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

IT HAS PREVIOUSLY STATED THE FOLLOWING

This Agreement on the processing of personal data and its annexes (hereinafter referred to as "Agreement") supplement the provisions of the General Terms and Conditions of Sale as well as the quote (together the "Contract") applicable between High Connexion and the Client (as mentioned on the participation order, acting in its name and on its behalf or through an agent in the name and on behalf of the Client) with regard to personal data processing operations carried out pursuant to the Contract. In this context, the Parties agree that the present "Contract for the processing of personal data" (hereinafter the "Agreement") determines the conditions under which the Parties may process personal data.

THIS HAVING BEEN PREVIOUSLY EXPOSED, IT WAS AGREED AS FOLLOWS

1. DEFINTIONS

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

Agreement	Refers to the present Data Protection Agreement completed by the Annexes on the methods of processing personal data.
Activities	Refers to the marketing and payment activities carried out by HIGH CONNEXION, as defined in the T&Cs.
Regulatory authority	Means any authority competent in the protection of Personal Data.
Contract	Refers to the contractual package at the end of which the Client entrusts HIGH CONNEXION to carry out the services. In the absence of a specific service contract, the General Terms and Conditions as well as the order for participation from High Connexion apply.
Authorized recipient	Means an administrator, employee or Subcontractor of one of the Parties who has a legitimate need to access Personal Data in connection with the performance of 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 it is Personal Data or not (ex: financial data, customer data, strategic data, technical, professional, administrative, commercial, legal, accounting, etc.).
Personal data	Means any information relating to an identified natural person or that can be identified as such, either directly or indirectly by aggregation of information, by reference to an identification number or elements specific to it: name, address, telephone number, IP address, email address, vehicle registration number, professional registration number, username/login, password, login data, etc.
Authorized purpose	Means the purpose of the Processing of Personal Data carried out by the Processor, in accordance with the Annexes.
Instructions	Refers to all instructions written by the Data Controller for the Processor. These instructions are a strict formalism and cannot be considered as such unless they are formulated in writing in the Agreement, in an email or paper from a duly authorized person. The instructions shall be accompanied by any necessary documentation for their proper execution and shall be set out in the Annexes. These annexes must be completed by the Client by any written means.
Third countries	Means any State not a member of the European Union. This terminology also includes any international organization with countries that are not members of the European Union.
Person concerned	Means any natural person whose Personal Data is subject to Processing.
Security measures	Means the physical, technical and organizational measures of the Parties and regularly updated.
Regulation on data protection	Refers to the regulations in force applicable to the Processing of Personal Data 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 «General Data Protection Regulation» (hereinafter «GDPR»); (ii) the law "Informatique et Libertés" n°78-17 of January 6, 1978 modified; (iii) any legislation coming into force that may affect the Processing covered by the Agreement; (iv) any best practice guidelines published by the competent Regulatory Authorities or the European Data Protection Board.
Data Processing Manager	Means, according to the Processing operations, the Client or High Connexion as a legal entity determining alone or jointly the means and purposes of the Processing carried out within the framework of the execution of the Contract.
Services	Refers to the services provided by High Connexion as part of the Contract.
Subcontractor	Means, according to the Processing, High Connexion or the Client as a legal entity carrying out Personal Data Processing operations on behalf of and according to the other Party. The subcontractor(s) who carry out Personal Data Processing strictly following the Instructions issued by the Controller are qualified as "Subsequent Subcontractor(s)".
Processing	Means any operation or set of operations carried out or not with the help of automated processes and applied to Personal Data or sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction.
Personal data breach	Means a security breach that accidentally or unlawfully results in access to or the destruction, loss, alteration, unauthorized disclosure of Personal Data transmitted, stored or processed.

2. DURATION AND CONTRACTUAL HIERARCHY

The Agreement enters into force upon acceptance of the quote for the duration necessary for the Treatments agreed between the Parties. The provisions of the Agreement which by nature are intended to last beyond the term of the Contract remain applicable and retain their full effect. In the event of a 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 case of contradiction between the terms of the contract itself of the Agreement and the terms of the Annexes, the terms of the Annexes shall prevail.

3. COMPLIANCE WITH THE REGULATION ON DATA PROTECTION

Each of the Parties undertakes to comply with the Data Protection Regulation.

