HighCONNEXION

AGREEMENT ON THE PROTECTION OF PERSONAL DATA
Applicable from 01/06/2021

WHEREAS

This Agreement on the processing of personal data and its annexes (hereinafter the "Agreement") supplements the stipulations of the General Terms and Conditions of Sale and the quotation (together the "Contract") applicable between High Connexion and the Customer (as mentioned on the order of participation, acting in its name and on its behalf or through an agent in the name and on behalf of the Customer) with regard to the processing of personal data performed in execution of the Contract. In this context, the Parties agree that this "Personal Data Processing Contract" (hereinafter the "Agreement") determines the conditions under which the Parties may process personal data.

NOW, THEREFORE, IT IS AGREED AS FOLLOWS

1. DEFINITIONS

For the purposes hereof and notwithstanding any other definitions provided in the Agreement, the following terms shall have the meanings given below:

Agreement	Refers to this Data Protection Agreement supplemented by the Annexes on the methods of processing personal data.
Activities	Refers to the marketing and payment activities performed by HIGH CONNEXION, as defined in the GTCS.
Regulatory Authority	Refers to any competent authority for the protection of Personal Data.
Contract	Refers to the entire contract according to which the Customer commissions HIGH CONNEXION to perform the services. In the absence of a specific service contract, the GTCS and the order of participation of High Connexion shall apply.
Authorised Recipient	Refers to an administrator, employee or Data Processor of one of the Parties who has a legitimate need to access Personal Data in the context of executing the Agreement.
Data	Refers to all types of information and/or data to which the Parties have access in the context of contractual relations, regardless of the format or medium, whether Personal Data or not (e.g. financial data, customer data, strategic, technical, professional, administrative, commercial, legal, accounting data, etc.).
Personal Data	Refers to any information relating to a natural person identified or identifiable as such, either directly or indirectly by grouping together information, by reference to an identification number or to elements specific to that person: name, address, telephone number, IP address, email address, vehicle registration number, professional registration number, username/login, password, connection data, etc.
Authorised Purpose	Refers to the purpose of Personal Data Processing implemented by the data processor, in accordance with the Annexes.
Instructions	Refers to all instructions written by the Data Controller for the Data Processor. These instructions shall follow a strict form and can only be considered as such insofar as they are formulated in writing in the Agreement, in an email or paper letter from a duly authorised person. The instructions shall be accompanied by any documentation necessary for their proper execution and shall be set out in the Annexes. These annexes must be supplemented by the Customer by any written means.
Third Country	Refers to any State that is not a member of the European Union. This terminology also covers any international organisation, including countries that are not members of the European Union.
Data Subject	Refers to any natural person whose Personal Data is the subject of Processing.
Security Measures	Refers to the Parties' physical, technical and organisational measures, regularly updated.
Data Protection Regulations	Refers to the regulations in force applicable to Personal Data Processing and, in particular: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable since 25 May 2018 known as the "General Data Protection Regulation" (hereinafter "GDPR"); (ii) French Law "IT and Liberties" No 78-17 of 6 January 1978 as amended; (iii) any legislation entering into force and likely to affect the Processing covered by the Agreement; (iv) any guide to good practice published by the competent Regulatory Authorities or the European Data Protection Board.
Data Controller	Refers, depending on the Processing, to the Customer or High Connexion as a legal entity determining alone or jointly the means and purposes of Processing implemented in the context of executing the Contract.
Services	Refers to the services provided by High Connexion under the Contract.
Data Processor	Refers, depending on the Processing, to High Connexion or the Customer as a legal entity performing Personal Data Processing operations on behalf of and according to the other Party. Data processor(s) who perform(s) Personal Data Processing strictly following the Instructions issued by the Data Controller is (are) qualified as "Data Sub-Processor(s)".
Processing	Refers to any operation or set of operations performed or not using automated processes and applied to Personal Data or sets of Personal Data, such as the collection, recording, organisation, structuring, retention, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, linking or interconnection, limitation, erasure or destruction.
Personal Data Breach	Refers to a security breach that accidentally or unlawfully results in access to or destruction, loss, alteration, or unauthorised disclosure of Personal Data transmitted, stored or processed.

2. CONTRACTUAL DURATION AND HIERARCHY

The Agreement enters into force upon acceptance of the quotation for the duration necessary for the Processing agreed between the Parties. The stipulations of the Agreement that by their nature are intended to continue beyond the term of the Contract remain applicable and retain their full effect. In the event of any contradiction between the provisions relating to Personal Data in the Contract and those of the Agreement, the Parties expressly agree that the Agreement shall prevail over the Contract. In the event of any contradiction between the contractual terms of the Agreement and the terms of the Annexes, the terms of the Annexes shall prevail.

3. COMPLIANCE WITH DATA PROTECTION REGULATIONS

Each Party undertakes to comply with the Data Protection Regulations.

