

Data processing agreement

BETWEEN

The controller, which has entered into an agreement with Payflip BV ("Main Agreement") regarding the provision by Payflip BV of (digital) services relating to flexible remuneration;

Hereinafter referred to as the "PROCESSING RESPONSIBILITY"

AND

Payflip BV, a company under Belgian law, with registered office at Edekestraat 44, 9800 Deinze, registered in the Crossroads Bank for Enterprises under company number **0746.748.857** and represented here by Maura Nachtergaele, in her capacity as director;

Hereinafter referred to as the "PROCESSOR"

The Controller and the Processor are referred to collectively as the "Parties" and individually as a "Party".

WHEREAS:

- A. The Controller is a company that, in its capacity as employer, is looking for a third party specialised in providing (digital) services around flexible remuneration.
- B. The Parties have concluded a Main Agreement concerning the provision by the Processor of (digital) services in the context of flexible remuneration for employees of the Controller ("Services").
- C. The Parties wish to enter into an agreement as part of the Main Agreement, to regulate the processing of personal data (hereinafter "Agreement") in accordance with Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation").
- D. The Parties wish to set out in this Agreement the rights and obligations of both the Controller and the Processor.

THE FOLLOWING HAS BEEN AGREED

ARTICLE 1: DEFINITIONS

For the purposes of this Agreement, the following definitions shall apply:

- 1.1. "Agreement" has the meaning given to the term in preamble C;
- 1.2. "Confidential Information" means any information disclosed to the other Party in any written or tangible form under this Agreement, which is considered or could be considered confidential due to the nature of the data or the nature of the circumstances under which it is required to be disclosed. This includes, but is not limited to, product information, customer lists, price lists and financial information;
- 1.3. "Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data carried out under its supervision, and which is deemed to be the Controller for the purposes of this Agreement;
- 1.4. "Data Subject" means an identified or identifiable natural person;
- 1.5. "Employee" means a person recruited by an employer who has entered into an employment contract or is bound under an employment contract to provide employment services for a salary or fixed remuneration. An employee does not provide professional services as part of a self-employed activity. Agents, distributors, advisors, consultants, freelancers, (independent) (sub)contractors or other third parties shall not be considered Employees for the purposes of this Agreement;
- 1.6. "Personal Data" means any information relating to a Data Subject;
- 1.7. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- 1.8. "Processor" means a natural or legal person, public authority, agency or other body authorised to process personal data for the benefit of the Controller, such as the Processor;
- 1.9. "Security Measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or loss,

as well as unauthorised access, alteration or transfer;

- 1.10. "Services" means the services performed by the Processor in accordance with the Main Agreement and as explained in preamble B;
- 1.11. "Sub-processor" means any processor engaged by the Processor as a subcontractor who agrees to process Personal Data for and on behalf of the Controller in accordance with this Agreement;
- 1.12. "Supervisory Authority" means an independent public authority which is established by a Member State pursuant to Article 51 of the Regulation;
- 1.13. "Third Party" means any party that is not a Data Subject, Controller, Processor or Sub-processor under this Agreement, nor a person authorised to process Personal Data under the direct authority of the Controller or Processor;
- 1.14. "Substantial Sub-processor" means a Sub-processor that provides substantial services or infrastructure in respect of the Services, including a cloud provider and integrated software applications.

The meanings of all other terms used but not defined, correspond to those they have in the Main Agreement

ARTICLE 2: SUBJECT MATTER OF THE AGREEMENT

- 2.1 The Controller wishes to entrust the Processor with the processing of Personal Data. The Processor shall process the Personal Data on behalf of and for the account of the Controller. For the provision of the Services, the Controller is responsible for processing Personal Data and the Processor is a data processor.
- 2.2 The Processor shall provide the Services in accordance with the provisions of this Agreement.
- 2.3 Both Parties expressly undertake to comply with the provisions of the relevant applicable data protection legislation, and they will not engage in or abstain from any action that could potentially lead the other Party to violate relevant and applicable data protection legislation.
- 2.4 **Processing activities.** The processing carried out by the Processor on behalf of and for the account of the Controller relates to the Services provided by the Processor. The Processing Activities consist of:
 - digital services in the context of flexible remuneration
 - improvement of the Services of the Processor
- 2.5 **Categories of Personal Data.** The Personal Data processed are:
 - Personal identification data of the employee (such as first name, surname, address, email address, etc.)
 - Electronic identification data (such as cookies, IP address, etc.)
 - Financial data (such as past expenditure, invoicing data, bank account or other payment details)
 - Payroll data
- 2.6 **Data subjects.** The Data Subjects are Employees of the Controller.
- 2.7 **Purposes.** The Processor only uses the Personal Data to ensure proper performance of the Services, as part of the Main Agreement in accordance with the provisions of this Agreement.
- 2.8 The Processor may and shall only process the Personal Data mentioned in Article 2.5. Moreover, Personal Data shall only be processed in light of the purposes specified by the Parties in this article.
- 2.9 Both parties undertake to take appropriate measures to ensure that Personal Data is not used improperly or obtained by an unauthorised Third Party.

