipment operate or are hosted, (3) network and premises inherent in the operation or maintenance of software and/or hardware and (4) administrative, technical and/or physical controls of the Partner inherent in such software and/or hardware. For Risk Assessments requiring the Partner’s involvement, resources, premises or systems, the Parties shall come to an agreement (1) on the extent of its involvement, (2) the resources, premises, or systems that would be required, and (3) the Risk Assessment schedule.

8.2. The right granted to Orange to carry out its own Risk Assessment shall not replace or be a substitute for, under any circumstances, the Partner's Risk Assessment Process specified in this Document. A third-party security provider may, at the discretion of Orange, be used to carry out this Risk Assessment.

9. VULNERABILITY MANAGEMENT

The Partner shall implement and maintain an Industrial Standard Vulnerability Management Program. The Partner shall assign one or more staff members to the monitoring of appropriate public channels for the disclosure of the vulnerability (such as the NIST, National Vulnerability Database) that affect its software or hardware. This program will include (1) the underlying platform (e.g. operating system, database product, web server, etc.) and (2) all third-party software or (3) freeware that is part of the Partner's software or hardware. This program shall include:

9.1. Assignment by the Partner of one or more staff member(s) to liaise with the Orange Vulnerability Management staff.

9.2. The Partner shall address the vulnerabilities identified in its hardware and software at its own expense.

9.3. With respect to the Partner's software and hardware included in the Orange network and managed by Orange, the Partner will be required to provide a patch with a regression test within fifteen (15) days from the date on which the vulnerability was initially disclosed or to which the Partner was notified by Orange.

9.4. With respect to the Partner's software and hardware hosted in the Orange network and managed by Orange, the Partner will be required to implement in production a patch with a regression test within fifteen (15) days from the date on which the vulnerability was initially disclosed or on which the Partner was notified by Orange.

9.5. With respect to the Partner's software and hardware hosted outside of the Orange network, the Partner will be required to implement in production a patch with a regression test within fifteen (15) days from the date on which the vulnerability was initially disclosed or on which the Partner was notified by Orange.

Appendix D - ORANGE SECURITY REQUIREMENTS

Orange allows the Partner to access its APIs remotely for the sole fulfillment of its Partner Services commitments.

This access to the Orange programming interface will be authorized under the following terms and conditions.

1. Definitions

The terms defined in this Section have the meanings below as they appear in Appendix D, unless the context in which they are used requires a different meaning or a different definition is indicated for a particular Section or provision.

"Services" means all services ordered and provided by the Partner, for which access to the Orange Network is required.

"Orange Network" means the internal network managed by Orange and all the Orange network access infrastructures that are necessary to ensure communication between the resources of each party.

"Access Point" means the technical network interface between Orange and the Partner. This Access Point consists of different types of equipment managed by Orange and made available to the Partner. This Access Point will be used to create a dedicated network between several partner sites. This Access Point will always be used for all network connections and communications between the Partner and Orange.

"Contributors" means everyone formally authorized by the Partner to access the Orange Network remotely to perform only the Services. The Contributors may be the Partner's staff members, agents or subcontractors.

"Resources" means the programming interfaces, networks, hardware, software, and/or data belonging to and/or managed under the responsibility of each Party to provide the Products stipulated or perform the Services.

2. Access Control

The Partner shall:

a. only use the Access Point to perform the Services, and

b. ensure that only the Partner's Contributors and only the resources of the duly authorized Partner are interconnected and in communication with Orange's resources.

c. implement and manage the organizational and technical processes necessary to accurately identify a person using this remote access and its use or action associated with Orange resources.

With regard to the connection provided by Orange to the Contributors to access Orange's resources, the Partner shall

a. not divulge to any third party, other than the authorized contributing members, any authentication of the data giving access to Orange's resources, and

b. implement and manage all organizational and technical processes to identify and authenticate a person using this connection.

3. Resource Management and Use

The Partner shall:

a. update, as soon as possible and as much as necessary, its IT security tools to maintain the level of security required for its resources, such as updated and effective anti-virus software,

b. implement logoff mechanisms after a short period of inactivity to protect access to its resources,

c. implement and organize a password management policy and connections to its own resources, so that passwords are changed regularly and are hard to guess,

d. implement all the means necessary to ensure the integrity of the data exchanged between Orange and the Partner,

e. implement all necessary means to ensure that the data transmitted to Orange by the Partner are not infected with malicious codes, and

f. return to Orange all its equipment, or return to Orange or destroy all the data that are its property after the Services are completed.

The Partner will only use the Orange Resources they need to deliver the Services.