4. PERSONAL DATA PROCESSING BY HIGH CONNEXION AS DATA CONTROLLER

4.1 Access and use of High Connexion platforms

4.1.1 Description of processing

High Connexion acts as Data Controller when it collects, stores, modifies, uses or deletes the Personal Data of Users, Administrators and any person acting in the name and on behalf of the Customer on the platforms set up by High Connexion (MGS, High Push, EP Gateway, Wallet, billing platform, etc.) for the purposes of the Services and on the basis of the execution of the Contract. In particular, it creates

and manages the accounts and properly monitors the management of the Customer's various actions via these platforms. In accordance with the privacy and cookie policy on High Connexion's platforms, Data Subjects may exercise their rights of access, rectification, erasure, objection, portability and restriction of personal data concerning them subject to Processing at High Connexion by sending an email to delegue-protection-donnees@highco.com. Details of this Processing are provided in **Annex I.**

4.1.2 Obligations of the Customer

The Customer is responsible for managing the access rights of users of High Connexion's platforms and must immediately notify High Connexion if Users and Administrators leave or change so that High Connexion can close and/or modify their accounts. Failing this, any action by a person representing the Customer who is not or no longer authorised cannot result in any liability for High Connexion.

4.2 Management of the Contract and the commercial relationship

As part of the administrative and contractual management of the commercial relationship with the Customer, High Connexion processes Personal Data identifying the Customer's representatives, employees and/or agents. The Personal Data collected concerns professional contact details, including in particular surname, first name, email address and telephone number. This Personal Data is mandatory to enter into the Contract. Details of this Processing are provided in **Annex I.**

5. PERSONAL DATA PROCESSING BY HIGH CONNEXION AS DATA PROCESSOR

5.1 Appointment and role of High Connexion

The Customer, in its capacity as Data Controller, designates High Connexion as a Data Processor to collect and process Personal Data in its name and on its behalf in order to achieve the Authorised Purposes set out in Annex II to the Agreement in the context of performing the Services. In accordance with the applicable regulations, High Connexion has appointed a data protection officer who can be contacted by email at delegue-protection-donnees@highco.com or by paper mail at the following address: HighCo – Service DPO, 365 avenue Archimède - 13799 Aix-en-Provence cedex 3, France. The Customer shall send High Connexion the name and contact details of its data protection officer by any written means, if it has appointed one in accordance with Article 37 of the GDPR.

5.2 General obligations of High Connexion as data processor

5.2.1 Orders and compliance

High Connexion guarantees the Customer that it shall:

- process only the Personal Data necessary for the Authorised Purposes, in accordance with the Instructions set out in **Annex II**, and refrain from processing Personal Data for other purposes;
- maintain the confidentiality of Personal Data processed under this Agreement;
- ensure that persons authorised to process Personal Data under the Agreement:
  - undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality;
  - are made aware of issues relating to the protection of Personal Data;
- comply with the Data Protection Regulations and the Instructions formulated by the Customer, and ensure they are complied with by Authorised Recipients and Data Sub-Processors;
- take into account, with respect to its tools, products, applications or services, the principles of Data protection by design and Data protection by default;
- cooperate and comply with the instructions or decisions of any Regulatory Authority, within a timeframe that allows the Customer to comply with the timeframes imposed by such Authorities; and
- not do or fail to do anything that would cause the Customer to breach the Data Protection Regulations.

5.2.2 Cooperation and assistance

High Connexion undertakes to:

- appoint a main contact person responsible for representing it towards the Customer. This main contact person must have the experience, competence, authority and means necessary to carry out their assignment;
- adhere to and actively participate in a spirit of cooperation in order to ensure compliance with the Data Protection Regulations and the good practices recommended by the Customer in the context of these regulations. As such, High Connexion undertakes to make available to the Customer all reasonable means in its possession with a view to providing it with full cooperation, information on the Processing entrusted and assistance in the event of a complaint, request for an opinion, communication, or real or alleged security breach affecting Personal Data. High Connexion further undertakes not to make any public statement or announcement to any third party, including a Regulatory Authority, without first consulting the Customer regarding the content of such public statement or announcement, unless otherwise expressly provided for by the law of a Member State or Third Country;
- modify, transfer and/or delete Personal Data held by it or on its behalf or by a Data Sub-Processor, in accordance with any written Instructions from the Customer;
- inform the Customer immediately:
  - if any Instructions issued by the Customer relating to the Processing are illegal or appear contrary to the doctrine and recommendations of the Regulatory Authority;
  - if the Data Processor deems an Instruction to constitute a violation of the GDPR or any other provision of European Union law or the law of the Member States relating to Data protection. In addition, if the Data Processor is required to transfer data to a third country or to an international organisation, under European Union law or the law of the Member State it is subject to, it must inform the Customer of this legal obligation before the processing, unless the law concerned prohibits such information for important reasons of public interest;
  - if a Personal Data Breach occurs, or if a security breach occurs that affects the IT system of High Connexion or one of its Data Sub-Processors, immediately after becoming aware of it;
  - if High Connexion or a Data Sub-Processor receives a complaint, notice or communication from a Regulatory Authority that directly or indirectly relates to the Processing or either Party's compliance with the Data Protection Regulations; and
  - if High Connexion or a Data Sub-Processor receives a complaint, notice or communication from a Data Subject in connection with exercising their rights.
- assist the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the Processing and the information made available to High Connexion. This assistance may include providing information and performing impact assessments in relation to Processing operations implemented by High Connexion when it is mandatory to perform such an assessment;
- ensure that Personal Data is securely transferred to Authorised Recipients and Data Sub-Processors;
- ensure that Data Sub-Processors comply with the Data Protection Regulations and document this obligation in writing. In the context of performing the Services, High Connexion makes use of Data Sub-Processors to carry out specific Processing. The contact details of the Data Sub-Processors already accepted by the Customer are listed in **Annex II**. In the event of a change or recourse to a new Data Sub-Processor, High Connexion shall inform the Customer in advance. This information must clearly indicate the sub-processed Processing activities, the identity and contact details of the Data Sub-Processor. Once informed by High Connexion, the Customer has a maximum period of 10 working days from the date of receiving this information to submit objections legitimately based in law and in fact. Any sub-processing performed in the context of the Services shall not release High Connexion from its responsibilities and obligations towards the Customer under this Agreement.

