

Annex 1 Data Protection

Valid from January 2024

A. General

- 1.1 This Annex 1 Data Protection (“**Annex 1**”) describes the obligations of the Parties with respect to the processing and security of the personal data concerned (as defined in each of the attached documents). Terms used and not defined in this Annex 1 shall have the meaning given to them in the reference data protection legislation.
- 1.2 This Annex 1 supersedes all previously applicable terms and conditions relating to the processing and security of personal data. The contents of the listed documentation may be changed or updated by Heidelberg from time to time as required. Such changes shall not alter the intent of this Annex.
- 1.3 The terms in each Appendix (overview in the table) to this Annex 1 apply only where the corresponding law applies to the processing of Customer personal data.

| Regions/Countries | Applicable Data Protection Regulation | Appendix |
|--|--|----------|
| Europe | | |
| <ul style="list-style-type: none"> • European Union (EU) and European Economic Area (EEA) | General Data Protection Regulation (GDPR) | 1 |
| <ul style="list-style-type: none"> • Switzerland | Federal Act on Data Protection (revFADP) | 2 |
| <ul style="list-style-type: none"> • United Kingdom | Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR) | 3 |
| America | | |
| <ul style="list-style-type: none"> • United States of America • - California | California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) | 4 |

Appendix No. 1 EU/EEA Data Processing Agreement ("DPA")

Preamble

The EU Commission published a DPA and named it Standard Contractual Clauses for controllers and processors located within the EU/EEA (https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en). The EU Commission deems that the standard contractual clauses as set out in the Annex fulfil the requirements for contracts between controllers and processors in Article 28(3) and (4) of Regulation (EU) 2016/679 and of Article 29(3) and (4) of Regulation (EU) 2018/1725 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale=en>).

1. Purpose and Scope

- 1.1 The purpose of these Standard Contractual Clauses ("Clauses") is to ensure compliance with 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 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).
- 1.2 These Clauses apply to the processing of personal data (available at <https://home.plus.heidelberg.com/#/legal/processings>).
- 1.3 These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- 1.4 These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2. Invariability of the Clauses

- 2.1 The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- 2.2 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.

3. Interpretation

- 3.1 Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- 3.2 These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- 3.3 These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. 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.

5. (Intentionally left blank)

6. 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 the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7. Obligations of the Parties

7.1 Instructions

The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State 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.

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

7.2 Purpose Limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>), unless it receives further instructions from the controller.

7.3 Duration of the Processing of Personal Data

Processing by the processor shall only take place for the duration specified in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7.4 Security of Processing

The processor shall at least implement the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) 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.

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.

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.

7.6 Documentation and Compliance

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

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

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 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.

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.

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.

7.7 Use of Sub-Processors

For purposes of this Clause 7.7, the processor has the controller's general authorisation for the engagement of sub-processors from an agreed list (available at <https://home.plus.heidelberg.com/#/legal/subprocessors>). 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 three weeks 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.

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.

At the controller's request, the processor shall provide a copy of such a sub-processor 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.

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.

The processor shall agree to 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.

7.8 International Transfers

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 to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

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 sub-processor 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.

8. Assistance to the Controller

8.1 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.

8.2 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 Clauses 8.1 and 8.2, the processor shall comply with the controller's instructions.

8.3 In addition to the processor's obligation to assist the controller pursuant to Clause 8.2, 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 by:

carrying 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;

consulting the competent supervisory authority/ies prior for 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;

ensuring 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;

complying with the obligations in Article 32 Regulation (EU) 2016/679.

8.4 The processor is required to assist the controller in the application of this Clause, including taking the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>).

9. 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.

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:

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);

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

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;

the likely consequences of the personal data breach;

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.

in complying, pursuant to Article 34 Regulation (EU) 2016/679, 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.

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

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

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 the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) 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.

10. Non-Compliance with the Clauses and Termination

10.1 Without prejudice to any provisions of Regulation (EU) 2016/679 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.