ARTICLE 3: DURATION OF PROCESSING

- 3.1 This agreement shall continue to apply as long as the Processor processes Personal Data on behalf of and for the account of the Controller as part of the Main Agreement. If the Main Agreement terminates, this Agreement also terminates.
- 3.2 In case of a breach of this Agreement or the applicable provisions of the Regulation, the Controller may instruct the Processor to stop processing the Personal Data immediately.
- 3.3 Upon termination of the Agreement or when the Personal Data is no longer relevant for the provision of the Services, the Processor shall anonymise and pseudonymise the Personal Data that was received or obtained during the provision of the Services, as far as it is feasible. It does so exclusively for the following internal purposes to further improve the Services provided by the Processor.

ARTICLE 4: INSTRUCTIONS OF THE CONTROLLER

- 4.1 The Processor shall process Personal Data only on the basis of the written instructions of the Controller and in any case

in accordance with the agreed Processing Activities outlined in Article 2.4 of this Agreement to provide the Services. The Processor shall not further process the Personal Data covered by this Agreement in a manner inconsistent with those instructions and with the provisions established in this Agreement.

- 4.2 The Controller may unilaterally make limited changes to the instructions. The Processor shall be consulted before significant changes are made to the instructions. Both parties must agree to any changes affecting the main provisions of the Agreement.
- 4.3 The Processor shall process the Personal Data in accordance with Article 4.1 of this Agreement, which includes the transfer of Personal Data to a third country or an international organisation, unless a provision of Union or Member State law applicable to the Processor mandates the processing, in which case the Processor shall notify the Controller of this legal obligation before proceeding with the processing, unless that law prohibits such notification for reasons of important public interest.

ARTICLE 5: ASSISTANCE TO THE CONTROLLER

5.1 Compliance with legislation. The Processor shall assist the Controller in enforcing the obligations under the Regulation, taking into account the nature of the processing and the information available to it.

5.2 Personal Data Breach. In the event of a Personal Data Breach relating to the subject matter of the processing of this Agreement, the Processor shall inform the Controller without unreasonable delay as soon as it becomes aware of a Personal Data Breach.

This notification shall include at least the following information:

- (a) The nature of the Personal Data Breach;
- (b) The categories of Personal Data to which the Breach relates;
- (c) The categories of Data Subjects concerned and, approximately, the number of Data Subjects concerned;
- (d) The categories of personal data records concerned and, approximately, their number;
- (e) The likely consequences of the Breach in relation to Personal Data;
- (f) The measures proposed or taken to address the Personal Data Breach, including, where appropriate, measures to mitigate any adverse effects thereof.

- 5.3 If the Processor uses a Sub-processor, the Processor shall require the Sub-processor to provide it with the same information if a Personal Data Breach occurs at the Sub-processor. The Processor shall immediately pass on the information received from the Sub-processor to the Controller.
- 5.4 The Processor and its Sub-processor(s) shall designate a person from their Employees who will serve as a single point of contact and who will be responsible for all communications between the Processor, the Sub-processor(s) and the Controller in the event of an incident that has led to or could lead to the accidental or unauthorised destruction or loss, unauthorised access, alteration or transfer of Personal Data processed on behalf of the Controller.
- 5.5 Only the Controller decides, at its discretion and in accordance with relevant and applicable data protection legislation, whether Data Subjects whose Personal Data are affected by a Personal Data Breach are informed. It is the responsibility of the Controller to notify the Supervisory Authority of a Personal Data Breach.
- 5.6 The Parties, and if applicable the Sub-processor(s), shall ensure that they cooperate in good faith to mitigate the potential adverse effects of a Personal Data Breach.
- 5.7 **Data protection impact assessment (DPIA).** In addition, the Processor shall assist the Controller when it carries out a Data Protection Impact Assessment in accordance with Article 35 of the Regulation. However, the Processor shall be free, at its discretion, to charge additional fees for the performance of these services. These costs are at all times proportional to the services provided.