5.2.3 Obligations of the Customer

The Customer, in its capacity as Data Controller, guarantees that only the Personal Data necessary to perform the Services shall be processed. As such, the Customer guarantees that it has ensured the lawfulness and compliance of the Processing with regard to the Data Protection Regulations and that it has the appropriate rights, authorisations and/or consents allowing High Connexion to process this Personal Data to perform the Services, and undertakes to compensate High Connexion for all costs, fees (including lawyers' fees), fines and damages incurred by High Connexion in the event of non-compliance with this guarantee. The Customer undertakes to communicate to High Connexion, directly or through the agencies they mandate to organise the Activities, only Personal Data necessary for Processing to perform the Services. The Customer also undertakes to:

- document in writing any Instructions concerning Personal Data Processing to be performed by High Connexion in the Activities, in particular in **Annex II**;
- guarantee, to the extent required by the Data Protection Regulations and, where relevant, that the consent of the Data Subjects whose Personal Data is the subject of the Processing has been collected under conditions that comply with the Data Protection Regulations and that it can demonstrate such compliance;
- if a Data Subject withdraws their consent to the Processing or exercises any of their rights over their Personal Data under the Data Protection Regulations vis-à-vis the Customer, the Customer undertakes to inform High Connexion without delay and to communicate its Instructions to it.

6. PERSONAL DATA PROCESSING BY HIGH CONNEXION AND THE CUSTOMER AS JOINT DATA CONTROLLERS

6.1 Rental of databases by High Connexion for the Customer's benefit

6.1.1 Description of processing

High Connexion has entered into partnerships in order to have qualified databases that allow the Customer to analyse, deduplicate and enrich its database and thus improve its commercial prospecting. High Connexion has entered into a personal data contract with the partner under which the latter, acting as Data Controller, undertakes to comply with the Data Protection Regulations and in particular to fulfil its obligations with regard to:

- collecting consent under the legal conditions,
- Data Subjects' right to be informed,
- taking into account requests for individuals' right to exercise their rights over Personal Data,

- implementation of security measures and organisational measures to ensure the confidentiality and security of Personal Data.

In the context of the Agreement, High Connexion, in its present capacity as Data Controller, is committed to complying with these provisions. This data is collected by High Connexion's partner and made available to the Customer according to specific conditions and provisions in order to develop its commercial prospecting campaigns. Given that the Customer becomes the recipient of this Personal Data collected and its possible combination or enrichment with other Personal Data held by the Customer, the latter acknowledges that it acts as joint Data Controller for the processing thereof. Details of the Processing methods are provided in **Annex III**.

6.1.2 Obligations of the Customer

By using the Personal Data from High Connexion's partners, the Customer acts as a joint data controller. In accordance with the right to information to be provided when the Personal Data has not been collected directly from the data subject (Article 14 of the GDPR), the Customer undertakes to provide all the information in Article 14 of the GDPR, in particular the source the Personal Data originates from, and to implement an effective means of objection in its communications. If the Personal Data relates to cookies and trackers, the Customer is also required to apply the regulations in force and in particular to provide a means for the internet user to effectively withdraw their consent. Upon request, the Customer undertakes to provide High Connexion with all the elements necessary to guarantee and demonstrate compliance with its obligations. It is expressly agreed between the Parties that it is the Customer's responsibility to provide its contact address to enable Data Subjects to exercise their rights. Details are provided in Article 11 of the Agreement. Should High Connexion undergo an inspection by a Regulatory Authority concerning all or part of the processing associated with this Processing, the Customer undertakes to cooperate actively with High Connexion and, where necessary, with this Authority provided that the Customer has the information, evidence or documents needed for this purpose.