4. PROCESSING OF PERSONAL DATA BY HIGH CONNECTION AS A CONTROLLER

4.1 Access and use of High Connexion platforms

4.1.1 Treatment description

High Connexion acts as a Data Controller when it collects, stores, modifies, uses or deletes the Personal Data of Users, Administrators and any person acting on behalf of and for the account of the Client on the platforms set up by High Connexion (MGS, High Push, EP Gateway, Wallet, billing platform, etc.) for the needs of the Services and on the basis of the execution of the Contract. He notably proceeds with the creation, management of accounts and the proper monitoring of the management of the different actions of the Client via these platforms. In accordance with the privacy and cookie policy on the High Connexion platforms, Data Subjects may exercise their rights of access, rectification, erasure, of opposition, portability and limitation of personal data concerning them for the purposes of Processing with High Connexion

by sending an email to dpo@highconnexion.com. Details on this Processing are provided in **Annex I.**

4.1.2 Obligations of the Client

The Client is responsible for managing the access rights of users to the High Connexion platforms and must immediately inform High Connexion in case of departure and/or change of Users and Administrators so that High Connexion closes and/or modifies their accounts. Failing this, any action by a person representing the Client who is not or no longer authorised cannot entail any liability on the part of High Connexion.

4.2 Management of the Contract and the commercial relationship

As part of the administrative and contractual management of the business relationship with the Client, High Connexion processes personal identification data of representatives, employees and/or agents of the Client. The personal data collected concerns professional contact details, including in particular, last name, first name, email address, phone number. This Personal Data is mandatory for the conclusion of the Contract. Details on this Processing are provided in **Annex I.**

5. PROCESSING OF PERSONAL DATA BY HIGH CONNECTION AS SUBCONTRACTOR

5.1 Nomination and role of High Connexion

The Client, in his capacity as Data Controller, designates High Connexion as Sub-Processor to proceed with the collection and to process the Personal Data on its behalf and for its account in order to achieve the Permitted Purposes referred to in Annex II of the Agreement in connection with the provision of the Services. In accordance with the applicable regulations, High Connexion has appointed a data protection officer who may be contacted by email at the email address dpo@highconnexion.com OR by paper mail to the following address: HIGH CONNEXION – DPO Service, 9 Avenue des Saules 69600 OULLINS, France. The Customer shall transmit by any written means to High Connexion the name and contact details of its data protection officer, if it has appointed one in accordance with Article 37 of the GDPR.

5.2 General obligations of High Connexion as a subcontractor

5.2.1 Instructions and compliance

High Connexion guarantees to the Client that it:

- processes only Personal Data necessary for the Authorized **Purposes, in accordance with the Instructions set out in** Annex II, and refrains from processing Personal Data for other purposes;
- preserves the confidentiality of Personal Data processed under this Agreement;
- ensure that persons authorized to process Personal Data under the Agreement:
  - undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality;
  - are sensitized on issues related to the protection of Personal Data;
- complies with the Data Protection Regulation as well as the Instructions formulated by the Client, and ensures their compliance by the authorized Recipients and subsequent Subcontractors;
- takes into account, with regard 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 period that allows the Client to meet the deadlines imposed by said Authorities; and
- does not do or fails to do something that would lead the Client to violate the Data Protection Regulations.

5.2.2 Cooperation and assistance

High Connexion is committed to:

- designate a privileged interlocutor in charge of representing it with the Client. This privileged interlocutor must be endowed with the experience, competence, authority and means necessary for the exercise of his mission;
- adhere to and actively participate in a logic of cooperation in order to ensure compliance with the Data Protection Regulation and the best practices recommended by the Client within the framework of this regulation. As such, High Connexion undertakes to provide the Client with all reasonable means in its possession to provide him with full cooperation, information on the Treatments entrusted and assistance in case of complaint, request for advice, communication, or actual or suspected security breach affecting Personal Data. High Connexion further undertakes not to make any statement or public announcement to a third party, including a Regulatory Authority, without having first consulted the Client regarding the content of such statement or public announcement, unless expressly otherwise provided by the law of a Member State or third country;
- modify, transfer and/or delete Personal Data held by him or on his behalf or by a subsequent Processor, in accordance with any written Instructions from the Client;
- inform the Client immediately:
  - if the Instructions issued by the Client relating to the Processing are illegal or appear contrary to the doctrine and recommendations of the Regulatory Authority;
  - if the Processor considers that an Instruction constitutes a violation of the GDPR or any other provision of Union law or the law of the Member States relating to Data protection. In addition, if the Processor is required to transfer data to a third country or an international organization under Union law or the law of the Member State to which it is subject, it must inform the Client of this legal obligation before processing, unless the law concerned prohibits such information for important reasons of public interest;
  - in the event of a Personal Data Breach, or in the event of a security breach affecting the computer system of High Connexion or one of its subsequent Subcontractors, immediately after becoming aware of it;
  - if High Connexion or a subsequent Subcontractor receives a complaint, notice or communication from a Regulatory Authority that directly or indirectly concerns the Processing(s) or compliance of either Party with the Data Protection Regulation; and
  - if High Connexion or a subsequent Subcontractor receives a complaint, notice or communication from a Data Subject in connection with the exercise of its rights.
- to 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 conducting impact assessments in relation to the Processing operations implemented by High Connexion where such an assessment is mandatory;
- ensure that the Personal Data is securely transferred to authorised Recipients and Sub-contractors;
- ensure that Sub-processors comply with the Data Protection Regulation and document this obligation in writing. As part of the provision of the Services, High Connexion uses subsequent Subcontractors to carry out specific Processing. The contact details of the subsequent **Subcontractors already accepted by the Client are mentioned in Appendix II**. In the event of a change or recourse to a new Subcontractor, High Connexion shall inform the Client beforehand. This information must clearly indicate the activities of Processing subcontracted, the identity and contact details of the subsequent Subcontractor. The Customer, informed by High Connexion, has a maximum period of 10 working days from the date of receipt of this information to present legitimate objections based on law and in fact. Any further subcontracting carried out in connection with the Services shall not release High Connexion from its responsibilities and obligations to the Customer under this Agreement.