ARTICLE 6: OBLIGATION TO PROVIDE INFORMATION

6.1 At any given time, upon the Controller's request (though the Controller must be granted a reasonable timeframe to fulfil the request), the Processor shall provide the Controller with all the information it requires and at least the information specified by the provisions of this clause:

- All relevant data on its own corporate structure as well as accurate and updated identification data on all entities of the Processor involved in the processing of Personal Data, including the location of their principal place of business;
- Without prejudice to what was agreed in Article 9, the aspects of the processing for which the services of the Sub-processor are used or intended to be used and the identification data of a Sub-processor including the location of its principal place of business. The Processor shall disclose to the Controller the agreement with the

Sub-processor(s) relating to or relevant to the processing of Personal Data, unless such agreement with the Sub-processor(s) contains Confidential Information, in which case it may remove such Confidential Information;

- Geographical data on processing locations, including backup capabilities and data destruction capabilities;
- The physical, organisational, technical and logical Security Measures taken by the Processor and its Sub-processor(s), as stipulated in Article 11 of this Agreement.

ARTICLE 7: OBLIGATIONS OF THE PROCESSOR

- 7.1 The Processor shall promptly or within a reasonable time (depending on the legal obligations stipulated in the Regulation) and properly address all reasonable requests from the Controller regarding the processing of Personal Data related to this Agreement.
- 7.2 The Processor assures that there are no obligations arising from applicable laws that would prevent it from fulfilling its obligations under this Agreement.
- 7.3 The Processor undertakes to process Personal Data only for the purpose of providing the Services and to fulfil the responsibilities of this Agreement in accordance with the written instructions of the Controller. If the Processor cannot comply with this requirement for any reason, it shall notify the Controller without delay.
- 7.4 The Processor shall notify the Controller without delay if it believes that an instruction of the Controller violates applicable data protection legislation.
- 7.5 The Processor assures that access to, inspection, processing and provision of Personal Data is only done in accordance with the principle of proportionality and the need-to-know principle (i.e. that data is only made available to those individuals who require the Personal Data to carry out the Services).
- 7.6 The Processor undertakes to provide Personal Data only to those Employees of the Controller who need the Personal Data to fulfil the obligations of this Agreement and shall ensure that the Employee concerned undertakes to maintain confidentiality or is bound by a legal duty of confidentiality, unless such provision is provided for under the Main Agreement.
- 7.7 As of 25 May 2018, the Processor is required to establish and maintain a register of the processing activities related to this Agreement; the Processor shall make the register available upon first request to the Controller, an auditor appointed by the Controller and/or the Supervisory Authority.

ARTICLE 8: OBLIGATIONS OF THE CONTROLLER

- 8.1 The Controller shall provide all necessary assistance to the Processor and cooperate with it in good faith to ensure that any processing of Personal Data complies with the requirements of the Regulation, in particular the principles relating to the processing of Personal Data.
- 8.2 The Controller shall agree appropriate communication channels with the Processor to ensure that instructions, guidelines and other communications relating to Personal Data processed by the Processor on behalf of the Controller are properly received by the Parties. The Controller shall notify the Processor of the identity of the person who is the Controller's single point of contact who the Processor should contact in application of this Article 8.2.
- 8.3 The Controller warrants that it will only issue instructions, guidelines or communications to the Processor that comply with the provisions of the Regulation.
- 8.4 Without prejudice to Article 14.2 of this Agreement, the Controller shall provide the necessary assistance to the Processor and/or its Sub-processor(s) in order to comply with any request, order, investigation or summons addressed to the Processor or its Sub-processor(s) by a competent national governmental or judicial authority.
- 8.5 The Controller warrants that it will not issue any instructions, guidelines or requests to the Processor that would require the Processor and/or its Sub-processor(s) to breach obligations imposed by applicable mandatory national legislation applicable to the Processor and/or its Sub-processor(s).
- 8.6 The Controller assures that it will cooperate in good faith with the Processor to mitigate the adverse effects of a security incident affecting Personal Data processed on behalf of the Controller by the Processor and/or its Sub-processor(s).

ARTICLE 9: THE USE OF SUB-PROCESSORS

- 9.1 The Controller acknowledges and agrees that the Processor has engaged Sub-processors to assist in the provision of the Processor's Services. Through this Agreement, the Controller gives its general written consent to the Processor to work with (Substantial) Sub-processors. In the case of general written consent, the Processor shall inform the Controller of any intended changes regarding the addition or replacement of other Substantial

Sub-processors, giving the Controller the opportunity to object to such changes.