6.2 Data enrichment and rental by the Customer for the benefit of partners

6.2.1 Description of processing

High Connexion wishes to be able to benefit from Personal Data for commercial prospecting purposes for the benefit of its partners. High Connexion therefore wishes to be considered a partner of the Customer in order to then be able to communicate, in the name and on behalf of partners, offers or Solutions to Data Subjects who have previously consented to receive such offers. High Connexion acts as joint Data Controller. High Connexion proposes to the Customer that the latter obtain consent from Data Subjects in a clear, explicit, specific and unambiguous manner, on the Customer's sites, applications or any other collection medium, according to the following wording:

"Do you agree to receive offers from our partners?

If so, by what means?

☐ email

☐ SMS

☐ pass wallet

The list of our partners can be found here [insert link]"

High Connexion undertakes to the Customer to ensure that its partner(s) comply(ies) with the Regulations and in particular implement(s) the right to information to be provided when the Personal Data has not been collected directly from the Data Subject (Article 14 of the GDPR), and in particular to mention the source the Personal Data originates from and to implement an effective means of objection in its communications. Details of the Processing methods are provided in **Annex III**.

6.2.2 Obligations of the Customer

By allowing High Connexion and/or its partners to carry out commercial prospecting based on Personal Data collected by the Customer on its website, application or by any other means, the Customer acts as joint data controller. In this context, the Customer undertakes to obtain the Data Subjects' prior and informed consent, in accordance with the applicable Regulations, to mention its privacy policy and to identify the partners concerned. The Customer undertakes to inform High Connexion of any request to exercise Data Subjects' rights that it receives in the context of this Processing and in particular of the rights of objection to receiving commercial prospecting. The Customer undertakes to keep the Personal Data for a limited period corresponding to the purpose. At the end of this period, the Customer undertakes to again obtain consent to commercial prospecting, under the same terms and conditions as before. Upon request, the Customer undertakes to provide High Connexion with all the elements necessary to guarantee and demonstrate compliance with its obligations (such as timestamps of actions taken and interactions of Data Subjects on the Customer's website, application or any other medium). Should High Connexion undergo an inspection by a Regulatory Authority concerning all or part of the processing associated with the personalisation, the Customer undertakes to cooperate actively with High Connexion and, where necessary, with this Authority provided that the Customer has the information, evidence or documents needed for this purpose.

7. SECURITY

High Connexion and the Customer undertake to implement the following security measures:

- ensure that appropriate technical and organisational measures have been put in place against accidental or unlawful destruction, loss, modification, unauthorised disclosure or access to Personal Data held or processed, including all necessary measures to ensure compliance with the Personal Data security requirements in the Data Protection Regulations. In the event of a mismatch between the security measures put in place and the Processing and/or Personal Data entrusted to High Connexion, the latter shall inform the Customer and propose a remediation plan within a reasonable timeframe;
- limit access to Personal Data to only those persons acting under its authority, and only to Personal Data strictly necessary to perform the Services subject to the Processing provided for in this Agreement;
- ensure that its IT systems are:
  - sufficiently protected, among other things, against viruses and the interception of Personal Data within the network;
  - able to restore the availability of and access to Personal Data within the appropriate timeframes in the event of a physical or technical incident.

8. PERSONAL DATA BREACH

If an actual or potential Personal Data Breach occurs that affects the Services of High Connexion or a Data Sub-Processor, High Connexion undertakes to:

- notify the Customer of any security breach that may result in a Personal Data Breach as soon as possible, and at the latest within a maximum of forty-eight (48) hours following knowledge of said breach by electronic message;
- accompany the notification with any useful documentation to enable the Customer, if necessary, to notify the Regulatory Authority or the Data Subject of this breach. As such, High Connexion shall specify the following points as far as possible:
  - a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects affected by the breach and the categories and approximate number of Personal Data records affected;
  - the name and contact details of the data protection officer and/or another point of contact from whom further information can be obtained;
  - a description of the likely consequences of the Personal Data Breach; and
  - a description of the measures taken or envisaged to remedy the Personal Data Breach, including, where applicable, measures to mitigate any negative consequences thereof.
- communicate the information defined above in a staggered manner and without undue delay if it is not possible for High Connexion to provide all the information specified at the same time, or if certain elements already communicated can be clarified.

Where the Parties act as joint Data Controllers, the Party concerned shall notify the other Party within 24 hours of becoming aware of it to enable joint notification by the Parties to the Regulatory Authority and, if necessary, communication to Data Subjects. They must be drafted jointly by the Parties and in accordance with the Data Protection Regulations.

9. ACCOUNTABILITY

The Parties mutually undertake, in a spirit of accountability, to:

- regularly update the register of Processing activities as provided for in Article 30(2) of the GDPR, and keep a written record of all Processing and Instructions relating to Processing carried out on behalf of the Customer;
- regularly update the register of security breaches which is filled in by the Parties as soon as a Personal Data Breach occurs, whether or not this breach has been reported to the Regulatory Authority;
- keep documentation relating to employee training or awareness on the protection of Personal Data;
- document, as far as possible, all procedures put in place to protect Personal Data through its Security Measures;
- regularly update the Security Measures.