5.2.3 Obligations of the Client

The Client, in its capacity as Data Controller, guarantees that only the Personal Data necessary for the performance of the Services are processed. In this respect, the Client guarantees that he has ensured the lawful and compliant nature of the Processing operations with regard to the Data Protection Regulations and that he has the rights, authorizations and/or adequate consents allowing the processing of this Personal Data by High Connexion for the performance of the Services and undertakes to indemnify High Connexion against all costs, fees (including those of a lawyer), fines, damages incurred by High Connexion in the event of non-compliance with this guarantee. The Client undertakes to communicate, directly or through the agencies they entrust for the organization of the Activities, to High Connexion only the Personal Data necessary for the Processing for the performance of the Services. The Client also undertakes to:

- document in writing any Instructions concerning the Processing of Personal Data to be carried out by High Connexion in the Activities, particularly in **Appendix II;**
- ensure, to the extent required by the Data Protection Regulation and, where relevant, that the consent of the Data Subjects whose Personal Data is subject to Processing has been obtained under conditions compliant with the Data Protection Regulations and that it is able to demonstrate this compliance;
- in the event that a Data Subject withdraws their consent to the Processing or exercises any of their rights over their Personal Data under the Data Protection Regulation with the Client, the Client undertakes to inform High Connexion without delay and to communicate its Instructions.

6. PROCESSING OF PERSONAL DATA BY HIGH CONNECTION AND BY THE CLIENT AS JOINT CONTROLLERS

6.1 Rental of databases by High Connexion for the benefit of the Client

6.1.1 Treatment description

High Connexion has entered into partnerships in order to have qualified databases allowing the Client to analyze, deduplicate, enrich its database and thus improve its commercial prospecting. High Connexion has concluded a personal data contract with the partner under which the latter, who acts as Data Controller, undertakes to comply with the Data Protection Regulation and in particular to fulfill its obligations regarding:

- collection of consent under the legal conditions,
- right of information for the Data Subjects,
- consideration of requests for rights from individuals in order to exercise their rights over Personal Data,
- implementation of security measures and organizational measures to ensure the confidentiality and security of Personal Data.

As part of the Agreement, High Connexion is strongly committed, in its present capacity as Data Controller, to respecting these provisions. This data is collected by the partner of High Connexion and made available to the Client under precise conditions and provisions in order to develop its commercial prospecting campaigns. Given that the Client is made a recipient of this collected Personal Data and their possible combination or enrichment with other Personal Data held by the Client, the

latter acknowledges that he acts as a joint Data Controller for their processing of these. Details on the terms of the Processing are provided in **Appendix III.**

6.1.2 Obligations of the Client

By using the Personal Data of High Connexion's partners, the Customer acts as a joint controller. In accordance with the right of information to be provided when the Personal Data have not been directly collected from the data subject (article 14 of the GDPR), the Client undertakes to provide all the information set out in article 14 of the GDPR, and in particular the source from which the Personal Data comes and to implement an effective means of opposition in its communications. If the Personal Data concerns cookies and tracers, the Client is also required to apply the regulations in force and in particular to provide a means for the user to effectively withdraw their consent. Upon request, the Client undertakes to provide High Connexion with all elements necessary to guarantee and demonstrate compliance with its obligations. It is expressly agreed between the Parties that it is the responsibility of the Client to provide their contact address to allow the Data Subjects to exercise their rights. Clarification is provided in Article 11 of the Agreement. In the event of a control of High Connexion by a regulatory Authority concerning all or part of the processing associated with this Processing, the Client undertakes to actively cooperate with High Connexion and, if applicable, with this Authority as soon as the Client holds the information, evidence or documents useful for this purpose.

6.2 Enrichment, data rental by the Client for the benefit of partners

6.2.1 Treatment description

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 as a partner of the Client in order to then be able to communicate, on behalf and for the account of partners, offers or Solutions to the Data Subjects who have previously agreed to receive such offers. High Connexion acts as a joint Data Controller. High Connexion proposes to the Client that the latter obtain consent from the Data Subjects in a clear, explicit, specific and unambiguous manner, on the Client's sites, applications or any other collection medium, according to the following wording:

« Do you agree to receive offers from our partners?