The Partner will only use their resources if they are needed to deliver the Services.

Access by physical interconnection (Pase Interco, for example)

In the event that Orange allows the Partner to access its network via a Pase Interco type infrastructure to execute the Contract, the Partner shall:

a. ensure that premises hosting the Orange equipment which constitutes this Access Point are subject to physical control and are only accessible by authorized Contributors,

b. ensure that remote access or control is not possible on its own interconnected equipment,

c. comply with the addressing rules imposed by Orange.

The Partner recognizes and accepts that routers and accesses are provided and administered by Orange.

4. Security Incident Management

The Partner shall designate a point of contact who will be notified in the event of a security incident and promptly notify Orange of any changes affecting this point of contact.

The Partner or Orange will notify the other Party if it detects a malicious action, system failure, or security incident that may affect the resources of the other Party using the procedures and contacts previously determined by the Parties.

In case of a serious incident related to the Partner's connection (such a virus or intrusion into the system) likely to affect or threaten the security of Orange resources, Orange may suspend remote access to the Orange Network without notice until the security incident is fully resolved.

5. Right of Audit and Logging

Orange reserves the right to:

a. log the Partner's accesses to Orange's resources,

b. implement management and monitoring tools on access infrastructure, and/or,

c. if needed, ask the Partner for the identity of the user accessing the Orange Network and, where applicable, its subcontractors.

In addition, Orange or any third party authorized by the Partner will be responsible for auditing the Partner's resources to verify that it complies with the commitments stipulated.

The Partner shall assist in the proper conduct of the audit. It will therefore have to agree to provide all the information necessary for this audit. This information will be covered by a non-disclosure agreement. The Partner and Orange will agree on the preparation and drafting of the audit requirements.

In the event that Orange allows the Partner to access its network via a Pase Interco infrastructure to execute the Contract or prepare the audit requirements, the Partner will provide, in writing, to Orange or any authorized third party in charge of the audit:

a. its policy for combating and avoiding malicious codes (such as names of anti-virus products used on workstations and servers, strategies to update signatures and anti-virus engines, and applications or tools on workstations and servers),

b. a diagram of the Partner's networks and of the equipment connected to the Orange network, and

c. any other information necessary for this audit (security policy item, daily log files, etc.).

If any non-compliance is revealed by the audit, the Partner shall establish a compliance program within ten (10) days after notifying Orange. The program shall contain all the measures to be implemented and their implementation dates within a reasonable timeframe. Once authorized by Orange, this compliance program shall be applied by the Partner. Otherwise, Orange may suspend remote access to the Orange network without notice and terminate the Contract as stipulated in Article 6 "Contract Duration and Termination" of said Contract.

6. Subcontracting

The Partner shall give Orange prior written notice of any changes inherent to the subcontracting parties involved during execution of the Services.

The Partner shall ensure that its Contributors - including subcontractors - comply with the terms and conditions of this section, in particular with regard to the strict confidentiality or integrity of all information to which they should

have access to deliver the Services. Orange may, depending on the type of information disclosed, ask the Partner to sign a non-disclosure agreement.

7. Information

The Partner shall notify Orange and specify in writing any modification of the items it must provide to Orange in accordance with the provisions of this Section, such as name of security contact or security rules.

Appendix E – BRANDS

“ORANGE” brand

Partner brand

[to be completed as appropriate: Partner's brand name and logo]

Appendix F Tariff Conditions

The Parties agree to apply the following tariff conditions:

- **Fixed Costs (excluding value-added tax)**

Commissioning	€2500
Monthly Fees	€500

- **Costs of the completed request (excluding value-added tax)**

From the date of entry into force	
Form ID	€0.25 per request
Match ID	€0.17 per request
Sim Verify	€0.022 per request
Home Verify	€0.35 per request
Number Verify	€0.025 per request
Match ID + Home Verify	€0.40 per request
Match ID + Sim Verify	€0.18 per request

In all cases, the API Eligibility option is included in the price of the Mobile ID service.