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

the processing of personal data by the processor has been suspended by the controller pursuant to Clause 10.1 and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

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

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 and/or Regulation (EU) 2018/1725.

10.3 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 7.1.2, the controller insists on compliance with the instructions.

10.4 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 requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Appendix No. 2 Swiss Data Processing Agreement ("DPA")

Preamble

The Parties aim to ensure that the Processor's processing of Personal Data complies with data protection regulations, as set out in the following Data Processing Agreement.

1. Purpose and Scope

- 1.1 The purpose of these Standard Contractual Clauses ("Clauses") is to ensure compliance with the Federal Act of 25 September 2020 on Data Protection (FADP) of the Federal Assembly of the Swiss Confederation with regard to the processing of personal data.
- 1.2 These Clauses apply to the processing of personal data (available at <https://home.plus.heidelberg.com/#/legal/processings>).
- 1.3 These Clauses are without prejudice to obligations to which the controller is subject to the Federal Act on Data Protection.
- 1.4 These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with the Section 2 and 3 of the Federal Act on Data Protection.

2. Invariability of the Clauses

- 2.1 The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- 2.2 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.

3. Interpretation

- 3.1 Where these Clauses use the terms defined in the Federal Act on Data Protection, or in Regulation (EU) 2016/679 or in Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that order therein defined.
- 3.2 These Clauses shall be read and interpreted in the light of the provisions of the Federal Act on Data Protection.
- 3.3 These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the Federal Act on Data Protection or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. 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.

5. (Intentionally left blank)

6. 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 the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7. Obligations of the Parties

7.1 Instructions

The processor shall process personal data only on documented instructions from the controller, unless required to do so by domestic 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.

The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the applicable data protection regulations.

7.2 Purpose Limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>), unless it receives further instructions from the controller.

7.3 Duration of the Processing of Personal Data

Processing by the processor shall only take place for the duration specified in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7.4 Security of Processing

The processor shall at least implement the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) 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.

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.

7.5 Sensitive Data

If the processing involves particularly sensitive personal data such as 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.

7.6 Documentation and Compliance

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

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

The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses. 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.

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.

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.

7.7 Use of Sub-Processors

For purposes of this Clause 7, the processor has the controller's general authorisation for the engagement of sub-processors from an agreed list (available at <https://home.plus.heidelberg.com/#/legal/subprocessors>). 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 three weeks 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.

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 applicable data protection regulations.

At the controller's request, the processor shall provide a copy of such a sub-processor 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.

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.

The processor shall agree to 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.

7.8 International Transfers

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 legal requirement to which the processor is subject and shall take place in compliance with the Section 3 of the Federal Act on Data Protection.

The controller agrees that where the processor engages a sub-processor in accordance with Clause 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 the Section 3 of the Federal Act on Data Protection, the processor and the sub-processor can ensure compliance by using standard contractual clauses adopted by the Federal Assembly of the Swiss

Confederation, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the Controller

8.1 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.

8.2 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 Clauses 8.1 and 8.2, the processor shall comply with the controller's instructions.

8.3 In addition to the processor's obligation to assist the controller pursuant to Clause 8.2, 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 by:

carrying 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;

where mandatory, consulting the competent supervisory authority/ies prior for 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;

ensuring 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;

complying with the obligations in Article 22 and 23 of the Federal Act on Data Protection.

8.4 The processor is required to assist the controller in the application of this Clause, including taking the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>).

9. 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 Article 24 of the Federal Act on Data Protection, where applicable, taking into account the nature of processing and the information available to the processor.

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:

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);

in obtaining the following information which, pursuant to Article 24 of the Federal Act on Data Protection, shall be stated in the controller's notification, and must at least include:

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;

the likely consequences of the personal data breach;
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, at least the nature of the data breach, its consequences and the measures taken or planned, and further information shall, as it becomes available, subsequently be provided without undue delay.

in complying, pursuant to Article 24 of the Federal Act on Data Protection, with the obligation to communicate without undue delay the personal data breach to the data subject, if it is necessary for their protection or if the Federal Assembly of the Swiss Confederation requests it.