If yes, by what means?

☐ e-mail

☐ SMS

☐ pass wallet

The list of our partners is here [put a link]»

High Connexion strongly supports the Client in ensuring that its partner(s) comply with the Regulation and, in particular, implements the right to information to be provided when the Personal Data has not been directly collected from the Person concerned. (article 14 of the GDPR), and in particular to mention the source from which the Personal Data comes and to implement an effective means of opposition in its communications. Details on the terms of the Processing are provided in **Appendix III.**

6.2.2 Obligations of the Client

By allowing High Connexion and/or its partners to conduct commercial prospecting based on the Personal Data collected by the Client on its website, application or by any other means, the Client acts as a joint controller. In this context, the Client undertakes to obtain the prior and informed consent of the Data Subjects, according to the applicable Regulations, to mention its privacy policy and to identify the partners concerned. The Customer undertakes to inform High Connexion of any request for the exercise of rights by Data Subjects that he/she receives in connection with this Processing, including the right to object to receiving marketing. The Client undertakes to retain the Personal Data for a limited duration corresponding to the purpose. At the expiry of this period, the Client undertakes to obtain consent for commercial prospecting again, under the same terms and conditions as previously. Upon request, the Client undertakes to provide High Connexion with all elements necessary to ensure and demonstrate compliance with its obligations (such as timestamp of actions taken and interactions of Data Subjects on the Client's website, application or any other support). In the event of a control by a regulatory Authority of High Connexion concerning all or part of the processing associated with personalization, the Client undertakes to actively cooperate with High Connexion and, if applicable, with this Authority as soon as the Client holds the information, evidence or documents useful 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, alteration, unauthorised disclosure of or access to Personal Data held or processed, including all necessary measures to ensure compliance with the security requirements of Personal Data in the Data Protection Regulation. In case of inadequacy between the security measures implemented and the Processing and/or Personal Data entrusted to High Connexion, the latter will inform the Client thereof and propose a remediation plan within a reasonable timeframe;
- limit access to Personal Data only to persons acting under its authority, and only to Personal Data strictly necessary for the performance of the Services subject to the Processing provided for in this Agreement;
- ensure that its computer systems are:
  - sufficiently protected inter alia against viruses and interception of Personal Data within the network;
  - in the ability to restore the availability of and access to Personal Data within the appropriate timeframes in case of a physical or technical incident.

8. VIOLATION OF PERSONAL DATA

In the event of an actual or potential Personal Data Breach affecting the Services of High Connexion or a subsequent Subcontractor, High Connexion undertakes to:

- notify the Client of any security breach that may lead to a Personal Data Breach as soon as possible, and at the latest within a maximum period of forty-eight (48) hours following knowledge of said breach by email;
- accompany the notification with any useful documentation in order to allow the Client, if necessary, to proceed with a notification of this violation to the Regulatory Authority or the Data Subject. As such, High Connexion will specify to the extent possible the following points:
  - a description of the nature of the Personal Data Breach including, if possible, the categories and approximate number of Data Subjects concerned by the breach and the categories and approximate number of records of Personal Data concerned;
  - the name and contact details of the Data Protection Officer and/or another contact point from which additional information can be obtained;
  - the 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 appropriate, measures to mitigate any adverse consequences.
- communicate the information defined above in a staggered manner and without undue delay in case it is not possible for High Connexion to provide all the specified information at the same time, or if clarifications can be provided on certain elements already communicated.

When the Parties act as joint Data Controllers, the Party concerned shall notify the other Party within 24 hours of becoming aware of it to allow for a joint notification by the Parties to the Regulatory Authority and, if applicable, the communication to the 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 logic of accountability, to:

- regularly maintain the register of Processing activities as provided for in Article 30(2) of the GDPR, and keep a written record of any Processing and Instructions relating to the Processing carried out on behalf of the Client;
- regularly maintain the security breach register which is completed by the Parties as soon as a Personal Data Breach occurs, whether or not this breach has been notified to the Regulatory Authority;
- keep the documentation relating to the training or awareness of employees regarding the protection of Personal Data;
- document, as far as possible, all the processes implemented in terms of protection of Personal Data through its Security Measures;
- regularly update the Security Measures.

10. RECIPIENTS OF PERSONAL DATA – USE OF SUBCONTRACTING

In addition to the provisions set out above, High Connexion and the Client may use one or more Sub-processors(s) to carry out specific processing activities in accordance with the Purposes defined for the Processing in the Annex. In this case, the Parties undertake and ensure that these selected Subcontractors provide sufficient guarantees to comply with the Data Protection Regulations. If the Subsequent Subcontractor(s) do not comply with their obligations regarding the protection of Personal Data, the Party having selected a subcontractor remains solely responsible for these failures. In the event that the Subcontractor is jointly selected by the Parties, responsibility for any breach by this subcontractor of its obligations regarding the protection of Personal Data shall be shared.

