DATA PROCESSING AGREEMENT

(a) This Data Processing Agreement (hereinafter the "DPA") is an integral part of the SaaS agreement (the "Agreement") signed between Client, referenced in the Order Form that incorporates the Agreement, in the role as a controller, and dRofus AS and/or its Subsidiary/Subsidiaries (dRofus AS and the Subsidiaries are referred to as "dRofus"), in the role as a processor.

(b) The controller and the processor have entered the Agreement under which processor shall provide certain services as detailed in the Agreement to the controller (the "Services").

(c) Definitions;

a. "account data" means personal data that relates to Client's relationship with dRofus, including name and contact information of individuals authorized by Client to access Client's account, billing information associated with Client's account, authorization information (e.g., username, password, two-factor authentication), as well as system logs and user account activity collected by dRofus in the general operation of its products and services.

b. "controller" is defined in accordance with Data Protection Law, as applicable, and generally means the entity which determines the purposes and means of the processing of personal data.

c. "Client data" means personal data received from Client and processed by dRofus in its performance of the Services. Client data does not include account data.

d. "data protection law" means, to the extent applicable to the Services, any laws, regulations, and other legal requirements relating to data protection, data security or otherwise with respect to the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any personal data.

e. "personal data" is defined in accordance with data protection law, as applicable, and generally means any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

f. "processing" (and "process") is defined in accordance with data protection law, as applicable, and generally means the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any personal data.

g. "processor" is defined in accordance with data protection law, as applicable, and generally means the entity which processes personal data on behalf of a controller.

h. "dRofus Privacy Policy" means the publicly-posted dRofus Privacy Policy, which is currently posted at https://www.drofus.com/privacy-policy.

i. "special categories of data" is defined in accordance with data protection law, as applicable, and generally means personal data deemed particularly sensitive.

j. "sub-processor" is defined in accordance with data protection law, as applicable, and generally means any third-party processor engaged by a processor to process personal data on behalf of the processor.

k. "third party request" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

l. "Standard Contractual Clauses" or "SCCs" refers to the EU Standard Contractual Clauses attached hereto.

m. Any defined terms herein shall apply to similar nomenclature that may be used in data protection laws, as applicable.

(d) The parties acknowledge and agree that (i) dRofus is a controller with respect to account data, and (ii) dRofus is a processor with respect to Client data. Client has provided any required disclosures and received any required consents as may be necessary to provide personal data to dRofus pursuant to the Agreement and this DPA.

(e) In processing Client data subject to this DPA, dRofus shall:

a. Comply with data protection law and ensure any person processing the personal data hereunder is subject to a duty of confidentiality;

b. Not collect, use, retain, disclose or otherwise process personal data except: (i) pursuant to Client's documented instructions as provided by the Agreement; (ii) as necessary to perform the Services for the business purpose(s) specified in the Agreement; (iii) within the direct business relationship of the parties; (iv) to implement, operate or improve the Services, provided that the use does not include building or modifying data subject profiles for another entity or correcting, combining or augmenting data acquired from another source; (v) to detect security incidents or protect against malicious, deceptive, fraudulent or illegal activity; or (vi) as required by applicable law; and

c. Not sell or share personal data (except as authorized by Client), and not combine Client data with personal data that dRofus may receive from or on behalf of another person or entity or that dRofus collects from its own interaction with a data subject unless otherwise required by applicable law.

(f) dRofus shall notify Client without undue delay of any actual or reasonably suspected breach of Client data, including information reasonably required by Client (as it becomes available) so Client can comply with its obligations under data protection law.

(g) Client shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal data by dRofus. dRofus shall notify Client if it (or its sub-processors) can no longer meet obligations under data protection law.

(h) Where dRofus is a controller, it will provide data subjects with appropriate disclosures in the dRofus Privacy Policy, and offer those data subjects a means to exercise any privacy rights they are entitled to under data protection law. In the event any other third-party request is made directly to dRofus in connection with Client data, dRofus will endeavor to notify and refer the request to Client except to the extent prohibited by law, and will otherwise comply with applicable laws with respect to such request.

(i) dRofus will ensure that any affiliates or employees it authorizes to process Client data are subject to non-disclosure and confidentiality obligations consistent with dRofus' confidentiality obligations in the Agreement and this DPA.

(j) dRofus may engage sub-processors to process Client data on its behalf, but: (A) dRofus will restrict any sub-processors' access to Client data on a need-to-know basis and prohibit sub-processors from processing Client data for any other purpose; (B) dRofus will impose on such processors contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, and the obligation to comply with data protection law; and (C) dRofus will remain liable to Client for any breach of the Agreement or this DPA that is caused by an act, error, or omission of its Processors as if such breach is attributable to dRofus itself, subject to the terms on liability and indemnity under the Agreement.

