Standard Contractual Clauses

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

between

The Customer
as specified in the agreement regarding the questionnaire survey (Project Service Agreement).

(the data controller)

and

Human House A/S
Company reg. no. (CVR) 61896813
Dynamovej 11
DK-2860 Søborg
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

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

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of collection of questionnaire responses from the Data Subjects with the purpose of preparing a questionnaire survey, the data processor processes personal data on behalf of the data controller in accordance with the Clauses.

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

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

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

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

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

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

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

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

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

3. If the data controller's instructions are in breach of the General Data Protection Regulation or data protection provisions in other EU law or the national law of the Member States, the parties are obliged to jointly find a lawful solution. If the parties cannot find a solution without it being unnecessarily burdensome for the data processor, each party has the option to terminate the data processing agreement with 1 months' notice.

5. Confidentiality

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

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

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

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

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

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

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

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

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

   If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR to engage another processor (a sub-processor).

2. The data processor may not use a sub-processor for the fulfilment of the Clauses without prior specific written approval from the data controller.

3. The data processor may only use sub-processors with the prior specific written approval of the data controller. The data processor must submit the request for specific approval at least 3 months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The list of sub-processors that the data controller has already approved is set out in Annex B. Upon termination of the use of a sub-processor, the data processor must notify the data controller in writing.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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

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

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

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

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

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

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

9. Assistance to the data controller

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

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

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

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

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

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

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

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

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

    b. the likely consequences of the personal data breach;

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

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so upon request from the data controller, unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

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

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of which the Project Service Agreement is effective.

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

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

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

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the contact responsible set in the Project Service Agreement.

2. The parties shall be under obligation to continuously inform each other of changes to the contact responsible.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:
The purpose of the data processing is to collect questionnaire responses from the Data Subjects and share these responses with the data controller. *[Sharing only relevant if agreed upon in the Project Service Agreement]*

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
The processing consists of:

1. Sending out a questionnaire and collecting responses from the Data Subjects for use in mapping the work environment
2. Preparing data reports and statistics based on questionnaire responses
3. Sharing the prepared reports, including anonymized data reports and statistics with the data controller. *[Only relevant if agreed upon in the Project Service Agreement]*

A.3. The processing includes the following types of personal data about data subjects:
The following general personal data is processed, cf. Article 6 of the General Data Protection Regulation, regarding the Data Subjects:

- Email address
- Name
- Department
- Responses to questionnaires and the possibility of filling in text/comment boxes

[As agreed in the Project Service Agreement]

The following personal data, cf. Article 9 of the General Data Protection Regulation, may be processed:

- Health information
- Sexual relations *[Only relevant if the theme is included in the questionnaire]*

Personal data, cf. Article 9 of the General Data Protection Regulation, is processed solely on the Data Subjects own initiative, if the Data Subject provides such information in a survey text/comment box.

A.4. Processing includes the following categories of data subject:
Employees employed by the data controller, and if specified in the Project Service Agreement, citizens and members. (collectively, the Data Subjects)

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:
Personal data shared by data controller (Excel sheet) for the data processor to send out questionnaires to the Data Subjects, will be deleted no later than 3 months after completion of the Project Service Agreement. *[Not relevant, if agreed in the Project Service Agreement to forward a generic self-registration link or anonymous letter]*
Personal data collected by the data processor (including comments in text/comment boxes) will be deleted no later than 3 months after completion of the Project Service Agreement.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	COMPANY REG. NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft EU Ireland Operations Ltd	IE256796	South County Business Park, Leopardstown, Dublin 18, D18 DH6k, Ireland	Microsoft 365 data storage.
Rambøll Management Consulting A/S	60997918	Hannemanns Allé 53, 2300 København S, Denmark	Distribution of questionnaire link. Data storage.
NHL Data ApS	25575555	Gammel Køge Landevej 55, 2500 Valby, Denmark	IT operations and support including backup and restore.

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

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

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data controller instructs the data processor to contact and collect questionnaire responses from the Data Subjects. The data processor is also instructed to share responses with the data controller. *[Sharing only relevant, if agreed in the Project Service Agreement]*

C.2. Security of processing

The high level of security reflects that in special cases the processing includes sensitive personal data covered by Article 9 of the Regulation as well as confidential information.

The data processor is then entitled and obliged to make decisions on which technical and organisational security measures must be implemented in order to establish the necessary (and agreed) level of security.