10. RECIPIENTS OF PERSONAL DATA – USE OF DATA PROCESSORS

In addition to the provisions provided above, High Connexion and the Customer may use one or more Data Sub-Processor(s) to carry out specific processing activities in compliance with the Purposes defined for the Processing in the Annex. In this case, the Parties undertake and ensure that these selected Data Sub-Processors provide sufficient guarantees to comply with the Data Protection Regulations. If the Data Sub-Processor(s) do not fulfil their obligations with regard to the protection of Personal Data, the Party that selected the processor remains solely and fully responsible for these breaches. If the Data Sub-Processor is jointly selected by the Parties, the responsibility if this processor breaches the Data protection obligations shall be shared.

11. DATA SUBJECTS

When acting as Data Processor, High Connexion undertakes to the Customer, in the context of a request to exercise rights, to:

- notify the Customer, by email to the email address indicated by the Customer in the Annexes, immediately and within a maximum of five (5)

working days, of any request from a Data Subject wishing to exercise their rights under the Data Protection Regulations (in particular, requests for access, rectification, erasure and portability of Data and requests to object to the Processing);
- cooperate fully with the Customer in order to respond, within a reasonable time in view of their nature and number, to requests from Data Subjects wishing to exercise their rights under the Data Protection Regulations, provided that the Customer does not have all the information in its possession allowing it to manage these requests to exercise rights; and
- not to disclose Data, including Personal Data, to the Data Subject without first consulting and obtaining the written consent of the Customer.

It is the responsibility of the Party acting as Data Controller to provide the information to the Data Subjects of the Processing operations at the time of collecting the Personal Data. If both Parties act as joint Data Controllers, it is the Customer's responsibility to provide the information to the Data Subjects of the Processing operations as provided for in Articles 13 et seq. of the GDPR at the time of collecting the Personal Data. The Customer undertakes in particular that Data Subjects' consent, when required, is collected in accordance with the provisions of the GDPR, i.e. a manifestation of free, specific, informed and unambiguous consent by which the Data Subject agrees, via a declaration or a clear positive act, to the processing of their Personal Data. In particular, the Customer undertakes to inform the Data Subjects that the Data transmitted to High Connexion may be transmitted to partners (mentioning them). The Customer undertakes to provide High Connexion on first request with proof of consents collected in connection with the Personal Data transmitted in this context. The Parties agree that Data Subjects may exercise their rights vis-à-vis the Customer, in accordance with its privacy policy. The Customer undertakes to notify High Connexion, by email to the email address indicated by High Connexion in the Annexes, immediately and within a maximum of five (5) working days of any request from a Data Subject wishing to exercise their rights under the Data Protection Regulations. The joint Data Controllers must help each other to respond to these requests to exercise the rights of Data Subjects.

12. TRANSFERS TO THIRD COUNTRIES

If it acts as data processor, High Connexion shall not transfer Personal Data to Third Countries without the Customer's prior written consent. High Connexion shall comply with the Instructions issued by the Customer concerning transfers of Data to Third Countries, except when High Connexion is required, in accordance with the applicable laws, to transfer Personal Data to a Third Country. The Customer consents via the Agreement to the transfer of Personal Data to the entities and locations mentioned in the Annexes, strictly for the purposes of performing the Services, and provided that:
- the Third Country is a country which, according to the European Commission, has an adequate level of protection of Personal Data; or
- High Connexion meets one of the following conditions:
  - High Connexion enters into or obtains from the entity identified in the Annexes an agreement on the transfer of data based on the model Standard Contractual Clauses drawn up by the European Commission;
  - Transfers made with the entity referred to in the Annexes fall under the exception regime referred to in Article 49 of the General Data Protection Regulation No 2016/679.

High Connexion shall ensure that no subsequent transfer of Personal Data to another Third Country takes place unless the Customer gives its prior consent to such transfer, or such subsequent transfer meets the requirements set out above.

13. LIABILITY

When acting as Data Processor, High Connexion agrees to indemnify the Customer for all direct material and immaterial damage it suffers resulting from a failing or negligence by High Connexion, its employees, representatives, agents or Data Sub-Processors in the security of Personal Data. High Connexion undertakes to implement all necessary and reasonable means to ensure the security of the Processing, and shall therefore be liable for damages related to a security failure attributable exclusively to High Connexion resulting in unavailability, loss of traceability, doubt about the integrity or lack of confidentiality of Personal Data. It is nevertheless expressly agreed between the Parties that zero risk in terms of security does not exist and that High Connexion remains subject to an obligation of means. Nor can it be held liable for damages related to a security failure attributable to the technological, software or IT choices made by the Customer, in particular for reasons of budgetary restrictions, when High Connexion has proposed other solutions ensuring a higher level of security and guarantees. High Connexion's liability for costs, expenses, losses, damages or other liabilities arising out of or in connection with the breach of the Agreement (whether by High Connexion or its employees, representatives, agents or Data Sub-Processors, the Authorised Recipients) may only be invoked within one (1) year of knowledge of the damage. When the Parties act as joint Data Controllers, each Party shall indemnify the other against any action, complaint or claim made by Data Subjects or the Regulatory Authority on Personal Data subject to Processing which has its source in non-compliance with the GDPR and/or the Agreement, and according to the specific obligations of each Party. In this case, the defaulting Party shall defend the other Party and bear the costs of advice and any damages to which the latter may be sentenced by a court decision based on a breach of the provisions of the GDPR.