(k) dRofus will reasonably cooperate with Client in connection with any data protection impact assessment or similar undertaking (at Client's expense if such cooperation will require dRofus to assign resources to that effort) or cooperation with regulatory authorities that may be required under data protection law.

(l) dRofus will delete or return to Client any Client data upon request, subject to any legal retention obligations. Client data stored in backup and disaster recovery repositories may be retained for a longer duration provided that it remains subject to this DPA until deleted.

(m) dRofus has implemented and will maintain technical and organizational security measures as set forth in the Agreement and this DPA.

(n) To the extent Client's use of the Services requires an onward transfer mechanism to lawfully transfer Client data from one jurisdiction to another, the following shall apply in accordance with the following order of precedence:

a. The Parties may expressly agree in writing (including via email) that a specified one-time transfer of Client data will be subject to a designated transfer mechanism (e.g., consent or another derogation);

b. The SCCs will apply to personal data that is transferred via the Services from the EEA/EU or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data;

c. The Parties agree that the SCCs, supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 and as amended or replaced thereafter ("UK Addendum") will apply to personal data that is transferred via the Services from the UK, either directly or via onward transfer, to any country or recipient outside of the UK that is not recognized by the competent UK regulatory authority or governmental body for the UK as providing an adequate level of protection for personal data. For data transfers from the UK that are subject to the UK Addendum, the UK Addendum is hereby entered into, incorporated by reference in this DPA, and completed as follows: (1) In Table 1, the Parties' details and key contact information is located in the Agreement and this DPA; (2) In Table 2, information about the version of applicable standard contractual clauses is provided in the SCCs attached hereto; (3) In Table 3, the list of parties is located in the Agreement and this DPA, and the description of the transfer and applicable security measures are addressed in annexes to the SCCs; and (4) In Table 4, both the importer and the exporter may end the UK Addendum in accordance with its terms; and

d. Except as otherwise addressed under the DPA, any jurisdiction requiring an onward transfer mechanism that is not expressly provided for under this DPA or the Agreement shall be subject to the SCCs, except that the governing law shall be the law of such jurisdiction, and the competent authority(ies) shall be the designated entities for such jurisdiction.

(o) To the extent there is any conflict or inconsistency between the (i) SCCs or UK Addendum and (ii) any other terms in the Agreement or this DPA, the provisions of the SCCs or UK Addendum, as applicable, will prevail. Notwithstanding the foregoing, any liability or indemnity claims brought in connection with this DPA (with the SCCs and UK Addendum) will be subject to the limitations of liability and other liability and indemnity terms and disclaimers set forth in the Agreement except to the extent prohibited by applicable law.

Standard Contractual Clauses (SCCs)

16 SECTION I

16.1 Clause 1

16.1.1 *Purpose and scope*

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with applicable data protection law, including Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) and/or Article 28(3) and (4) the UK GDPR (as defined in section 3(1) of the United Kingdom's Data Protection Act 2018) (the "UK GDPR").

(b) The controllers and processors listed in Annex I have agreed to these Clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 / the UK GDPR, and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679, the UK GDPR, and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679, the UK GDPR, and/or Regulation (EU) 2018/1725.

16.2 Clause 2

16.2.1 *Invariability of the Clauses*

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

16.3 Clause 3

16.3.1 *Interpretation*

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, the UK GDPR, or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679, the UK GDPR, or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / the UK GDPR / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

16.4 Clause 4

16.4.1 *Hierarchy*

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

16.5 Clause 5

16.5.1 *Docking clause*

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

17 SECTION II – OBLIGATIONS OF THE PARTIES

17.1 Clause 6

17.1.1 *Description of processing(s)*

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

17.2 Clause7

17.2.1 *Obligations of the Parties*

17.2.1.1 7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law or UK law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / the UK GDPR / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions or UK data protection provisions.

17.2.1.2 7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

17.2.1.3 7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

17.2.1.4 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

17.2.1.5 7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

17.2.1.6 7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679, the UK GDPR, and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

17.2.1.7 7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list as set out in Annex IV. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a subprocessor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

17.2.1.8 7.8. International transfers

(a) *[EEA/EU/UK Clients:]* Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law or UK law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679, the UK GDPR or Regulation (EU) 2018/1725.

(b) *[EEA/EU Clients:]* The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

(c) *[UK Clients:]* The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the UK GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the UK GDPR by using either the international data transfer agreement ("IDTA") or the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (the "UK Addendum") adopted by the UK's Information Commissioner's Office in accordance with Section 119A of the Data Protection Act 2018 of the UK, provided the conditions for the use of the IDTA or the UK Addendum (as applicable) are met.

17.3 Clause 8

17.3.1 *Assistance to the controller*

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679 and the UK GDPR.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

17.4 Clause 9

17.4.1 *Notification of personal data breach*

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

17.4.1.1 9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/ the UL GDPR, shall be stated in the controller's notification, and must at least include:

(1) 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;

(2) the likely consequences of the personal data breach;

(3) 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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679/the UK GDPR, with the obligation to communicate without undue delay 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.

