ImpactGo
Data Processing Agreement

Version 1.0 DRAFT

Published: 18 April 2024

Table of Contents

1. Standard Contractual Clauses 3
2. Preamble 4
3. The rights and obligations of the Data Controller 4
4. The Data Processor acts according to instructions 5
5. Confidentiality 5
6. Security of processing 5
7. Use of sub-processors 6
8. Transfer of data to third countries or international organisations 7
9. Assistance to the Data Controller 8
10. Notification of personal data breach 9
11. Erasure and return of data 10
12. Audit and inspection 10
13. The parties' agreement on other terms 10
14. Commencement and termination 11
15. Contact Details 11

Appendix A: Information about the processing 12

Appendix B: Instruction pertaining to the use of personal data 13

1. Standard Contractual Clauses

This Data Processing Agreement (”DPA”) and its Schedules and Annexes reflects the Parties’ agreement with respect to the provisions of Services as defined in the Terms and Conditions to which you agreed as a Customer (available at https://impactgo.uk/legal/service-terms-and-conditions/) or any separate written agreement which references this DPA (the “Principal Agreement”).

This DPA is supplemental to, forms part of, and is effective upon its incorporation into, the Principal Agreement by and between CM Russell Limited (“Data Processor”) and You (“Customer”).

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Customer (the Data Controller)

AND

CM Russell Limited (the Data Processor)

(each a “Party” and together, “Parties”)

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

If any terms and conditions contained herein are in conflict with the terms and conditions set forth in the Principal Agreement, the terms and conditions set forth in this DPA shall apply.

Unless specifically defined herein, all capitalised terms shall have the same meanings given to them in the Principal Agreement.

Terms used in this DPA but not defined herein or in the Principal Agreement shall have the meanings given to them in the Regulation (EU) 2016/679 of the European Parliament and of the Council (“GDPR”).

2. Preamble

2.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3. In the context of the provisions set out in the Principle Agreement, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

2.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5. Two appendices are attached to the Clauses and form an integral part of the Clauses.

2.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7. Appendix B contains the Data Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Data Processor and how audits of the Data Processor and any sub-processors are to be performed.

2.8. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.9. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the Data Controller

3.1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

3.2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The Data Controller shall be responsible, among others, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

4. The Data Processor acts according to instructions

4.1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and B. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1. The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2. The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the above mentioned confidentiality.

6. Security of processing

6.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. According to Article 32 GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

6.3. Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the Data Controller – mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall specify these additional measures to be implemented in Appendix B.

7. Use of sub-processors

7.1. The Customer generally agrees that Data Processor may engage sub-processors (as well as advisors, contractors, and auditors) to process Personal Data. The Customer authorises Data Processor to appoint (and permit each sub-processor appointed in accordance with this Section 7 to appoint) sub-processors in accordance with this Section 7 and any restrictions in the Principal Agreement.

7.2. Data Processor may continue to use those sub-processors already engaged by Data Processor as at the date of this DPA as listed on the sub-processor list available at https://impactgo.uk/legal/sub-processors/ (the "Sub-processors Page") and may update the Sub-processors Page to include new sub-processors engaged to deliver the Services from time to time.

7.3. Customer may object to the engagement of such new sub-processor by notifying Data Processor in writing within 14 (fourteen) days of Data Processor's posting of a new sub-processor on the sub-processors Page.

7.4. With respect to each sub-processor (which, for the purposes of this Section 7.4 includes new sub-processors engaged in accordance with Section 7.3), Data Processor shall ensure that the arrangement between Data Processor and the relevant sub-processor is governed by a written contract including terms that offer at least the same level of protection for Customer Personal data as those set out in this DPA and meet the requirements of Article 28(3) of the GDPR.