- 9.2 Without prejudice to the foregoing, the Parties agree that the Processor will not be required to disclose the identity of each Substantial Sub-processor (categories of Sub-processors in conjunction with the information stipulated in Articles 6 and 7 regarding Substantial Sub-processors will be sufficient). Notwithstanding the above, the Controller may at any time request the Processor to disclose the identity of a Sub-processor. The Processor shall do so if such disclosure does not violate any confidentiality clause or business secrecy clause concluded between the Processor and the relevant Substantial Sub-processor. If the Processor is not allowed to disclose the identity of a Substantial Sub-processor, the Processor will have to provide a formal written justification.
- 9.3 The Processor shall ensure that its (Substantial) Sub-processors are bound by the same obligations in relation to the Personal Data as those that bind the Processor under this Agreement.
- 9.4 The Processor shall correctly and promptly pass on the purposes defined and instructions provided by the Controller to the (Substantial) Sub-processor(s) whenever and wherever those purposes and instructions pertain to the part of the processing in which the (Substantial) Sub-processor(s) are involved.
- 9.5 As a part of this Agreement, the Processor uses the following categories of Substantial Sub-processors to ensure the performance of the Services to the Data Subjects.
- Databases
 - Cloud servers
 - Freelance consultants

ARTICLE 10: RIGHTS OF DATA SUBJECTS

- 10.1 Taking into account the nature of the processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, in fulfilling its duty to respond to requests for exercising the data subject's rights laid down in Chapter III of the Regulation;
- 10.2 The following stipulations shall be applicable to any requests from Data Subjects pertaining to their rights concerning the processing of their Personal Data by the Processor and/or its Sub-processors:
- The Processor shall make every possible effort to notify the Controller without delay of any request from a Data Subject pertaining to the Personal Data processed by the Processor and/or its Sub-processor(s) on behalf of the Controller. The Processor should not comply with such a request unless the Controller explicitly gives consent;
 - The Processor shall promptly comply with, and require its Sub-processor(s) to promptly comply with, any request from the Controller so as to enable the Controller to comply with a request from the Data Subject who wishes to exercise any of their rights;
 - The Processor shall ensure that both it and its Sub-processor(s) have the required technical and organisational capabilities to block access to Personal Data and physically destroy the data without any possibility of retrieval if and when the Controller makes such a request;
 - Upon a simple request from the Controller, based on best efforts, the Processor shall provide all necessary assistance and any required information that the Controller needs to defend its interests in any type of proceedings – be it judicial proceedings, arbitration or others – brought against the Controller or its Employee for infringing upon the fundamental rights to privacy and the protection of Personal Data of Data Subjects.

ARTICLE 11: SECURITY MEASURES

- 11.1 For the duration of this Agreement, the Processor shall implement and maintain appropriate technical and organisational measures in a manner that ensures that the processing meets the requirements of the Regulation and guarantees the protection of the Data Subject's rights.
- Among other things, the Processor shall implement technical and organisational measures against unauthorised or unlawful processing and regularly assess the adequacy of the Security Measures and adjust them if necessary.
- 11.2 More specifically, the Processor shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, according to Article 32 of the Regulation.
- 11.3 In assessing the appropriate level of security, particular consideration was given to the risks associated with processing, particularly those arising from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, Personal Data transmitted, stored

or otherwise processed.

- 11.4 The Controller reserves the right to suspend and/or terminate the Main Agreement if the Processor can no longer provide technical and organisational measures appropriate to the processing risk.
- 11.5 The Processor has implemented a variety of general physical, logical, technical, and organisational security measures, which include, but are not limited to, the following:
- Personal Data is stored in a secure Microsoft Azure infrastructure;
 - All databases are located in the Netherlands with a failover system (a system that takes over tasks when the other system fails) situated in Ireland, ensuring everything remains within the borders of the European Union;
 - Personal Data is encrypted and protected both when it is stored in the database (at rest) and during its transmission to the user (in transit);
 - Personal Data can only be accessed by the Data Controller and more specifically by the authorised staff of the Data Controller on a need-to-know principle (i.e., they can only access the data that is strictly necessary);
 - The platform uses 256-bit SSL for identification at login;
 - All API calls are authenticated by Microsoft's API management;
 - Only test code in a development environment without access to the data of the Controller;
 - The Processor Employee's hardware is secured by two-factor authentication;
 - Use of cloud-based storage solutions to reduce the risk of data theft;
 - An elaborate Data Protection Breach Notification Policy that is applied by all Employees of the Processor;
 - Employees will have limited access to the data of the Controller (only via the platform) and only after the written consent of the Controller;
 - Any activity of the Employees of the Processor on the account of the Controller is automatically tracked;
 - Upon termination of the Main Agreement, store the data of the Controller for a period of six months only.

