Version 4 – February 2025

DATA PROCESSING AGREEMENT

Standard Contractual Clauses

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

Between

The Customer to Summit's services
(as specified in the applicable Order Form, or Statement of Work or Engagement Letter or as set out below under signature)
(the "Data Controller")

and

Summit Sweden AB
Holländergatan 17B
111 60 Stockholm, Sweden
Org.no. 559423-3578 -

(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.

Signatures:

For Summit A/S:

Name: Karsten Søderberg

Job title: CEO

For Customer (the Data Controller):

Name:

Job title:

Date of signing:

Company name:

VAT-no.:

Address:

Country:

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 the provision of the Data Processor's services as set out in the applicable Order Form (or Statement of Work) or Engagement Letter, which may include use of online personality assessment tools, support and consultancy services in connection hereto, or otherwise as agreed between the Parties, the Data Processor will process 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. Five 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. Appendix E contains the Data Processor's technical and organisation safety measures.

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

12. 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.

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.

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.

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

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.

4. 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 in order to engage another processor (a sub-processor).

2. The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.

3. The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Data Controller can be found in Appendix B.

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. The Data Processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the Data Processor – the Data Controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the Data Processor, e.g. enabling the Data Controller to instruct the sub-processor to delete or return the personal data.

7. 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 organisation

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

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

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, 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 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 seventy-two (72) 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 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 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 the 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 i) of both Parties' signature, or ii) as set out in the initial Order Form (or Statement of Work) or Engagement Letter or iii) when the Data Processor starts to process personal data on behalf of the Data Controller – whichever is first.

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.

5. Signature
The Data Processor and the Data Controller have signed on page 1 of these Clauses.

15. Data Controller and data processor contacts/contact points

1. The Parties may contact each other using the following contacts/contact points:

2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for the Data Controller:
For contact information for the Data Controller reference is made to the applicable Order Form (or Statement of Work) or Letter of Engagement. The Data Controller must ensure that the Data Processor always has the correct contact information.

Contact information for the Data Processor:
Telephone: +45 45851515
E-mail for support and standard requests and other information: support@summitlead.com
E-mail for data protection requests only: data@summitlead.com
E-mail for deletion requests only: deletion@summitlead.com

Appendix A – Information about the processing

Summit acts as data controller in relation to our consultancy services and our workshops.
Summit acts as Data Processor as part of providing access to and support to our customer's (the Data Controller) use of the online personality assessment platform(s), primarily HALO, which is provided by Hogan Assessment Systems Inc.

A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:
The Data Processor's provision of its data processing services as ordered by or agreed with the Data Controller.
These services may include:

- Distribution and support of online personality assessment products provided by Hogan Assessment Systems Inc., including the online platforms HALO and Hogan Talent (HT), and – depending on Customer's order - other third-party providers.
- Other data processing services as agreed (for example handling of the Data Controller's access and use of the platforms)

Anonymised data may be processed for research purposes by the relevant provider (sub-processor). Data anonymization will be irreversible and will at all times take into account the legal and technical criteria established by the European data protection authorities.

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):
Collection, review, processing, transfer, storage, deletion, etc. for use in the following purposes:

- Provision of the data processing services agreed between the Parties, such as access and support to the online platform(s), including HALO and Hogan Talent (HT);
- Handling of data protection issues as well as other technical issues, such as transfer of and access to personal data, etc.;
- Storage of personal data, including in connection with back-up (primarily in the platform(s)); and
- Fulfilment of the Agreement and these Clauses.

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

- User ID, name, e-mail address, job role, information about the employer (the Data Controller), answers to questions in a personality assessment and the results of the personality assessment.
- The Data Processor does not process special categories of personal data, cf. article 9 of the GDPR. The Data Controller should make sure and instruct the data subject to not provide special categories of personal data subject to article 9 of the GDPR.

A.4. Processing includes the following categories of data subject:
Depending on the nature of the Data Controller's organization, the processing of personal data will include the following data subjects (depending on the instruction given by Data Controller):

- Job applicants, employees, consultants, executives, board members, other third parties etc. connected to the Data Controller, e.g. the person completing the personality test or end-users using the online personality assessment platform (typically the Data Controller's HR staff).

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:

Processing of personal data is performed for as long as the Data Processor processes personal data on behalf of the Data Controller, including processing and storage in the Platform(s). The Data Controller may at any time request ongoing deletion of personal data in accordance with the deletion process described below.