8. Transfer of data to third countries or international organisations

8.1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

8.2. In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the Clauses:

a. transfer personal data to a Data Controller or a Data Processor in a third country or in an international organisation

b. transfer the processing of personal data to a sub-processor in a third country

c. have the personal data processed in by the Data Processor in a third country

8.4. The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the Data Controller

9.1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject

c. the right of access by the data subject

d. the right to rectification

e. the right to erasure ('the right to be forgotten')

f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing

h. the right to data portability

i. the right to object

j. the right not to be subject to a decision based solely on automated processing, including profiling

9.2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.3., the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

a. The Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Information Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the Data Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the Data Controller's obligation to consult the competent supervisory authority, the Information Commissioner, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

9.3. The parties shall define in Appendix B the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

10.1. In case of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

10.2. The Data Processor's notification to the Data Controller shall, if possible, take place within 24 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3. In accordance with Clause 9(2)(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the Data Controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4. The parties shall define in Appendix B all the elements to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

11.1. On termination of the provision of personal data processing services, the Data Processor shall be under obligation to delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

12.1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

12.2. Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and sub-processors are specified in Appendix B.

12.3. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or

prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

14.1. The Clauses shall become effective on the date of the Subscription Term as set out in the Principle Agreement.

14.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3. The Clauses shall apply for the duration of the provision of the Principle Agreement. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1. and Appendix B.4., the Clauses may be terminated by written notice by either party.

15. Contact Details

15.1. Please contact us at legal@impactgo.uk if You have any questions about this Data Processing Agreement, or our Services.

Appendix A: Information about the processing

A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

Delivery of Services as set out in the Principle Agreement.

A.2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

CM Russell Limited will process Personal Data as necessary to perform the Services under the Principal Agreement, as further specified in the applicable Order or Quotation, and as further instructed by the Customer in the use of the Services.

A.3. The processing includes the following types of personal data about data subjects:

Name, email address, telephone number, job title, company name, company address, company website address

A.4. Processing includes the following categories of data subject:

Customers of CM Russell Limited, their employees, clients, suppliers and other commercial partners, exclusively where such Personal Data is provided to CM Russell Limited for use of the Services under the terms of the Principle Agreement.

A.5. The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. Processing has the following duration:

For the duration of the Subscription Term as set out in the Principle Agreement.

Appendix B: Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

- for the purpose of granting the Customer access to, and use of, the Services as set out in the Principle Agreement; and
- for the purpose of auditing and monitoring Customer's use of the Services to ensure appropriate use under the terms of the Principle Agreement.

C.2. Security of processing

The level of security shall take into account:

- that the Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security; and
- that the Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller:
  - Personal Data is encrypted "at rest" and in transit throughout the Platform, and to/from the Platform
  - Daily data backups are maintained to support the timely restoration of data, in the event of a data loss incident
  - Backups are automatically deleted after not more than thirty (30) days from the time of creation
  - Customer access to, and use of, the Platform requires authenticated User Accounts and such User activity is recorded in an audit log
  - Data Processor access to, and use of, the Platform's database, infrastructure and sub-components will requires authenticated user accounts, secured with two-factor authentication and such user activity is recorded in an audit log

C.3. Assistance to the Data Controller

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- the Data Processor undertakes ongoing security monitoring of the Services, and will take reasonable steps to ensure the ongoing security of said Services;
- the Data Processor has undertaken a Data Impact Assessment of their processing operations, will periodically review and/update this, and make this available to the Data Controller if requested;
- the Data Processor will notify the Data Controller, without undue delay, in the event of a data breach, or suspected data breach, within the Services;
- the Data Processor will notify the Data Controller, without undue delay, when notified by any Sub-processor of a data breach, or suspected data breach, affecting the Services; and
- Data Subjects, or the Data Controller may contact legal@impactgo.uk with requests to exercise their rights under the GDPR, or rights under this agreement. Where practicable, the Data Processor will enact these requests without undue delay.

C.4. Storage period/erasure procedures

Personal data is stored for the duration of the Subscription Term as set out in the Principle Agreement after which the Personal Data is erased by the Data Processor.

Upon termination of the provision of personal data processing services, the Data Processor shall delete the personal data in accordance with Clause 11.1., unless the Data Controller – after the signature of the contract – has modified the Data Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

CM Russell Limited relies upon Digital Ocean to manage the physical access to their data centres, which are located in the United Kingdom.

CM Russell Limited does not maintain a dedicated physical office location where any processing or sub-processing will occur.

CM Russell Limited does not physically retain any data sets or processing functions outside of the core digital platform.

CM Russell Limited does not authorise or support the use of general access accounts or terminals, with all devices associated to a single individual.

C.6. Instruction on the transfer of personal data to third countries

If the Data Controller does not in the Clauses, or subsequently, provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the Data Controller's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance.