Joint Data Responsibility Arrangement

Between

Data controller 1

[Name]

CVR [CVR number]

[Address]

[Zip code and city]

[Country]

and

Data controller 2

Health Group

CVR 30273893

Kongevejen 377

2840 Holte

Danmark

1 Shared data responsibility

1.1 This arrangement sets out the division of responsibilities between Data controller 1 and Data controller 2 in relation to:

Implementation of occupational health and safety assessment(s) and/or well-being survey(s) according to the agreement between the parties.

1.2 According to Article 26 of the General Data Protection Regulation, joint Data controllership exists when two or more Data controllers jointly determine the purposes and means of the processing.

In the case of joint Data controllership, the joint Data controllers shall determine in a transparent manner their respective responsibilities for compliance with the obligations under the General Data protection Regulation, in particular to exercise the data subject's rights and their respective obligations to provide the information referred to in Articles 13 and 14, by means of an arrangement between them, unless and to the extent that the respective responsibilities of the Data controllers are laid down in Union or Member States' national law to which the Data controllers are subject.

The arrangement shall, in accordance with Article 26(2) of the General Data Protection Regulation, duly reflect the respective roles of the joint Data controllers and their relationship with the data subjects. The main content of the arrangement must also be made available to data subjects.

However, regardless of the terms of the arrangement, the data subject may exercise their rights under the General Data Protection Regulation with regard to and against the individual Data controller.

Similarly, the "internal" division of responsibilities in the joint Data controller arrangement does not prevent the supervisory authority from exercising its powers in relation to both Data controller 1 and Data controller 2.

1.3 There is an arrangement between Data controller 1 and Data controller 2 that there is joint data controller in the context of [specify processing activity]. In assessing this, account has been taken, inter alia, of:

Workplace Assessment

The basis for the processing of personal data is a comprehensive solution where Health Group has designed the questionnaire and, therefore, defines which personal information should be processed and the purposes for which the information is collected, such as overall quality assurance of the occupational health and safety assessment (APV survey).

Since the customer participates in decisions regarding the customization of questions, including potential adjustments to the questionnaire and the addition of extra questions to meet any CSR requirements (such as diversity in employment and well-being), there will generally be a shared responsibility between Health Group and the customer.

Health Group is responsible for the IT operation of the utilized IT system, DigiHealth, including ongoing operation and development of the solution, decisions on which personal data is necessary to process for a good user experience, information obligation texts, obtaining any necessary consent, cybersecurity, etc.

In some cases, an alternative IT system, Enalyzer, may be used, with the customer's agreement, if DigiHealth is not compatible with the customer's needs.

Employee Satisfaction Survey

An employee satisfaction survey will typically be based on Health Group's standard questionnaire, with Health Group determining which personal data needs to be processed and for what purpose. As the customer will assist in customizing/adding questions, the starting point will be a joint data responsibility between Health Group and the customer.

Health Group is responsible for the IT operation of the utilized IT system, DigiHealth, including ongoing operation and development of the solution, decisions on which personal data is necessary to process for a good user experience, information obligation texts, obtaining any necessary consent, cybersecurity, etc. In some cases, an alternative IT system, Enalyzer, may be used with the customer's agreement.

1.4 This arrangement is designed to enable Data controller 1 and Data controller 2 to comply with the joint liability requirements of Article 26 of the Data Protection Regulation. The arrangement sets out the respective responsibilities of Data controller 1 and Data controller 2 to comply with the obligations of the General Data protection Regulation, in particular to exercise the data subject's rights and the obligation to provide the information referred to in Articles 13 and 14.

2 Overall allocation of responsibilities

2.1 Data Controller 1 is the employer and thus has the overall responsibility for the employees who are data subjects in connection with the processing activity. Data Controller 1 ensures that the employees are invited to the planned activities and may customize the questionnaire in collaboration with Data Controller 2.

2.2 Data Controller 2 is an expert in delivering workplace assessments and employee satisfaction surveys. They have developed the questionnaire, supporting tools, including IT systems, and processes related to data processing. In collaboration with Data Controller 1, Data Controller 2 adjusts the questionnaire, conducts analyses, and formulates recommendations based on the collected data.