11. PEOPLE CONCERNED

High Connexion, when acting as a Subcontractor, commits to the Client, as part of a request to exercise rights, to:

- notify the Client, by email to the email address indicated by the Client in the Annexes, immediately and within a maximum period of five (5) working days of any request by a Data Subject wishing to exercise their rights under the Data Protection Regulation (in particular, requests for access, rectification, erasure and portability of Data and requests to object to Processing);
- cooperate fully with the Client in order to respond, within reasonable time limits given their nature and number, to requests from Data Subjects wishing to exercise their rights under the Data Protection Regulation, as soon as the Client does not have all the elements in their possession allowing them to manage these requests for the exercise of rights; and
- not disclose to the Data Subject, including Personal Data, without having first consulted and obtained the written consent of the Client.

It is the responsibility of the Party acting as Data Controller to provide information to Data Subjects concerned by Processing operations at the time of collection of Personal Data. In the event that both Parties act as joint Data Controllers, it is the

Client's responsibility to provide information to the Persons concerned by the Processing operations and provided for by articles 13 et seq. of the GDPR at the time of collecting Personal Data. The Client undertakes in particular that the consent of the Data Subjects, when required, is collected in accordance with the provisions of the GDPR, i.e. a manifestation of free, specific, informed and unequivocal consent by which the Data Subject accepts, by a statement or by a clear positive act the processing of his personal data. In particular, the Client undertakes to inform the Data Subjects that the Data transmitted to High Connexion may be transmitted to partners (mentioning them). The Client undertakes to provide High Connexion at first request, proof of the consents collected in connection with the Personal Data transmitted in this context. The Parties agree that the Data Subjects may exercise their rights with the Client, 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 period of five (5) business days of any request from a Data Subject wishing to exercise their rights under the Data Protection Regulation. The joint Controllers shall assist each other in responding to such requests for the exercise of rights by Data Subjects.

12. TRANSFERS TO THIRD COUNTRIES

In the event that it acts as a processor, High Connexion does not transfer any personal data to third countries without the prior written consent of the Client. High Connexion complies with the Instructions issued by the Client regarding transfers of Data to Third Countries, except in the event that High Connexion is required, in accordance with applicable laws, to transfer Personal Data to a Third Country. The Customer consents by the Agreement to the transfer of Personal Data to the entities and locations mentioned in the Annexes, for the strict purpose of performing the Services, and provided that:

- the Third Country is a country which, according to the European Commission, justifies an adequate level of protection of Personal Data; or
- High Connexion meets one of the following conditions:
  - High Connexion concludes or obtains from the entity identified in the Annexes an agreement on the transfer of data incorporating the model Standard Contractual Clauses developed by the European Commission;
  - The 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 ensures that no further transfer of Personal Data to another Third Country takes place unless the Customer gives its consent prior to such transfer, or unless such further transfer meets the requirements set out above.

13. RESPONSIBILITY

When acting as a Subcontractor, High Connexion agrees to indemnify the Customer for all direct material and immaterial damages suffered by him and originating from a defect or negligence on the part of High Connexion, its employees, representatives, agents or Subcontractorssubsequent 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 will therefore be liable for damages related to a security failure attributable exclusively to High Connexion resulting in unavailability, a loss of traceability, a doubt about the integrity or a 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. It can also not be held responsible for damages related to a security failure that could be attributable to the technological, software or IT choices made by the Client, notably for reasons of budgetary restrictions, whereas High Connexion will have proposed other solutions ensuring a higher level of security and guarantees. The liability of High Connexion 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 subsequent employees, representatives, agents or Subcontractors, the authorized Recipients) may only be engaged within one (1) year from knowledge of the damage. Where the Parties act as joint Controllers, each Party shall indemnify the other against all actions, complaint, claim made by Data Subjects or the Regulatory Authority concerning Personal Data subject to Processing that originates from non-compliance with the GDPR and/or the Agreement, and depending on each Party's own obligations. In this case, the defaulting Party shall ensure the defence of the other Party and shall bear the costs of advice and any damages that may be ordered against the latter by a court decision based on a breach of the provisions of the GDPR.