Appendix G - Form Identifying Service Providers

Desired implementation date:	

	Identity of the Service Provider ***Must be completed by the Service Provider***
Company Name	Name: Legal Form: SIREN No.: SIRET No.: Intra-Community VAT No.: APE Code: RCS (Trade and Corporate Register) No. and City: Nature of the Activity: VAT Liability:
Legal Representative	Type: Last Name: First Name: Title: Phone No.: E-mail:
Registered Offices	No.: Street: Zip Code: City: Country:
URL of the website(s) concerned:	

Commercial Contact:		
Last Name:	First Name:	Title:
Phone No.:		E-mail:
Address:		
Zip Code:	City:	
Technical Contact:		
Last Name:	First Name:	Title:
Phone No.: Address:		E-mail:
Zip Code:	City:	

Selection of the Mobile ID services to be activated for the Service Provider:

Form ID Service **with or without Eligibility API**	☐ **YES** ☐ **WITH**	☐ **NO** ☐ **WITHOUT**
Match ID Service **with or without consent** **with or without Eligibility API**	☐ **YES** ☐ **WITH** ☐ **WITH**	☐ **NO** ☐ **WITHOUT** ☐ **WITHOUT**
SIM Verify Service **with or without Eligibility API**	☐ **YES** ☐ **WITH**	☐ **NO** ☐ **WITHOUT**
Number Verify Service **with or without Eligibility API**	☐ **YES** ☐ **WITH**	☐ **NO** ☐ **WITHOUT**
Home Verify Service **with or without Eligibility API**	☐ **YES** ☐ **WITH**	☐ **NO** ☐ **WITHOUT**

In the event that one or more services are to be activated without consent (Match ID Service, SIM Verify Service or Number Verify Service), explain below the legitimate interest of the Service Provider to carry out the processing:

Select the authentication method to enable for the Service Provider:

Form ID	**Type of Customer Experience**	**YES**	**NO**
Mobile Customers	**3G/4G/5G Experience**		
	SMS URL Experience (Orange SMS)		
	Consent OTP SMS Experience		
Internet Customers	**Access with explicit authentication**		

Match ID **General case**	**Type of Customer Experience**	**YES**	**NO**
Mobile Customers	**3G/4G/5G Experience**		
	SMS URL Experience (Orange SMS)		
	Consent OTP SMS Experience		
Internet Customers	**Access with explicit authentication**		

Match ID Particular case of legitimate interest	Type of Customer Experience	YES	NO
Mobile Customers	3G/4G/5G Experience		
Internet Customers	Access with explicit authentication		

Home Verify	Type of Customer Experience	YES	NO
Mobile Customers	3G/4G/5G Experience		
	SMS URL Experience (Orange SMS)		
	Consent OTP SMS Experience		
Internet Customers	Access with explicit authentication		

3	Notes

The Partner has entered into a contract with the Service Provider organizing the technical and legal conditions under which the latter may become a Recipient of Orange data. This contract includes the implementation conditions provided for in the Contract made between Orange and the Partner.

The Service Provider's customer experience(s) must be appended to this Form, bearing in mind that the Orange pages (identification / sign in / consent validation) cannot be modified.

As a reminder, the Partner will not use the End-Users' data for its own purposes but will make them available to the Service Provider. The Service Provider then uses this data for its own business purposes. It is responsible for processing the data transmitted and is obliged to fulfil all the obligations incumbent on it in this respect, particularly with regard to the persons concerned,

The Partner shall create a dedicated Application per Service Provider.

Given in two (2) copies on _____

Partner's Representative	Orange Representative
Date	Date
Last Name:	Last Name:
First Name:	First Name:
Title:	Title:
Signature:	Signature:
Stamp	Stamp

Appendix H Partner Form

Company Name	
Legal Category	
Capital	
SIREN No.	
SIRET No.	
Intra-Community VAT No.	
EPA Code	
Trade & Corp. Reg. City	
Trade & Corp. Reg. No.	
Main Activity	
VAT Regime	
VAT Liability	
Date published in the Official Journal[1]	
Legal Representative	
Title	
First Name	
Last Name	
Occupation/Position	
Phone No.	
Email	
Registered Office Address	
Address 1	
Address 2	
Zip Code	
City	
Country	

Domicile under the Contract	
Domicile[2]	
If Other, please specify:	
Address 1	
Address 2	
Zip Code	
City	
Country	
Commercial Contact	
Company Name	
Title	
First Name	
Last Name	
Position	
Phone No.	

Billing Contact

Title	
First Name	
Last Name	
Position	
Phone No.	
Email	
Billing Address	*If different from the registered offices' address*
Address 1	
Address 2	
Zip Code	
City	
Country	

[1] *to be completed for companies in mm/dd/yyyy format*

[2] *if the registered offices are not in the European Union, please indicate a domicile address in the European Union.*

Signing this appendix implies unreserved acceptance of the general conditions of operation of the Mobile ID Service by Orange under the conditions set out in the Contract.