ARTICLE 12: AUDIT

- 12.1 The Processor acknowledges that the Controller is under the supervision of one or more Supervisory Authorities. The Processor acknowledges that any relevant Supervisory Authority has the right to conduct an audit at any time, specifically during the Processor's normal business hours, for the duration of this Agreement in order to assess the Processor's compliance with the Regulation and the stipulations of this Agreement. The Processor shall provide the necessary cooperation.
- 12.2 The Processor shall appoint an independent auditor every two (2) years to conduct such an audit. The final results of such audit report (without confidential information) will be provided to the Controller upon first request. The cost of such an audit shall be borne by the Processor.
- 12.3 In addition to the Processor's audit obligation, the Controller is only permitted to conduct supplementary audits if it has legitimate reasons for doing so (such as a suspected undisclosed data breach, when the Controller itself is the subject of an audit, or if there is a serious suspicion of fraud).
- 12.4 Upon receiving a written request from the Controller, the Processor is required to grant access to an independent third party, a certified auditor, or an auditor appointed by the Controller or the relevant Supervisory Authority. This access includes the relevant parts of the Processor's records and all information and locations relevant to the Processor (including its agents, subsidiaries and subcontractors) to ascertain the Processor's compliance with the Regulation and the stipulations of this Agreement. At the request of the Processor, the parties involved shall enter into a confidentiality agreement.
- 12.5 The Controller shall take all appropriate measures to minimise any disruptions that the audit might pose to the Processor's daily operations or to the Services provided by the Processor.
- 12.6 If the Processor and the Controller agree on a material failure to comply with the Regulation and/or the Agreement, as evidenced by the audit, the Processor shall remedy such failure as soon as possible. The Parties may agree to establish a plan, including a timescale for its implementation, to remedy deficiencies identified during the audit.
- 12.7 The Controller shall bear the costs of any audit carried out within the meaning of this article. However, if the audit reveals that the Processor has manifestly failed to comply with the Regulation and/or the provisions of this Agreement, the Processor shall bear the cost of such audit.

ARTICLE 13: TRANSFER TO THIRD PARTIES

13.1 The transfer of Personal Data to Third Parties in any manner whatsoever is prohibited, unless it is mandated by law or the Processor has secured the explicit approval of the Controller for such action. If a legal obligation applies to the transfer to Third Parties of Personal Data covered by this Agreement, the Processor shall notify the Controller prior to the transfer.

ARTICLE 14: INTERNATIONAL TRANSFER

14.1 The Parties agree that Personal Data may only be transferred to and/or stored with the recipient outside the European Economic Area (EEA), in a country not covered by an adequacy decision adopted by the European Commission by way of exception, and only if it is necessary to fulfil the obligations of this Agreement. Such transfers shall be governed by the terms of a personal data transfer agreement containing standard contractual clauses as published in the European Commission Decision of 4 June 2021 (Decision 2021/914/EC) or by other mechanisms provided for by applicable data protection legislation.

14.2 Before the international transfer, the Processor shall inform the Controller of the special measures taken to ensure the protection of the Data Subject's Personal Data in accordance with the Regulation.

ARTICLE 15: CONDUCT IN RELATION TO NATIONAL PUBLIC BODIES AND JUDICIAL AUTHORITIES

15.1 The Processor shall notify the Controller immediately of any request, order, investigation or summons addressed to the Processor or its Sub-processor by any competent national governmental or judicial authority. This includes any communication involving the Personal Data processed by the Processor or a Sub-processor, or any data and/or information related to such processing undertaken by the Processor on behalf of the Controller.

15.2 Without prejudice to Article 15.1 of this Agreement, the Processor assures that there are no obligations of applicable law, which make it impossible for the Processor to fulfil its obligations under this Agreement.

ARTICLE 16: INTELLECTUAL PROPERTY RIGHTS

16.1 Nothing in this Agreement constitutes a transfer of Intellectual Property Rights, neither from the Controller to the Processor, nor vice versa, unless otherwise contractually agreed between the Parties.