14. CONFIDENTIALITY

In the context hereof, the phrase "Confidential Data" includes any Data, information or documents disclosed by the Parties, in writing or orally, meeting the conditions of this article, and including without limitation any written or printed documents, any samples, models or data communicated by either Party, or resulting therefrom, or more generally any means of disclosing Confidential Data. The provisions hereof shall apply to information or documents, in whatever form, transmitted by a Party and designated as Confidential Data by affixing or adding a stamp or a formula to their support or by establishing and delivering or sending a written notification to this effect, or when they are disclosed orally, whose confidential status has been brought to the Parties' attention, at the time of their disclosure; the confidential status also applies to Data which by its nature is confidential, regardless of any such mention. The Parties undertake during the term of the Contract, and for a period of ten (10) years from its expiry for any reason whatsoever, that all Data (including information, documents, know-how, methods, of any nature whatsoever) exchanged under the Contract and this Agreement:
- shall be protected and kept strictly confidential and processed with the same degree of care and protection as they accord to their own Confidential Data of equal importance;
- shall be disclosed internally only to the members of their respective staff who need to know about it and shall be used by them only for the purpose defined herein;
- shall not be used, in whole or in part, for any purpose other than that defined herein, without the other Party's prior written consent;
- shall be neither disclosed nor liable to be disclosed, either directly or indirectly, to any third party or to any persons other than those mentioned in subparagraph (ii) above;
- shall not be copied, reproduced or duplicated in whole or in part when such copies, reproductions or duplicates would be liable to harm the other Party's interests.

All Data, information and reproductions thereof transmitted by the Parties shall remain their property and must be returned to the other Party immediately upon its request. Conversely, the Parties shall have no obligation and shall not be subject to any restriction with regard to all the Confidential Data which they can prove:
- entered the public domain voluntarily before disclosure or after but in this case without any fault being attributable to the Party; or
- is already known to the other Party, which knowledge can be demonstrated by the existence of appropriate documents in their files; or
- was lawfully received from a third party, without restriction or violation hereof; or
- was published without contravening the provisions hereof; or
- the use or disclosure thereof was authorised in writing by the other Party; or
- has not been designated or confirmed as Confidential Data.

The expiration or termination hereof shall not have the effect of releasing the Parties from their obligations to comply with the provisions of this article concerning the use and protection of information received before the date of termination or the arrival of the expiration. The obligations contained in these provisions shall remain in force for the period defined in this article. It is understood that the Parties may communicate the Confidential Data to their insurers, advisers, lawyers, persons in charge of audit and internal control or to any administration or jurisdiction provided that the latter are bound by a confidentiality clause and/or by professional secrecy.

15. AUDIT AND CONTROL

The Customer may conduct audits on documents to make sure of High Connexion's level of compliance. Confidential items entrusted to High Connexion by other customers are not concerned by the audit on documents. The Customer may also conduct objective audits of compliance with the Data Protection Regulations on the Processing operations carried out for the purpose of performing the Services under the conditions defined below:
- the audit is conducted by an external auditor selected by the Customer for its expertise, independence and impartiality;
- the selected auditor is bound to the Parties by a confidentiality agreement and/or by professional secrecy;
- the Customer shall notify High Connexion, in writing and subject to a minimum of ten (10) working days' notice, of its intention to have a compliance audit carried out;
- in no way may the audit carried out deteriorate or slow down the Services offered by High Connexion or adversely affect High Connexion's organisational management. Audit operations must not involve actions that could potentially damage High Connexion's infrastructure or interfere with other services provided by High Connexion to other customers;
- an identical copy of the audit report shall be given to the Customer as well as to High Connexion following the completion of the audit assignment and on which the Parties may make comments. This report may, if necessary, be subject to in-depth examination by a steering committee;
- the costs of the compliance audit shall be borne exclusively by the Customer;
- the Customer may only order compliance audits within the limit of one (1) audit per year; and
- High Connexion shall have a period of three (3) months from the communication of the audit report to correct, at its own expense, the failures and/or non-conformities. If necessary, High Connexion may exceptionally

extend this period by three (3) months after expressly informing the Customer and objectively justifying such an extension.

High Connexion undertakes to allow the selected auditor access to its sites, facilities, documents and information necessary to assess its good level of compliance, and shall cooperate with it fully on the successful completion of its assignment.

In the event of an inspection carried out by a competent Regulatory Authority that may concern the Customer's Processing, High Connexion undertakes to cooperate fully with the Regulatory Authority. In the event of an inspection carried out by a competent Regulatory Authority with regard to the Customer, High Connexion undertakes to fully assist the Customer regarding the Processing carried out in the context of the Services. All the Data collected under the Audits and Inspections is considered "Confidential Data" within the meaning of the article "Confidentiality" hereof.