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

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

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, at least the nature of the data breach, its consequences and the measures taken or planned, and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Article 24 of the Federal Act on Data Protection.

10. Non-Compliance with the Clauses and Termination

10.1 Without prejudice to any provisions of applicable data protection regulations, 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.

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

the processing of personal data by the processor has been suspended by the controller pursuant to Clause 10.1 and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

the processor is in substantial or persistent breach of these Clauses or its obligations under applicable data protection regulations;

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 under applicable data protection regulations.

10.3 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 7.1.2, the controller insists on compliance with the instructions.

10.4 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 the applicable law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Appendix No. 3 UK Data Processing Agreement ("DPA")

Preamble

The Parties aim to ensure that the Processor's processing of Personal Data complies with data protection regulations, as set out in the following Data Processing Agreement.

1. Purpose and Scope

- 1.1 The purpose of these Standard Contractual Clauses ("Clauses") is to ensure compliance with the Data Protection Act 2018 of 23 May 2018 as the UK's implementation of the General Data Protection Regulation (UK GDPR), and therefore Article 28(3) and (4) of that Regulation.
- 1.2 These Clauses apply to the processing of personal data (available at <https://home.plus.heidelberg.com/#/legal/processings>).
- 1.3 These Clauses are without prejudice to obligations to which the controller is subject by virtue of the Data Protection Act 2018..
- 1.4 These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the United Kingdom General Data Protection Regulation.

2. Invariability of the Clauses

- 2.1 The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- 2.2 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.

3. Interpretation

- 3.1 Where these Clauses use the terms defined in United Kingdom General Data Protection Regulation, those terms shall have the same meaning as in that Regulation.
- 3.2 These Clauses shall be read and interpreted in the light of the United Kingdom General Data Protection Regulation.
- 3.3 These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in United Kingdom General Data Protection Regulation or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. 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.

5. (Intentionally left blank)

6. 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 the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7. Obligations of the Parties

7.1 Instructions

The processor shall process personal data only on documented instructions from the controller, unless required to do so by domestic 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.

The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the United Kingdom General Data Protection Regulation or any other applicable domestic data protection regulation.

7.2 Purpose Limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>), unless it receives further instructions from the controller.

7.3 Duration of the Processing of Personal Data

Processing by the processor shall only take place for the duration specified in the description of data processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

7.4 Security of Processing

The processor shall at least implement the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) 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.

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.

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.

7.6 Documentation and Compliance

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

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

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 the United Kingdom General Data Protection Regulation or applicable data protection law. 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.

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.

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.

7.7 Use of Sub-Processors

For purposes of this Clause 7.7, the processor has the controller's general authorisation for the engagement of sub-processors from an agreed list (available at <https://home.plus.heidelberg.com/#/legal/subprocessors>). 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 three weeks 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.

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 the United Kingdom General Data Protection Regulation or domestic data protection law.

At the controller's request, the processor shall provide a copy of such a sub-processor 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.

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.

The processor shall agree to 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.

7.8 International Transfers

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 domestic law to which the processor is subject and shall take place in compliance with Chapter V of the United Kingdom General Data Protection Regulation.

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 United Kingdom General Data Protection Regulation, the processor and the sub-processor can ensure compliance by using standard contractual clauses made by the Secretary of State in

accordance with of section 17C of the 2018 Act, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the Controller

8.1 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.

8.2 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 Clauses 8.1 and 8.2, the processor shall comply with the controller's instructions.

8.3 In addition to the processor's obligation to assist the controller pursuant to Clause 8.2, 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 by:

carrying 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;

consulting the competent supervisory authority/ies prior for 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;

ensuring 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;

complying with the obligations in Article 32 of the United Kingdom General Data Protection Regulation.

8.4 The processor is required to assist the controller in the application of this Clause, including taking the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>).

9. 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 of the United Kingdom General Data Protection Regulation, where applicable, taking into account the nature of processing and the information available to the processor.