14. CONFIDENTIALITY

For the purposes hereof, "Confidential Data(s)" shall mean any data, information or documents disclosed by the Parties, in writing or orally, meeting the requirements of this article, and including without limitation any written or printed documents, any samples, models, data communicated by or resulting from either of the Parties, or more generally any means of disclosure of Confidential Data. Shall be governed by the provisions of these Terms and Conditions, information or documents in whatever form, transmitted by a Party and designated as Confidential Data by affixing or adding to their medium a stamp or form or by the establishment and delivery or sending of a written notification to that effect, or when they are disclosed orally, of which the character of Confidential Data has been brought to the attention of the Parties, at the time of their disclosure, the confidentiality also applies to Data that by nature are confidential, regardless of such a mention. The Parties undertake during the term of the Contract, and for a period of ten (10) years from its expiration for any reason whatsoever, that all Data (including information, documents, know-how, methods, of any kind whatsoever) which will have been exchanged within the framework of the Contract and this Agreement:

- are protected and kept strictly confidential and are treated with the same degree of care and protection as they give to their own Confidential Data of equal importance;
- are disclosed internally only to the members of their respective staff who have to know them and are used by them only for the purpose defined herein;
- are not used, in whole or in part, for any purpose other than that defined herein, unless prior written consent of the other Party;
- are not disclosed or likely to be disclosed, either directly or indirectly to any third party or persons other than those mentioned in sub-paragraph (ii) above;
- are not copied, reproduced or duplicated in whole or in part when such copies, reproductions or duplications could harm the interests of the other Party.

All the Data, information and their reproductions, transmitted by the Parties, will remain their property and must be returned to the other Party immediately upon request. On the other hand, the Parties will have no obligation and will not be subject to any restriction with regard to all the Confidential Data of which they can provide proof:

- that they have voluntarily entered the public domain before or after their disclosure but in this case in the absence of any fault attributable to them; or
- that they are already known by the other Party, this knowledge being demonstrated by the existence of appropriate documents in their files; or
- that they have been received from a third party in a lawful manner, without restriction or violation of these presents; or
- that they have been published without contravening the provisions of these present; or
- that the use or disclosure has been authorized in writing by the other Party; or
- that they have not been designated or confirmed as Confidential Data.

The termination or termination of this document shall not have the effect of relieving the Parties from their obligations to comply with the provisions of this article regarding the use and protection of information received before the date of termination or the expiration of the term. 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, consultants, 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 Client may carry out audits on documents to ensure the level of compliance of High Connexion. Confidential elements entrusted to High Connexion by other clients are not concerned by the audit on documents. The Client may also carry out objective audits of compliance with the Data Protection Regulation 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 Client for their expertise, independence and impartiality;
- the selected auditor is bound to the Parties by a confidentiality agreement and/or professional secrecy;
- the Client notifies, in writing and subject to a minimum of ten (10) working days' notice, High Connexion of its intention to have a compliance audit carried out;
- in no way, the audit carried out may deteriorate or slow down the Services offered by High Connexion or undermine the organizational management of High Connexion. Audit operations shall not involve actions that could potentially damage the infrastructure of High Connexion or interfere with other services provided by High Connexion to other clients;
- a copy of the identical audit report is given to the Client as well as to High Connexion following the completion of the audit mission and for which observations can be made by the Parties. This report may, where appropriate, be the subject of an in-depth review within the framework of a steering committee;
- the costs of the compliance audit will be borne exclusively by the Client;
- the Client may only order compliance audits within the limit of one (1) audit per year; and
- High Connexion will have a period of three (3) months from the communication of the audit report to correct at its expense the shortcomings and/or non-conformities found. Where applicable, High Connexion may exceptionally extend this period by three (3) months after having expressly informed the Client and objectively justified such extension.

High Connexion is committed to providing the selected auditor with access to its sites, facilities, documents and information necessary for the assessment of its good level of compliance, and cooperates fully with the selected auditor in the proper performance of his/her duties.

In the event of a control carried out by a competent regulatory authority that may be relevant to the Customer's Processing operations, High Connexion undertakes to fully cooperate with the regulatory authority. In the event of a control carried out by a competent regulatory authority with regard to the Client, High Connexion undertakes to fully assist the latter regarding the Processing carried out as part of the Services. All the Data collected under the Audits and Controls are considered as "Confidential Data" within the meaning of the article "Confidentiality" hereof.

16. APPLICABLE LAW AND COMPETENT JURISDICTION

The Agreement shall be governed by and construed in accordance with French law and any dispute arising out of or in connection with the Agreement as to its validity,

interpretation or further performance shall be subject to the exclusive jurisdiction of the Tribunal de commerce de Paris, as well as to the National Commission on Computing and Freedoms (Cnil) to which each of the Parties irrevocably submits. Before any contentious action, the Parties shall seek, in good faith, to settle amicably their disputes relating to the validity, interpretation, performance, non-performance, interruption, the termination or denunciation of this Agreement as well as the partial or total cessation of commercial relations between the Parties, for any reason and on any basis whatsoever. The Parties shall meet in order to compare their points of view and make any useful findings 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 from the notification by one of them of the need for an amicable agreement, by registered letter with acknowledgment of receipt.