3 Principles and treatment eligibility

3.1 Data Controller 2 collects any necessary consents directly from the employees, while Data Controller 1, as the employer, is legally obligated to conduct workplace assessments according to the Occupational Health and Safety Act.

3.2 Data controller 1 and Data controller 2 are both responsible for complying with the Principles for the Processing of Personal Data to the extent that the rules apply to the Data controller's responsibilities under this arrangement.

4 Rights of data subjects

4.1 Both parties shall be responsible for safeguarding the rights of data subjects by complying with the following rules of the General Data Protection Regulation:

- the obligation to provide information when collecting personal data from the data subject,
- the obligation to provide further information if personal data have not been collected from the data subject,
- the data subject's right of access,
- the right of rectification,
- right to erasure (right to be forgotten),
- the right to restriction of processing,
- the obligation to provide information in relation to the rectification or erasure of personal data or the restriction of processing,
- the right to data portability (except for public authorities); and
- the right to object to processing.

4.2 If Data controller 1 receives a request or an enquiry from a data subject concerning the matters covered by the responsibilities of Data controller 2 as set out above, it shall be transmitted to Data controller 2 for reply as soon as possible.

4.3 If Data controller 2 receives a request or an enquiry from a data subject concerning the matters covered by the responsibilities of Data controller 1 as set out above, it shall be transmitted to Data controller 1 for reply as soon as possible.

4.4 Both Parties shall be responsible for assisting each other to the extent appropriate and necessary for both Parties to comply with their obligations to data subjects.

5 Security of processing and evidence of compliance with the GDPR

5.1 Both parties will be responsible to implement appropriate technical and organisational measures to ensure and demonstrate that the processing is in compliance with the General Data Protection Regulation; taking into account the nature, scope, context and purposes of the processing involved, as well as the risks of varying degrees of likelihood and severity for the rights and freedoms of natural persons. The measures shall be reviewed and updated as necessary (Article 24 of the Data Protection Regulation). This may involve, for example, Both parties establishing procedures for dealing with security breaches, access requests or compliance with the obligation to provide information.

5.2 Both parties measures shall include, where proportionate to the processing activities, the implementation of appropriate data protection policies.

5.3 Both parties shall be responsible for compliance with the data protection by design and data protection by default rule of Article 25 of the General Data Protection Regulation.

5.4 Both parties is responsible for complying with the requirement of Article 32 of the General Data Protection Regulation on security of processing. This implies Both parties taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing operation concerned, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure an appropriate level of security appropriate to those risks.

Both parties shall carry out and evident a risk assessment form and then implement measures to mitigate the identified risks.

5.5 Since Data Controller 2 operates the IT systems in which the majority of personal data is collected and processed, Data Controller 2 is responsible for Article 24, 25, and 32 with regard to these systems.

6 Use of data processors and sub-processors

6.1 Both parties are entitled to use processors and/or any sub-processors in connection with the joint processing operation.

6.2 In the event of the use of processors and/or sub-processors, Both parties shall be responsible for complying with the requirements of Article 28 of the General Data Protection Regulation. Accordingly, Both parties shall, inter alia:

- use only processors that can provide the necessary guarantees that they implement appropriate technical and organizational measures in such a way as to ensure that processing complies with the requirements of this Regulation and safeguards the rights of the data subject,
- ensure that a valid data processing arrangement is in place between Party and the processor; and
- ensure that there is a valid sub-processor arrangement between the processor and any sub-processor.

6.3 Both parties shall be informed, upon request, whether the data is processed by processors and, where applicable, sub-processors of the other party.

6.4 If processors process the data and, where applicable, sub-processors, Parties shall be informed, upon request, of the content of the arrangements between Parties and the processor/sub-processor.

7 Records of processing activities

7.1 Both Parties shall be responsible for complying with the requirement of Article 30 of the General Data Protection Regulation on records of processing activities. This implies that Both parties shall establish a record of the processing activities for which the Parties are joint controllers.

7.2 Both parties shall inform the other of the content of the above record.

7.3 Both Parties shall establish - based on the contents of the other record - their own record of the processing activities covered by the arrangement.