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:

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);

in obtaining the following information which, pursuant to Article 33 (3) of the United Kingdom General Data Protection Regulation, shall be stated in the controller's notification, and must at least include:

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;

the likely consequences of the personal data breach;
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.

in complying, pursuant to Article 34 of the United Kingdom General Data Protection Regulation, 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.

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

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

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 the technical and organisational measures (available at <https://home.plus.heidelberg.com/#/legal/toms>) 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 the the United Kingdom General Data Protection Regulation.

10. Non-Compliance with the Clauses and Termination

10.1 Without prejudice to any provisions of the the United Kingdom General Data Protection Regulation, 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.

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

the processing of personal data by the processor has been suspended by the controller pursuant to Clause 10.1 and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

the processor is in substantial or persistent breach of these Clauses or its obligations under the United Kingdom General Data Protection Regulation or domestic data protection law;

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 the United Kingdom General Data Protection Regulation or domestic data protection law.

10.3 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 7.1.2, the controller insists on compliance with the instructions.

10.4 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 applicable law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Appendix No. 4 California Data Processing Agreement

1. Definitions.

- 1.1 The following definitions shall apply for purposes of interpreting this California DPA:

"Applicable Law(s)" means all applicable U.S. federal and/or state laws, rules, regulations, directives, governmental and regulatory requirements and guidance including, but not limited to, security, confidentiality, and/or privacy laws, standards, guidelines, policies, regulations, and procedures that are applicable to Heidelberg, the Services, Customer Personal Information, and/or any other programs or products provided pursuant to the Contract, including but not limited to the California Consumer Privacy Act of 2018 (California Civil Code § 1798.100 *et seq.*), as amended (including, without limitation, by the California Privacy Rights Act ("CPRA"))("CCPA").

"Approve", "Approved", and "Approval" mean approved in writing by an authorized representative of Customer.

"Business Purposes" shall mean the enumerated Business Purposes set forth in Cal. Civ. Code section 1798.140(e)(1)-(8) that are applicable to the Services as set forth in the Contract, including but not limited to: performing Services on behalf of Customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or providing similar services on behalf of Customer.

"Collects", "collected", "collection", "consumer", "process(ing)", "personal information", "sell", "sensitive personal information", "share", "selling", "sale", "sold", and "service provider" shall have the meanings given to such terms in Applicable Laws.

"Customer Personal Information" means personal information that is received, collected or accessed by Heidelberg in connection with the Services or Contract.

"Consumer Rights Request" means a communication from a consumer requesting to exercise their individual rights under Applicable Laws.

"Services" means the services and other activities that Heidelberg shall provide or carry out for Customer as set forth in the underlying Contract.

2. Details of the Processing:

- 2.1 Details regarding Heidelberg's Processing of Customer Personal Information. are set forth in the description of Personal Information processing (available at <https://home.plus.heidelberg.com/#/legal/processings>).

3. Restrictions on Heidelberg's Processing:

- 3.1 Heidelberg is permitted to Process Customer Personal Information solely for purposes of performing the Services and to carry out the Business Purposes under the Contract, or as otherwise required or permitted by Applicable Law of a Service Heidelberg, or as agreed to or instructed by Customer. Without limiting the generality of the foregoing, except as otherwise permitted by the forgoing sentence, Heidelberg is prohibited from:

Selling or Sharing Customer Personal Information;

retaining, using, disclosing, or otherwise Processing Customer Personal Information for any purpose other than for the specific purpose of providing Services to Customer and to carry out the Business Purposes under the Contract;

retaining, using, or disclosing Customer Personal Information for any commercial purpose other than to perform

the Services and to carry out the Business Purposes under the Contract;

retaining, using, disclosing, or Processing Customer Personal Information outside of the direct business relationship between Customer and Heidelberg; and

combining Personal Information received from or on behalf of Customer with Personal Information it receives from, or on behalf of, another person(s), or collects from its own interaction with a consumer, except where expressly required to perform the Services.