ANNEX 1 ON TERMS OF PERSONAL DATA PROCESSING

I. High Connexion as a Data Controller

I.a) Personal data of the Client processed by High Connexion on the platforms of High Connexion for the implementation and realization of the Services

Controller	High Connexion
Subcontractor	The Client
Subsequent subcontractor	TH2, SFR,
Data hosting	The Data is hosted at TH2 located in Paris or at SFR in Venissieux
Purpose of the Processing	Management of access by the Client (Users and Administrators) to the High Connexion platforms and allow the proper performance of the Services by High Connexion for the benefit of the Client
Personal data processed	• Identification data of administrators and users of the High Connexion platforms: Title, last name, first name, email, function, status, phone • Login data: login and password, registration date, last login, action histories on the platform, account closure • Cookies and trackers: functional and analytical
Legal basis of the processing	• Contractual basis (Contract for the provision of Services) • Consent of individuals (for the opt-in newsletter if applicable) • Legitimate interest (to prevent fraud and for statistical purposes and to improve the Services) • Legal obligation (request from administrations or institutions)
Categories of data subjects	Users and Administrators of the High Connexion platforms, Client's employees or persons authorized by the Client (mandated agencies)
Source of Personal Data	Registration of people on the High Connexion platforms (hosted environment)
Information and management of people's rights	People are informed of their rights on the High Connexion platforms (privacy policy) and can exercise their rights with dpo@highconnexion.com by specifying "*High Connexion Platform"*
Non-EU data flows	None
Data retention period	The personal data will be kept for the duration of the contractual relationship with the Client and for 5 years after the end of this relationship. The logs are kept between 6 months and 1 year. Cookies and trackers are kept for a maximum of 25 months.

I.b) Personal data of the Customer processed by High Connexion for the purpose of managing the business relationship with the customer

Controller	High Connexion
Subcontractor	The Client
Data hosting	The Data is hosted at TH2 located in Paris or at SFR in Venissieux
Purpose of the Processing	Management of the commercial relationship with the Client, including sending quotes, invoices
Personal data processed	Identification data of the Client's employees: Title, last name, first name, email, function, address, phone
Legal basis of the processing	• Contractual basis (Contract for the provision of Services) • Legitimate interest (to avoid fraud to improve the Services) • Legal obligation (request from administrations or institutions)
Categories of data subjects	Employees of the Client or any person mandated by the Client
Source of Personal Data	Documents and commercial exchanges
Information and management of people's rights	People are informed of their rights in the Contract and can exercise their rights withdpo@highconnexion.com
Non-EU data flows	None
Data retention period	The personal data will be kept for the duration of the contractual relationship with the Client and for 5 years after the end of this relationship.

II. High Connection as a Subcontractor

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

II. a) Personal data of the persons concerned processed by High Connexion in the name and on behalf of the Client in the context of the implementation of the Solutions (technical solutions such as game implementation, pass wallet, etc.)

Controller	The Client
Subcontractor	High Connexion
Subsequent subcontractors	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 wallet pass Google for the "Verified SMS" option
Purpose of the Processing	Implementation and management of promotional, marketing or payment technical solutions (billing) on behalf of the Client: ● For marketing services: ○ Messaging (sending SMS, email, voice messages, push notification, MMS, instant messaging, enriched SMS...), ○ Provision of digital solutions (distribution of content on the wallet, SMS game, Web & mobile and audiotel), ● For billing services: management of financial transactions for the person concerned who makes a payment on an operator invoice or via any other payment channel for: ○ the purchase of digital content (music, videos, press articles, ticketing, etc.) ○ for donation campaigns (one-time or recurring) ○ participate in SMS+, SVA+ or Internet+games
Personal data processed	● Identification data: last name, first name, email, phone number, etc. ● Connection data: ID pass, log management, download date, last interaction date, history of links clicked on the wallet, history of offers, etc. ● Transaction data: purchase, amount, payment method, etc. ● Cookies and trackers
Legal basis of the processing	● Contract: acceptance of the conditions of the offer (CGU, game rules, Client's policies, etc.) ● Legitimate interest (to prevent fraud and improve the Services) ● Legal obligation (request from administrations or institutions)
Categories of data subjects	Consumers (client or prospect of the Client) wishing to benefit from the offers or content put in place by the Client
Source of Personal Data	● Collection via a form (desktop or mobile) or ● Data provided by the Client or ● Data collected during the purchase of content, donations or games
Information and management of people's rights	Information in the Client's privacy policy Exercise of rights with the Client
Non-EU data flows	None
Data retention period	The personal data are kept for 1 year from the date of processing by High Connexion. Cookies and tracers are kept for a maximum of 25 months.