17.4.1.2 9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679/the UK GDPR.

18 SECTION III – FINAL PROVISIONS

18.1 Clause 10

18.1.1 *Non-compliance with the Clauses and termination*

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, the UK GDPR and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679, the UK GDPR and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679, the UK GDPR and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law or UK law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

18.2 Clause 11

18.2.1 *Commercial Terms*

18.2.1.1 11.1 Interpretation

In accordance with Clause 2 above, no portion of this Clause 11 shall be deemed to amend, contradict or modify any portion of Clauses 1 to 10 above. In the event of any conflict or inconsistency between any portion of Clauses 1 to 10 above and this Clause 11, the relevant portion of Clauses 1 to 10 above shall prevail.

11.2 Confidentiality

(a) Without prejudice to any confidentiality undertakings included in the Agreement, the processor shall use all reasonable efforts to keep and maintain all personal data confidential and not disclose such personal data to any third party, unless otherwise authorized in advance in writing by the controller or otherwise required by applicable law or where explicitly required by these Clauses or the Agreement.

(b) Subject to any confidentiality undertakings in the Agreement, the controller undertakes to keep any and all information that the controller may receive about the processor's security measures, routines, IT systems, its business, Clients, working methods or that is otherwise of confidential nature, strictly confidential and not disclose confidential information about the processor to any third party. The controller accepts that this confidentiality undertaking shall survive the termination of these Clauses.

11.3 Notification, information and documentation

(a) Where these Clauses require notification to be made or information to be provided to either Party, the notice shall be sent to the following e-mail addresses:

1. The controller:
   The email address that has been communicated by the controller in relation to the online subscription and electronic signature related to execution of the Agreement
2. The processor: support@drofus.com

(b) For the purposes of Clause 7.6 (c), in relation to the controller's decision of a review or an audit, the controller may additionally take into account any attestations or other similar documentation held by the processor.

(c) Without prejudice to section (a) above, for the purposes of Clause 7.7 section (a), the Parties agree that the processor shall inform the controller of any intended changes of the list of sub-processors by way of updating the list that is made available by the processor online cf. Annex IV to these Clauses.

11.4 Liability

(a) The Parties acknowledge and agree that neither Party shall have an obligation to indemnify the other Party for any administrative fines imposed by a supervisory authority, the Information Commissioner's Office, or a court under Applicable Data Protection Legislation.

(b) Any other liability for each of the Parties under these Clauses shall be limited in accordance with the cap agreed upon in the Agreement.

(c) For the purposes of section (a) above, each Party shall, upon request and to the extent reasonably practicable, provide information to the other Party which may be useful within the scope of a supervisory authority or the Information Commissioner's Office matter or a court proceeding relating to the subject matter of these Clauses.

11.5 Assignment

Neither the rights nor the obligations of either Party under these Clauses may be assigned in whole or in part without the prior written consent of the other Party, unless otherwise stated in these Clauses.

11.6 Waiver

Failure by either Party to exercise or enforce any right available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of the Party's rights under these Clauses.

11.7 Invalidity

If any term or provision of these Clauses is held by a court of competent jurisdiction to be illegal or unenforceable, in whole or part, the validity of the remaining provisions and of these Clauses and/or the Agreement shall remain unaffected. The same shall apply if these Clauses are incomplete.

11.8 Entire agreement

These Clauses form the entire agreement and understanding between the Parties with respect to its subject matter, and supersedes all prior discussions, agreements and understandings, of any kind, whether written or oral, between the Parties with respect to the subject matter of these Clauses.

11.9 No variation

No variation of these Clauses shall be valid or binding upon either Party unless it is made in writing and signed by a duly authorised representative of each Party.

11.10 Governing law and venue

These Clauses shall be governed and construed in accordance with the same laws as governing the Agreement, including with regard to agreed venue.

11.11 Dispute resolution

Any dispute arising out of or in connection with these Clauses shall be finally settled in accordance with the provisions regarding dispute resolution in the Agreement.

ANNEX I LIST OF PARTIES

Controller(s): The controller is the Client as referenced in the Order Form that incorporates the Agreement.

Processor(s): The processor is the designated dRofus legal entity referenced in the Order Form that incorporates this Agreement.

ANNEX II: DESCRIPTION OF THE PROCESSING

A complete description of the processing available at https://www.drofus.com/privacy-policy

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organisational measures implemented to secure the security of the data are set out in dRofus' Security and Data Protection Addendum made available at: https://support.drofus.com/support/solutions/articles/16000022255-security-and-data-protection

ANNEX IV: LIST OF SUB-PROCESSORS

A complete list of sub-processors is available at: https://www.drofus.com/subprocessors