However, the data processor must – in all circumstances and as a minimum – implement the following measures agreed with the data controller:

- Personal data is stored with the sub-processors mentioned in point B.1 and deleted no later than 3 months after completion of the Project Service Agreement. The specific technical and organisational measures are documented in the sub-processors' annual ISAE-3000 declaration for implemented IT controls.
- The agreed level of security is established with the necessary physical, logical security, including securing access conditions, user accounts and data protection.
- All employees of the data processor are subject to a general duty of confidentiality contained in their employment contract, and various professional groups such as nurses, doctors and psychologists are also subject to additional legislation on confidentiality.

The data processor regularly checks and assesses technical and organizational measures to ensure the security of processing at sub-data processors.

The data processor's employees have received instructions on the correct and secure handling of personal data.

The data processor uses sub-data processors that are certified according to ISO 27001 supplemented with ISAE-based auditor's statements. The data processor has outsourced all technical services to certified and controlled sub-data processors who have the necessary experience and the necessary guarantees to assist with business continuity activities and the accompanying measures.

The data processor is building a similarly high level according to an ISO 27001 based Statement of Applicability, which will ensure the maturation of all processing systems and services.

The personnel handbook and awareness campaigns create the basis for all the data processor's employees to be aware of their obligations regarding data protection.

In general, the data processor uses MFA and VPN as well as Bitlocker-protected devices and user accounts. All activities around the life cycle of documents, emails and personal data-bearing systems are logged.

C.3. Assistance to the data controller

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

The data processor shall, in accordance with the agreement with the data controller, assist the data controller to the extent possible in ensuring compliance with the obligations of the agreement, including in Articles 32 (implementation of appropriate technical and organizational measures), 35 (conducting a data protection impact assessment) and 36 (prior consultation) of the Regulation.

The data controller's expenses in connection with audits, inspections, etc., shall be borne by the data controller itself. The data processor is entitled to invoice the data controller for necessary expenses and time spent, including costs for sub-processors and third-party assistance in connection with audits, inspections, etc. that may result from any request, instruction or assistance pursuant to this agreement, just as the data controller will be invoiced for any payments to sub-processors and for other third-party assistance.

C.4. Storage period/erasure procedures

Personal data is not returned to the data controller but is deleted by the data processor after termination of the services or no later than 3 months after completion of the Project Service Agreement.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

Personal data is stored in a data center at Microsoft at the address: South County Business Park, Leopardstown, Dublin 18, D18 DH6k in Ireland, Rambøll at the address: Silkeborgvej 53, 8000 Århus C in Denmark, and NHL Data ApS at the address: Gammel Køge Landevej 55, 2500 Valby, in Denmark.

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

The processing of personal data that the data processor carries out in agreement with the data controller may only be carried out by the data processor or sub-processors within the borders of EU/EEA.

The data processor is not entitled to allow data processing to take place outside the borders of EU/EEA without the written consent of the data controller.

If the data controller does not provide documented instructions regarding the transfer of personal data to a third country in these Terms or subsequently, the data processor is not entitled to carry out such transfers within the framework of these Terms.

C.7. Procedures for the data controller’s audits, including inspections, of the pro-cessing of personal data being performed by the data processor

The data controller or the data controller’s representative shall have access to carry out inspections, including physical inspections, of the places and systems where the processing of

personal data is carried out by the data processor. Inspections can be carried out when the data controller deems it necessary, as long as the services regarding the processing of personal data have not ceased in accordance with Clause 14.4, e.g., upon deletion according to Appendix A.5, and the data processor cannot refuse or limit the data controller's right thereto. However, inspections must be requested with reasonable notice, so that the data processor can arrange access and allocate the necessary resources for conducting the inspection.

Upon request, the data processor shall make available the documentation necessary for the data controller to assess the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and these Clauses, including internal policies, procedures and relevant controls, and any statements in accordance with section C.8.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall annually carry out inspections of the sub-processors by obtaining the sub-processor's latest audit statement regarding the sub-processor's compliance with the GDPR, data protection provisions in other EU law or the national law of the Member States, and these Provisions. The data controller may at any time request the data processor to obtain a copy of the sub-processor's latest audit statement.

The data processor or a representative of the data processor may request access to carry out inspections, including physical inspections, of the premises from which the Sub-processor processes personal data, including physical premises and systems used for or in connection with the processing.

In the event, that an inspection is carried out, documentation of the results thereof may be forwarded to the data controller for information. The data controller may challenge the framework and/or method of the inspection and may in such cases request the performance of a new inspection under a different framework and/or using a different method against payment of expenses and time spent.

Appendix D The parties' terms of agreement on other subjects

No regulation of other subjects has been agreed between the parties, other than as stated in the Project Service Agreement.