II. b) Personal data of consumers processed by High Connexion in the name and on behalf of the Client for commercial prospecting purposes

Controller	*The Client*
Subcontractor	*High Connexion*
Subsequent subcontractors	*N/A*
Data hosting	*The Data is hosted at TH2 located in Paris or at SFR in Venissieux*
Recipients	*Partners of the Client*
Purpose of the Processing	*Commercial prospecting on behalf of the Client and/or its partners*
Personal data processed	● *Identification data: civility, last name, first name, email, city, postal code* ● *Log and connection data: date and tracking of connections* ● *Présence du pass (ID pass)* ● *Consents and opt-in* ● *Cookies and trackers*
Legal basis of the processing	*Consent of individuals (via the opt-in newsletter and/or partner); this consent is collected in a free, specific, informed, and univocal manner*
Categories of data subjects	*Consumers wishing to receive information or commercial offers from the Client and/or its partners*
Source of Personal Data	*Opt-in case (not pre-checked) during collection (desktop or mobile)*
Information and management of people's rights	*Information in the privacy policy* *Exercise of rights with the Client*
Non-EU data flows	*None*
Data retention period	*Personal data is kept for 12 months from the date of consent (unless consent is withdrawn, which may be at any time)* *Cookies and tracers are kept for a maximum of 25 months.*

III. High Connexion as a joint Data Controller

III. a) Location of personal data from High Connexion to the Client

Controller	High Connexion The Client
Purpose of the Processing	Enrichment and/or deduplication and/or analysis of the Client's databases for commercial prospecting purposes via sending commercial offers, in particular
Personal data processed	• Identification data: last name, first name, phone number, email, etc. • Cookies and trackers: token, etc.
Legal basis of the processing	Consent (opt in)
Categories of data subjects	People who have agreed beforehand to receive offers from identified partners (qualified opt-in)
Source of Personal Data	• Enriched databases of High Connexion or • Databases leased from third party partners
Information and management of people's rights	• *(for reminder: right to direct information of Data Subjects under Article 13 of the GDPR:* ○ *Information by High Connexion clients (who feed the High Connexion database)* ○ *Information by third parties from whom High Connexion rents the databases)* • Right of indirect information to be carried out by the Client (article 14 of the GDPR) • Exercise of rights with the Client, High Connexion being able to collaborate
Non-EU data flows	None
Data retention period	3 years max from the last action of the person Withdrawal of consent at any time upon request by the person

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

Joint Processors	• *The Client* • *High Connexion*
Recipients	*Partners*
Purpose of the Processing	*Enrichment and rental of data to third party partners in order to allow them to send commercial offers (generate leads) to people who have agreed to receive such offers (opt-in)*
Personal data processed	• *Identification data: civility, last name, first name, email, city, postal code* • *Log and connection data: date and tracking of connections* • *Consents and opt-in* • *Cookies and trackers*
Legal basis of the processing	• *Consent: clear, free, specific opt-in not pre-checked* • *Legitimate interest (to prevent fraud and improve the Services)* • *Legal obligation (request from administrations or institutions)*
Categories of data subjects	*Clients and prospects of the Client wishing to benefit from offers from partners*
Source of Personal Data	• *Collection via an opt-in or* • *Client File*
Information and management of people's rights	• *Right of information to be provided by the Client* • *Exercise of rights with the Client, High Connexion being able to collaborate*
Non-EU data flows	*None*
Data retention period	*The personal data are kept for 1 year from the end of the reimbursement operation. Cookies and tracers are kept for a maximum of 25 months.*

ANNEX 2
OF THE AGREEMENT ON THE PROTECTION OF PERSONAL DATA
Applicable from 01/06/2021

According to the general terms and conditions, the parties undertake to comply with the provisions of the Personal Data Processing Agreement available at: https://www.highconnexion.com/wp-content/uploads/DPA_HighConnon.pdf.

This sheet is part of this agreement, entered into between the client and High Connexion, as part of the service linking High Connexion and the client. It allows the sharing of the contact details of the DPOs necessary for the contractual framework.

It is valid between the Parties for all operations implemented as of this day. **Any modification must be reported in writing to** dpo@highconnexion.com

1. THE CONTROLLER

We kindly ask you to complete the table below with the highlighted elements in yellow with the information you have at the date hereof:

Controller	Company name: _____ (above named "Client") registered under the RCS number _____ registered at _____
Contact details of the DPO	Name : _____ First name : _____ email : _____ Phone : _____

2. THE SUBCONTRACTOR:

Subcontractor	HIGH CONNEXION (registered under no. 502 539 794 RCS Lyon)
Contact DPO	For the Provider: HIGH CONNEXION has a DPO, Mallory Rabot (dpo@highconnexion.com)

3. SIGNATURE:

Done at	_____
The	_____

Company	_____	High Connexion
First name, Last name	_____	François COSPAIN
Function	_____	General Manager
Signature and stamp		