ARTICLE 17: CONFIDENTIALITY

17.1 The Processor undertakes to keep the Personal Data and its processing extremely confidential. The Processor shall ensure confidentiality with measures no less restrictive than those it uses to protect its own confidential material, including Personal Data.

17.2 The Processor guarantees that Employees or Sub-processors authorised to process the Personal Data have undertaken to observe confidentiality or are bound by an appropriate legal obligation of confidentiality.

ARTICLE 18: LIABILITY

18.1 The Controller involved in the processing shall be liable for damages caused by any processing that violates the Regulation. Without prejudice to the Main Agreement, the Processor is only liable for damages resulting from processing if it has failed to comply with the obligations of the Regulation specifically intended for processors, or if it has acted outside or contrary to the lawful instructions of the Controller.

18.2 The Controller or the Processor shall be released from liability under section 18.1 if it proves that it is not in any way responsible for the event that caused the damages.

18.3 The Processor is liable for the payment of administrative fines based on a breach of the provisions of the Regulation. Under no circumstances will the Processor be liable if it proves that it is not responsible for the event that caused the damages.

18.4 In the event that both the Processor and the Controller are found to be responsible for the damages caused by the processing of Personal Data, both Parties shall bear the liability. Each Party shall pay damages in proportion to their individual share of responsibility for the damages caused by the processing.

18.5 In the event that both the Controller and the Processor are involved in the same processing operation and they are responsible under sections 18.1 and 18.4 for damages caused by the processing, both the Controller and the Processor shall be held liable for the total damages in order to ensure effective compensation of the Data Subject.

18.6 In the event that either the Controller or the Processor has paid full compensation for the damages suffered in accordance with section 18.5, the respective Controller or Processor shall be entitled

to reclaim from the other party the portion of the compensation corresponding to their share of the responsibility for the damages, in accordance with the terms of section 18.1 and/or in accordance with the limitation of liability as stipulated in this Article 18.

18.7 A Party shall be liable (either contractually or through unlawful actions (including non-performance) or in any manner related to this Agreement, including liability for gross negligence) for verified failures attributable to it. The liability of the Parties for any breach under this Agreement, shall be limited to suffered foreseeable, direct and personal damages, excluding consequential damages (even if informed of the possibility of such consequential damages or if the likelihood of such consequential damages was reasonably foreseeable), where "consequential damages" is understood to mean: damages that do not result directly and immediately from non-performance and/or extra-contractual non-performance, but instead indirectly and/or over time, including but not limited to loss of revenue, interruption or stagnation of business operations, increase in personnel costs and/or the costs of personnel reduction, damages consisting of or resulting from third-party claims, failure to achieve expected savings or benefits, and loss of data, profit, time or income, loss of orders, loss of customers, increase in overhead costs, consequences of a strike, regardless of the causes thereof.

18.8 In any event, the total liability of the Processor under this Agreement shall be limited to the cause of the damages and to an amount equivalent to the total sum of the fees that the Controller has paid to the Processor for the provision and performance of the Services for a period not exceeding twelve months immediately preceding the cause of the damages. Under no circumstances shall the Processor be held liable if the Processor can demonstrate that they are not responsible for the event or cause giving rise to the damages.

18.9 The Processor shall be liable for the (Substantial) Sub-processors it engages in accordance with the provisions of this article.

ARTICLE 19: MEDIATION AND JURISDICTION

19.1 The Processor agrees that in the event the Data Subject initiates a claim for damages under this Agreement, the Processor shall respect the decision made by the Data Subject:

- To refer the dispute to an independent person for mediation;
- To refer the dispute to the courts in Belgium.

19.2 The Parties agree that the Data Subject's choice does not affect its substantive or procedural rights to seek redress in accordance with other provisions of applicable national or international law.

19.3 Any dispute between the Parties concerning the terms of this Agreement shall be brought before the competent courts as stipulated in the Main Agreement.

ARTICLE 20: TERMINATION OF THE AGREEMENT

20.1 This Agreement shall continue to apply for as long as the Processor processes Personal Data on behalf of the Controller.

20.2 If a breach of this Agreement or the Regulation occurs, the Controller may instruct the Processor to stop processing the Personal Data immediately.

20.3 The Processor will not store the data longer than necessary to perform the Services for which the data is provided. At the discretion of the Controller, once the Services related to the processing have been completed, the Processor shall delete all Personal Data or return it to the Controller, delete all existing copies and declare that it has done so. This is unless the storage of the Personal Data is mandated by Union or Member State law; The Personal Data shall be provided to the Controller at no cost, unless otherwise agreed upon.