Signed on _____

Partner's Representative

Date
Last Name:
First Name:
Title:

Signature:

Stamp

Appendix I Security Questionnaires

As a reminder, the Partner must complete the following security questionnaires to access the APIs so that they can use the Mobile ID Service:

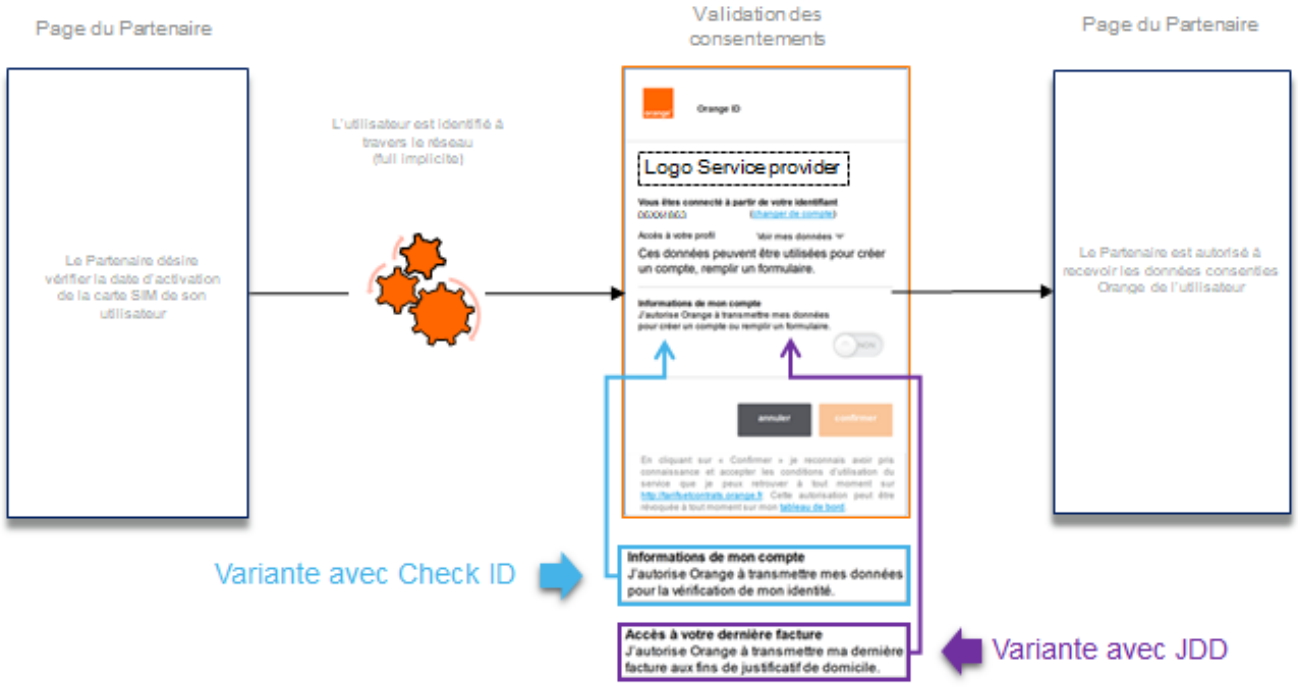
- combined security questionnaire for the Form ID Service and the Match ID Service
- security questionnaire for the SIM Verify Service with consent
- security questionnaire for the SIM Verify Service without consent
- security questionnaire for the Home Verify Service
- security Questionnaire for Number Verify Service

The above questionnaire(s) will be sent to the Partner at the same time as this Contract and must be validated by Orange before any connection to the APIs for the Mobile ID Service.