8 Notification of personal data breaches to the supervisory authority

8.1 Both Parties shall be responsible for compliance with Article 33 of the General Data Protection Regulation on the notification of personal data breaches to the supervisory authority.

9 Communication of personal data breaches to the data subject

9.1 Both parties shall be responsible for compliance with Article 34 of the General Data Protection Regulation regarding the communication of personal data breaches to the data subject.

10 Data protection impact assessment and prior consultation

10.1 Both Parties shall be responsible for compliance with the requirement of Article 35 of the General Data Protection Regulation on data protection impact assessments. This implies that, where a type of processing, in particular using new technologies and by virtue of its nature, scope, interrelation and purposes, is likely to result in a high risk to the rights and freedoms of natural persons, Both parties shall, prior to the processing, carry out an analysis of the implications of the envisaged processing activities for the protection of personal data.

10.2 Both parties shall also comply with the requirement of Article 36 of the General Data Protection Regulation to consult the supervisory authority in advance, where appropriate.

10.3 Both parties agree that it is unlikely that the processing will result in a high risk for the data subjects, and therefore, there is no need to conduct a impact assessment.

11 Transfer of personal data to third countries or international organizations

11.1 Both parties may decide that personal data may be transferred to third countries or international organizations.

11.2 Both parties shall be responsible for compliance with the requirements of Chapter V of the General Data Protection Regulation in the event of transfers of personal data to third countries or international organizations.

12 Complaints

12.1 The Parties shall each be responsible for handling any complaints from data subjects, if the complaints relate to a breach of the provisions of the General Data Protection Regulation, for which the Party is responsible under this arrangement.

12.2 If one of the Parties receives a complaint, which should rightly be dealt with by the other Party, the complaint shall be forwarded to that controller as soon as possible.

12.3 If one of the Parties receives a complaint, part of which should rightly be dealt with by the other Party, that part shall be forwarded to the Party for reply as soon as possible.

12.4 The data subject shall be informed of the essential content of this arrangement when one Party forwards a complaint or part thereof to the other Party.

13 Informing the other party

13.1 The Parties shall inform and liaise with each other of any material facts affecting the joint processing operation and this arrangement.

14 Regulation of other matters

14.1 This agreement comes into effect upon the signature of both parties.

14.2 The agreement is valid as long as the relevant information is processed, or until the agreement is replaced by a new agreement that establishes the allocation of responsibilities regarding the processing.

15 Entry into force and termination

15.1 This arrangement shall enter into force upon signature by both Parties hereto.

15.2 The arrangement shall remain in force for as long as the data concerned are processed or until it is replaced by a new arrangement laying down the division of responsibilities in relation to the processing.

15.3 Signature

On behalf of [Data controller 1]	On behalf of Health Group
_____	
Name:_____	Name: Adam Rosenkilde
Position:_____	Position: CEO
Date: _____	Date: _____

16 Appendix A – Article 30 record

Contact information:

Data Controller 2

[Name], [Adress], [Zip code and City], [Country]

CVR [CVR-number]

Contact information for any representative and/or Data Protection Officer (DPO):

Data Controller 2

Health Group A/S, Kongevejen 377, 2840 Holte, Danmark

CVR 30273893

Contact information for any representative and/or Data Protection Officer (DPO): dpo@healthgroup.dk

Purposes of the processing:

If workplace assessment is selected:

- To comply with the requirements of the Occupational Health and Safety Act for workplace assessments, including ongoing follow-up and evaluation of improvement measures and initiatives in the occupational health and safety field.

If employee satisfaction survey is selected:

- To conduct employee satisfaction surveys, including ongoing follow-up and evaluation of improvement measures and initiatives in the occupational health and safety field.

Categories of data subjects:

- Current and former employees and other participants in workplace assessment(s) and/or employee satisfaction survey(s).

Categories of recipients:

- Data processors, as well as Data Controller 1 and Data Controller 2.

Chapter V transfers and legal bases:

- No transfers to third countries or international organizations.

Expected timeframes for processing:

- Personal data is deleted or anonymized when no longer necessary.

General description of technical and organizational security measures:

- Modern security measures are employed, including strong encryption during transmission over open networks, pseudonymization or anonymization to the extent possible, and data minimization measures in the design of questions and solutions.