Data Processing Agreement

Pro-Controller

This Data Processing Agreement has been concluded on this day_____,

BETWEEN;

[●], a private limited liability company, duly incorporated and validly existing under the laws of _____, having its registered office and its principal place of business at [●], at [●] registered with the [●] trade register under number [●] ("Controller"); and

[●], a private limited liability company, duly incorporated and validly existing under the laws, having its registered office and its principal place of business at [●], at [●] registered with the [●] trade register under number [●] ("Processor").

Definitions

In this Agreement:

Applicable Law means:

(a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;

(b) the common law and laws of equity as applicable to the parties from time to time;

(c) any binding court order, judgment or decree;

(d) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

Complaint means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

Data Controller has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

Data Protection Laws means any Applicable Law relating to the processing, privacy, and use of Personal Data, as applicable to the Data Controller, the Data Processor and/or the Services, including:

(a) in member states of the European Union: the General Data Protection Regulation (EU) 2016/679 (GDPR), and once applicable, the Directive

2002/58/EC (ePrivacy Directive), and all relevant member state laws or regulations giving effect to or corresponding with any of them; and

(b) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority;

Data Protection Losses	means all liabilities and other amounts, including all: **(a)** costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); **(b)** loss or damage to reputation, brand or goodwill; **(c)** to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation paid to a Data Subject (including compensation to protect goodwill and ex gratia payments); (iii) costs of compliance with investigations by a Supervisory Authority; and **(d)** the costs of loading Data Controller Data, to the extent the same are lost, damaged or destroyed, and any loss or corruption of Data Controller Data (including the costs of rectification or restoration of Data Controller Data);
Data Subject	has the meaning given to that term in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
International Organisation	means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
International Recipient	has the meaning given to that term in clause 6.1;
Personal Data	has the meaning given to that term in Data Protection Laws;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;
processing	has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);

Processing Instructions	has the meaning given to that term in clause 2.1.1;
Protected Data	means Personal Data received from or on behalf of the Data Controller, or otherwise obtained in connection with the performance of the Data Processor's obligations under this Agreement; and
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

In this Agreement:

(a) references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including particularly the GDPR) and the equivalent terms defined in such Applicable Laws, once in force and applicable;

(b) a reference to a law includes all subordinate legislation made under that law; and

(c) clauses 1 to 10 (inclusive) shall survive termination (for any reason) or expiry of this Agreement (or of any of the Services).

1 Data Processor and Data Controller

1.1 The Data Processor shall comply with all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement and shall not by any act or omission cause the Data Controller (or any other person) to be in breach of any Data Protection Laws.

1.2 The Data Controller shall comply with all Data Protection Laws in respect of the performance of its obligations under this Agreement.

2 Instructions and details of processing

2.1 Insofar as the Data Processor processes Protected Data on behalf of the Data Controller, the Data Processor:

2.1.1 unless required to do otherwise by Applicable Law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Data Controller's documented instructions as set out in this clause 2 and the Schedule (Data Processing Details), and as updated from time to time by the written agreement of the parties (**Processing Instructions**); and

2.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Data Controller of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest).

2.2 The Data Processor shall immediately inform the Data Controller in writing if, in the Data Processor's opinion, a Processing Instruction infringes the Data Protection Laws or any other Applicable Laws relating to data protection and explain the reasons for its opinion, provided that this shall be without prejudice to clause 1.1.

3 Technical and organisational measures

3.1 The Data Processor shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Data Processor:

3.1.1 such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;

3.1.2 so as to ensure a level of security in respect of Protected Data processed by it that is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed; and

3.1.3 without prejudice to clause 5.1, insofar as is possible, to assist the Data Controller in the fulfilment of the Data Controller's obligations to respond to Data Subject Requests relating to Protected Data.

3.2 Without prejudice to clause 3.1, the Data Processor shall, in respect of the Protected Data processed by it under this Agreement comply with the requirements regarding security of processing set out in Data Protection Laws (as applicable to Data Processors) and in this Agreement.