16. APPLICABLE LAW AND JURISDICTION

The Agreement shall be governed by and interpreted in accordance with French law. Any dispute arising out of or in connection with the Agreement as to its validity, interpretation or execution shall be subject to the exclusive jurisdiction of the Commercial Court of Paris and to the French National Data Protection Authority (Commission Nationale Informatique et Libertés, CNIL), to which each of the Parties irrevocably submits. Before any litigation, the Parties shall seek, in good faith, to amicably settle their disputes relating to the validity, interpretation, performance, non-performance, interruption, termination or cessation of this Agreement as well as the partial or total termination of commercial relations between the Parties, for any reason and on any basis whatsoever. The Parties must meet to compare their points of view and make any useful observations to enable them to find a solution to the conflict between them. The Parties shall endeavour to reach an amicable agreement within thirty (30) days of notification by one of them of the need for an amicable agreement, by registered letter with acknowledgement of receipt.

ANNEXES ON THE METHODS OF PROCESSING PERSONAL DATA

I. High Connexion as Data Controller

I.a) The Customer's Personal Data processed by High Connexion on High Connexion's platforms for the implementation and performance of the Services

Data Controller	High Connexion
Data Processor	The Customer
Data Sub-Processor	TH2, SFR, TDF, HighCo
Data hosting	The Data is hosted at TH2 located in Paris or at SFR in Venissieux or at TDF (via HighCo) located in Aix-en-Provence
Purpose of Processing	Management of access by the Customer (Users and Administrators) to High Connexion's platforms and to allow the proper performance of the Services by High Connexion for the Customer's benefit
Personal Data processed	• Identification data of administrators and users of High Connexion's platforms: Title, surname, first name, email, position, status, telephone • Connection data: login and password, registration date, last login, history of actions on the platform, account closure • Cookies and trackers: functional and analytical
Legal basis of processing	• Contractual basis (Contract for the performance of the Services) • Consent of individuals (for the opt-in newsletter if applicable) • Legitimate interest (to prevent fraud and for statistical and Service improvement purposes) • Legal obligation (request from administrations or institutions)
Categories of data subjects	Users and Administrators of High Connexion's platforms, employees of the Customer or persons authorised by the Customer (mandated agencies)
Source of Personal Data	Registration of individuals on High Connexion's platforms (logged-in environment)
Information and management of individuals' rights	Individuals are informed of their rights on High Connexion's platforms (privacy policy) and can exercise their rights by contacting delegue-protection-donnees@highco.com, specifying "*High Connexion Platform*"
Data flows outside of the EU	None
Data retention period	Personal data shall be kept for the duration of the contractual relationship with the Customer and for 5 years after the end of this relationship. Logs are kept for between 6 months and 1 year. Cookies and trackers are kept for a maximum of 25 months.

I.b) The Customer's Personal Data processed by High Connexion for the purpose of managing the commercial relationship with the customer

Data Controller	High Connexion
Data Processor	The Customer
Data hosting	The Data is hosted at TH2 located in Paris or at SFR in Venissieux or at TDF (via HighCo) located in Aix-en-Provence
Purpose of Processing	Management of the commercial relationship with the Customer and in particular sending quotations and invoices
Personal Data processed	Identification data of the Customer's employees: Title, surname, first name, email, position, address, telephone
Legal basis of processing	• Contractual basis (Contract for the performance of the Services) • Legitimate interest (to avoid fraud and to improve the Services) • Legal obligation (request from administrations or institutions)
Categories of data subjects	Employees of the Customer or any person mandated by the Customer
Source of Personal Data	Commercial documents and exchanges
Information and management of individuals' rights	Individuals are informed of their rights in the Contract and can exercise their rights by contacting delegue-protection-donnees@highco.com
Data flows outside of the EU	None
Data retention period	Personal data shall be kept for the duration of the contractual relationship with the Customer and for 5 years after the end of this relationship.

II. High Connexion as Data Processor

It is the Customer's responsibility to give High Connexion instructions for the processing of Personal Data and therefore to supplement/modify these annexes by any written means. Failing this, High Connexion cannot be held responsible for any breach resulting from a lack of precision in the Customer's instructions.

II.a) Personal Data of data subjects processed by High Connexion in the name and on behalf of the Customer in the context of implementing the Solutions (technical solutions such as the implementation of games, pass wallet, etc.)