- 3.2 Heidelberg certifies it understands the restrictions in this section and will comply with them. Heidelberg shall not provide access to Customer Personal Information to any other entity, unless agreed to or instructed by Customer or required by Applicable Law, except it may use subcontractors to perform the Services, provided (i) Heidelberg provides Customer a reasonable opportunity to object to the engagement of subcontractors and (ii) such subcontractors agree in writing to substantially the same terms that apply to Heidelberg through this California DPA.

- 3.3 Notwithstanding anything herein to the contrary, Customer acknowledges that Heidelberg may retain, use, disclose, or otherwise Process Customer Personal Information in manners permitted of a Service Heidelberg or as otherwise required by Applicable Laws (e.g., to engage subcontractors for sub-processing, for permitted internal uses such as improving products and services, for security and fraud prevention, compliance with legal obligations, etc.).

4. Heidelberg's Obligations:

- 4.1 Heidelberg shall, with respect to the Services and the Customer Personal Information:

comply with Applicable Laws in performing the Services, reasonably assist Customer in meeting its obligations under Applicable Laws, and make available to Customer information in Heidelberg's possession necessary to demonstrate its compliance with its obligations under Applicable Laws upon Customer's reasonable request (subject to time and materials charges at standard rates for efforts that require material effort);

ensure the reasonable security of Customer Personal Information including by: (i) providing the same level of privacy protection to Customer Personal Information as is required by Applicable Laws and (ii) ensuring each person Processing Customer Personal Information is subject to a duty of confidentiality with respect to such Customer Personal Information;

notify Customer within the time period required by Applicable Laws if it determines it can no longer meet its obligations under Applicable Laws and allow Customer to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Customer Personal Information;

provide reasonable assistance to enable Customer to fulfill Consumer rights requests ("CRRs") (subject to time and materials charges at standard rates for efforts that require material effort), including but not limited to notifying Heidelberg's subcontractors to delete Customer-specified Customer Personal Information in response to a CRR made to Customer. Customer shall inform Heidelberg of CRRs that it needs Heidelberg's assistance to comply with and shall provide Heidelberg with information necessary to assist Customer to comply with such CRRs;

if Heidelberg receives a CRR from a Consumer that might relate to Customer Personal Information it shall respond that it cannot act upon requests made to it as to Personal Information it Processes as a Service Heidelberg. If the request specifically identifies Customer in connection with the CRR, Heidelberg shall inform Customer of such request;

notify Customer of security incidents affecting Heidelberg's Processing of Customer Personal Information that require notification to Personal Information subjects and/or government authorities under Applicable Law ("Breach") and provide reasonable assistance and information regarding such Breach;

provide Customer information to reasonably enable it to conduct and document data protection assessments;

delete Customer Personal Information at the end of the provision of Services, or as otherwise instructed by Customer, unless retention is (i) required by Applicable Laws; or (ii) retained as part of backup or record keeping, so long as only used for such purposes and only for as long as reasonably necessary, subject to Applicable Laws and this California DPA; and

not more than once annually, allow and cooperate with reasonable assessments by Customer, or its designated assessor (or if mutually agreed and at Heidelberg's expense, Heidelberg's qualified assessor), to conduct an assessment of Heidelberg's policies and technical and organizational measures in support of the obligations under Applicable Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments and subject to reasonable access and confidentiality restrictions. If Heidelberg engages its own assessor, it shall provide a report of such assessment to Customer upon request.

5. Customer Obligations:

- 5.1 Customer acknowledges that it is the Controller of the Customer Personal Information and shall take all steps necessary to ensure that it has all necessary authority and Consent to enable Heidelberg to use the Customer Personal Information to provide the Services and Process the Customer Personal Information consistent with Applicable Law, the Contract and this California DPA, including without limitation timely providing Heidelberg all instructions for Heidelberg's Processing as may be required by Applicable Law (e.g., notice to delete, notice discontinue certain processing, etc.).