4 Using staff and other processors

4.1 The Data Processor shall not engage another Data Processor (or any replacement) for carrying out any processing activities in respect of the Protected Data without the Data Controller's specific prior written consent.

4.2 The Data Processor shall ensure that the Data Processor Personnel and all other persons authorised by it, or by any person acting on its behalf (including by any Data Processor pursuant to clause 4.1), to process Protected Data are subject to a binding written contractual obligation with the Data Processor or with the Data Processor that has engaged them to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Data Processor shall, where practicable and not prohibited by Applicable Law, notify the Data Controller of any such requirement before such disclosure).

4.3 The Data Processor shall ensure that access to Protected Data is limited to the authorised persons who need access to it to supply the Services.

5 Assistance with the Data Controller's compliance and Data Subject rights

5.1 The Data Processor shall (at no cost to the Data Controller):

5.1.1 promptly record and then refer all Data Subject Requests it receives to the Data Controller within three [*3*] Business Days of receipt of the request;

5.1.2 provide such information and cooperation and take such action as the Data Controller reasonably requests in relation to each Data Subject Request, within the timescales reasonably required by the Data Controller; and

5.1.3 not respond to any Data Subject Request or Complaint without the Data Controller's prior written approval.

5.2 Without prejudice to clause 2.1, the Data Processor shall, at its cost and expense, provide such information, co-operation and other assistance to the Data Controller as the Data Controller reasonably requires (taking into account the nature of processing and the information available to the Data Processor) to ensure compliance with the Data Controller's obligations under Data Protection Laws.

6 International data transfers

6.1 The Data Processor shall not transfer any Protected Data to any country outside the European Economic Area (EEA) or to any International Organisation (an **International Recipient**) without the Data Controller's prior written consent.

6.2 If the processing carried out by the Data Processor includes the transfer of Personal Data to a country outside of the EEA which is not recognised by the European Commission to have an adequate level of protection in accordance with the Data Protection Laws, the Data Controller and the Data Processor shall enter into a supplementary agreement containing the Standard Contractual Clauses (SCC).

6.3 If and to the extent this Agreement and the SCC are inconsistent, the provisions of the SCC shall prevail.

7 Records, information and audit

7.1 The Data Processor shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Data Controller, containing such information as the Data Controller may reasonably require, including:

7.1.1 where applicable, details of transfers of Protected Data to an International Recipient; and

7.1.2 a general description of the technical and organisational security measures referred to in clause 3.1.

7.2 The Data Processor shall make available to the Data Controller on request in a timely manner (and in any event within three [*3*] Business Days):

7.2.1 copies of the records under clause 7.1; and

7.2.2 such other information as the Data Controller reasonably requires to demonstrate the Data Processor's and the Data Controller's compliance with their respective obligations under Data Protection Laws and this Agreement.

7.3 The Data Processor shall at no cost to the Data Controller:

7.3.1 allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller for the purpose of demonstrating compliance by the Data Processor and the Data Controller with their respective obligations under Data Protection Laws and under clauses 1 to 10 (inclusive); and

7.3.2 provide (and procure) reasonable access for the Data Controller or such other auditor (where practicable, during normal business hours) to:

(a) the facilities, equipment, premises and sites on which Protected Data and/or the records referred to in clause 7.1 are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Data Processor); and

(b) to the Data Processor Personnel,

provided that the Data Controller gives the Data Processor reasonable prior notice of such audit and/or inspection.

7.4 The Data Processor shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by the Data Controller and reported to the Data Processor that reveal a breach or potential breach by the Data Processor of its obligations under any of clauses 1 to 10 (inclusive).

7.5 If the Data Processor is in breach of its obligations under any of clauses 1 to 10 (inclusive), the Data Controller may suspend the transfer of Protected Data to the Data Processor until the breach is remedied.