Data Controller	The Customer
Data Processor	High Connexion
Data Sub-Processors	Facilitators for push SMS, emails, voice, notifications
Data hosting	The Data is hosted at TH2 located in Paris or at SFR in Venissieux
Recipients	French operators (Orange, Free, SFR Altice, Bouygues Telecom, etc.) Apple and Google Pay for the pass wallet Google for the "Verified SMS" option
Purpose of Processing	Implementation and management of technical promotional, marketing or payment (billing) solutions on behalf of the Customer: ● For marketing services: ○ Messaging (sending SMS, email, voice messages, push notification, MMS, instant messaging, enhanced SMS, etc.), ○ Provision of digital solutions (distribution of content on the wallet, SMS, web & mobile and audiotel games), ● For billing services: management of financial transactions of a data subject who makes a payment of an operator bill or via any other payment channel: ○ to purchase digital content (music, videos, press articles, ticketing, etc.) ○ for donation campaigns (one-off or recurring) ○ to participate in SMS+, SVA+ or Internet+ games
Personal Data processed	● Identification data: surname, first name, email, telephone number, etc. ● Connection data: pass ID, log management, download date, date of last interaction, history of links clicked on the wallet, history of offers, etc. ● Transaction data: purchase, amount, payment method, etc. ● Cookies and trackers
Legal basis of processing	● Contract: acceptance of the terms of the offer (GTCU, game rules, the Customer's policies, etc.) ● Legitimate interest (to avoid fraud and improve the Services) ● Legal obligation (request from administrations or institutions)
Categories of data subjects	Consumers (customer or prospect of the Customer) wishing to benefit from offers or content put in place by the Customer
Source of Personal Data	● Collection via a form (desktop or mobile) or ● Data provided by the Customer or ● Data collected during the purchase of content, during donations or games
Information and management of individuals' rights	Information in the Customer's privacy policy Exercise of rights vis-à-vis the Customer
Data flows outside of the EU	None
Data retention period	Personal data is kept for 1 year from processing by High Connexion. Cookies and trackers are kept for a maximum of 25 months.

II.b) Consumers' Personal Data processed by High Connexion in the name and on behalf of the Customer for the purposes of commercial prospecting

Data Controller	*The Customer*
Data Processor	*High Connexion*
Data Sub-Processors	*N/A*
Data hosting	*The Data is hosted at TH2 located in Paris or at SFR in Venissieux*
Recipients	*Partners of the Customer*
Purpose of Processing	*Commercial prospecting on behalf of the Customer and/or its partners*
Personal Data processed	● *Identification data: title, surname, first name, email, town/city, postcode* ● *Log and connection data: date and tracking of logins* ● *Presence of the pass (pass ID)* ● *Consents and opt-ins* ● *Cookies and trackers*
Legal basis of processing	*Consent of individuals (via the opt-in newsletter and/or partner); this consent is collected in a free, specific, informed and unambiguous manner*
Categories of data subjects	*Consumers wishing to receive information or commercial offers from the Customer and/or its partners*
Source of Personal Data	*Opt-in box (not pre-selected) during collection (desktop or mobile)*
Information and management of individuals' rights	*Information in the privacy policy* *Exercise of rights vis-à-vis the Customer*
Data flows outside of the EU	*None*
Data retention period	*Personal data is kept for 12 months from obtaining the consent (unless consent is withdrawn, which may occur at any time)* *Cookies and trackers are kept for a maximum of 25 months.*

III. High Connexion as joint Data Controller

III.a) Rental of personal data from High Connexion to the Customer

Data Controller	High Connexion The Customer
Purpose of Processing	Enrichment and/or deduplication and/or analysis of the Customer's databases for the purpose of commercial prospecting through sending commercial offers in particular
Personal Data processed	● Identification data: surname, first name, telephone number, email, etc. ● Cookies and trackers: token, etc.
Legal basis of processing	Consent (opt-in)
Categories of data subjects	Individuals who have agreed upstream to receive offers from identified partners (qualified opt-ins)
Source of Personal Data	● Enriched databases of High Connexion or ● Databases rented from third-party partners
Information and management of individuals' rights	● *(as a reminder: right to direct information of Data Subjects under Article 13 of the GDPR:* ○ *Information by High Connexion customers (who supply High Connexion's database)* ○ *Information by the third parties from which High Connexion rents the databases)* ● Indirect right to information to be provided by the Customer (Article 14 of the GDPR) ● Exercise of rights towards the Customer, with High Connexion being able to collaborate
Data flows outside of the EU	None
Data retention period	Maximum 3 years from the individual's last action Withdrawal of consent at any time at the individual's request

	● *High Connexion*
Recipients	*Partners*
Purpose of Processing	*Enrichment and rental of data to third-party partners to enable them to send commercial offers (generate leads) to people who have agreed to receive such offers (opt-in)*
Personal Data processed	● *Identification data: title, surname, first name, email, town/city, postcode* ● *Log and connection data: date and tracking of logins* ● *Consents and opt-ins* ● *Cookies and trackers*
Legal basis of processing	● *Consent: opt-in not pre-checked, clear, free, specific* ● *Legitimate interest (to avoid fraud and improve the Services)* ● *Legal obligation (request from administrations or institutions)*
Categories of data subjects	*Customers and prospects of the Customer wishing to benefit from offers from partners*
Source of Personal Data	● *Collection via an opt-in or* ● *Customer's file*
Information and management of individuals' rights	● *Right to information to be provided by the Customer* ● *Exercise of rights towards the Customer, with High Connexion being able to collaborate*
Data flows outside of the EU	*None*
Data retention period	*Personal data is kept for 1 year from the end of the reimbursement operation. Cookies and trackers are kept for a maximum of 25 months.*

III.b) Personal data of consumers by High Connexion for enrichment and rental to third parties

Joint Data Controllers	● *The Customer*