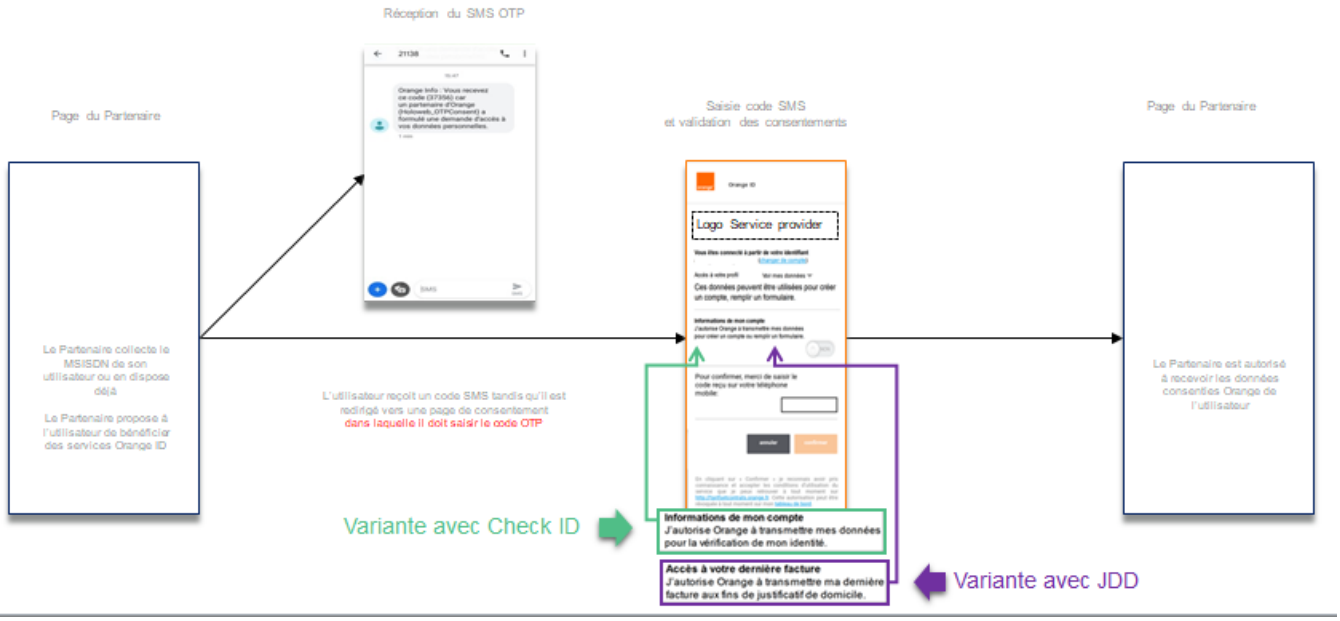
Appendix J Orange Customer Experiences

As a reminder, the Service Provider's customer experience(s) must be appended to the Contract, bearing in mind that the Orange pages (identification / sign in / consent validation) cannot be modified. They are necessary to ensure the collection of the consent of the Person Concerned when consent is the legal basis for making the Service Provider a recipient of the data.

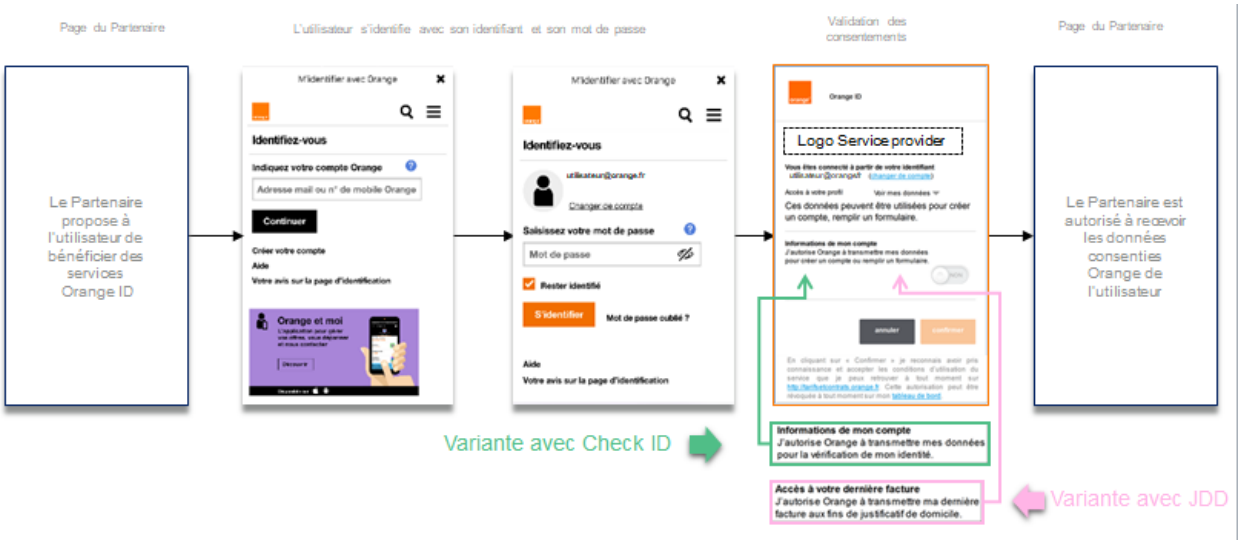
3G/4G Customer Experience (available for Form ID, Match ID, Home Verify)



SMS Customer Experience OTP Consent (available for Form ID, Match ID, Home Verify)



Internet Customer Experience (available for Form ID, Match ID, Home Verify)



URL SMS (Orange SMS) Customer Experience available for Form ID, Match ID, Home Verify