7.6 The Data Controller shall be entitled to share any notification, details, records or information provided by or on behalf of the Data Processor under any of clauses 1 to 10 (inclusive) (including under clauses 7 or 8) with the Data Controller Group, its professional advisors and/or the Supervisory Authority.

8 Breach notification

8.1 In respect of any Personal Data Breach, the Data Processor shall:

8.1.1 notify the Data Controller of the Personal Data Breach without undue delay (but in no event later than twelve [*12*] hours after becoming aware of the Personal Data Breach); and

8.1.2 provide the Data Controller without undue delay (wherever possible, no later than twenty-four [*24*] hours after becoming aware of the Personal Data Breach) with such details as the Data Controller reasonably requires regarding:

(a) the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Protected Data records concerned;

(b) any investigations into such Personal Data Breach;

(c) the likely consequences of the Personal Data Breach; and

(d) any measures taken, or that the Data Processor recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if the Data Processor cannot provide all these details within the timeframes set out in this clause 8.1.2, it shall (before the end of such timeframes) provide the Data Controller with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the Data Controller regular updates on these matters.

8.2 The Data Processor shall promptly (and in any event within *two* (2) Business Days) inform the Data Controller if it receives a Complaint and provide the Data Controller with full details of such Complaint.

9 Deletion or return of Protected Data and copies

9.1 The Data Processor shall (and shall ensure that all persons acting on its behalf and all Data Processor Personnel shall) without delay (and in any event within fourteen [*14*] days), at the Data Controller's written request, either securely delete or securely return all the Protected Data to the Data Controller in such form as the Data Controller reasonably requests after the earlier of:

9.1.1 the end of the provision of the relevant Services related to processing of such Protected Data; or

9.1.2 once processing by the Data Processor of any Protected Data is no longer required for the purpose of the Data Processor's performance of its relevant obligations under this Agreement,

and securely delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Data Processor shall inform the Data Controller of any such requirement).

10 Liability and indemnities

10.1 The Data Processor shall indemnify and keep indemnified the Data Controller in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Data Controller or any member of the Data Controller Group arising from or in connection with:

10.1.1 any breach by the Data Processor of any of its obligations under clauses 1 to 9 (inclusive); or

10.1.2 the Data Processor (or any person acting on its behalf) acting outside or contrary to the lawful Processing Instructions of the Data Controller in respect of the processing of Protected Data.

10.2 This clause 10 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

10.2.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

10.2.2 that it does not affect the liability of either party to any Data Subject.

11 Conflicts

11.1 Unless otherwise expressly stated in this Agreement:

11.1.1 the Data Processor's obligations and the Data Controller's rights and remedies under clauses 1 to 10 (inclusive) are cumulative with, and additional to, any other provisions of this Agreement;

11.1.2 nothing in this Agreement relieves the Data Processor of any responsibilities or liabilities under any Data Protection Laws; and

11.1.3 clauses 1 to 10 (inclusive) shall prevail over any other provision of this Agreement in the event of any conflict.

12 Contact details

If you have any queries in relation to this Agreement please contact:

Information Security & Compliance Co-ordinator

Email address: privacy@controlunion.com

privacy@onepeterson.com

Postal address: Boompjes 270

3011 XZ

Rotterdam

The Netherlands

THE SCHEDULE
DATA PROCESSING DETAILS

1 **Subject-matter of processing**:

[*INSERT*]

2 **Duration of the processing:**

[*INSERT*]

3 **Nature and purpose of the processing:**

[*INSERT*]

4 **Type of Personal Data:**

[*INSERT*]

5 **Categories of Data Subjects:**

[*INSERT*]

6 **Processing Instructions:**

[*INSERT, including any specific security measures that are required to be taken, eg encryption*]

Thus agreed and signed by:

Data Controller

Undersigned by and on behalf of: _____

Name:_____

Title: _____

Date and place: _____

Signature: _____

Data Processor

Undersigned by and on behalf of: _____

Name:_____

Title: _____

Date and place: _____

Signature: _____