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	Address	Description of processing
Hogan Assessment Systems, Inc. Company reg.no.: 1900458310	11 S. Greenwood, Tulsa, OK 74120, USA	Provider of online personality assessment platform(s), including HALO and Hogan Talent (HT). Processing of personal data, incl. assessment results, relates to the use of the online platform(s), incl. collection, review/analysing, processing, transfer, storage, incl. for backup, deletion, support etc., to the extent necessary to provide the services.
Summit A/S Company reg.no.: 26787610	Sundkrogsgade 7,4. DK-2100 Copenhagen, Denmark	Provider of all support services necessary to fulfil the contractual obligations under the service agreement as well as all invoicing services.
Supporters A/S Company reg.no.: 32272592	Ledreborg Alle 118E 4000 Roskilde Denmark	Supporters functions as an external IT department. Provider of IT Support for Microsoft 365, supporting SharePoint, OneDrive, Teams and Exchange to Summit.
Acronis International GmbH Company reg.no.: CHE-113.666.835	Rheinweg 9, Schaffhausen, 8200 Switzerland	Summit has an offsite backup of data stored in the Microsoft 365 platforms. The backup is handled by Acronis, with a minimum of 180 days retention. Automated, cloud-to-cloud backup of Microsoft 365, supporting SharePoint, OneDrive, Teams and Exchange. Includes cloud storage, with ongoing maintenance managed by Acronis. This is located at the Acronis Cloud Backup ISO27001 certified datacentre in EU (Frankfurt, Germany).
Microsoft Ireland Operations Limited Company reg.no.: IE 8256796U	One Microsoft Place, South County Busi-ness Park, Dublin D18 P521, Ireland	Microsoft 365 for hosted services like SharePoint, OneDrive, Exchange and Teams used for storage, day-to-day communication, meetings and for providing the services. Location of data centre is in EU.

The Data Controller shall on the commencement of the Clauses authorise the use of the abovementioned relevant 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.

B.2. Prior notice for the authorisation of sub-processors

If the Data Controller wishes to object to the change or addition of sub-processors, the Data Controller must notify the Data Processor within 14 (fourteen) days of receipt of the notification in accordance with Clause 7.

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: Provision and delivery of the services agreed with or ordered by the Data Controller pertaining to Data Controller's use of the online Platform(s), incl. HALO and Hogan Talent (HT), and other services regarded as data processor-activities.

C.2. Security of processing

In addition to the security measures described under Clause 6 the Data Processor shall adhere to the security measures described in Appendix E. The security measures only describe the Data Processor's own internal security measures and not those of the sub-processors, incl. Hogan Assessment Systems Inc. Such security measures may be provided upon request and are included in the EU Standard Contractual Clauses entered into with the sub-processors.

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 Controller has independent access to the personal data processed by the Data Processor via the self-service solution on the Platform(s) (including HALO and Hogan Talent (HT) and subsequent versions hereof) or the documents received, and the Data Controller thereby has, as a starting point, the ability to independently fulfil the data subject's rights as set out in Chapter III of the GDPR and handle requests from the data subjects, cf. Clause 9.1. The Data Controller may request additional assistance from the Data Processor to the extent necessary and to the extent the Data Controller is not able to independently respond to such requests.
- If the Data Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Data Controller, and the request concerns personal data processed on behalf of the Data Controller, the Data Processor shall without undue delay forward the request to the Data Controller.
- The Data Processor will provide timely assistance to the Data Controller in accordance with Clause 9.2.

C.4. Storage period/erasure procedures

Personal data, including participant information and the results of the personality assessment, are stored in the platform(s), including HALO and Hogan Talent (HT) provided by Hogan Assessment systems Inc., for a period of 2 years from the time of carrying out of the personality assessment, after which it is automatically deleted or fully anonymised by the sub-processor. The Data Controller may instruct the Data Processor in writing to delete personal data ongoingly and/or within another timeframe. The Data Controller shall ongoingly review its admin-user site to verify correct erasure of personal data and personality assessment results. These deletion timeframes apply regardless of whether the services have been terminated, is still active or subject to inactivity. Personal data may also be processed for as long as necessary to provide the services.

Personality assessments related to trials and workshops, including certification workshops, are not part of the data processing activities as Summit is the data controller for such services and this data will automatically be deleted after 6 months unless requested transferred to the customer's HALO account (data transfers are subject to a fee payable to Hogan Assessment Systems Inc.).

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: The processing of personal data takes place from the Data Processor's locations as well as sub-processors' locations listed in Appendix B.

C.6. Instruction on the transfer of personal data to third countries
Where, in accordance with these Clauses, the Data Processor transfers personal data to sub-processors in third countries outside the EU/EEA, the Data Processor shall secure a legal basis for the transfer in accordance with Chapter V of the GDPR. By entering into these Clauses, the Data Controller agrees that the Data Processor transfers personal data to and stores personal data in third countries to the extent necessary using the sub-processors listed in Appendix B.

The Data Processor uses the EU Commission's Standard Contractual Clauses as a basis for the transfer of personal data to third countries. The Data Controller authorizes the Data Processor to enter into the EU Commission's Standard Contractual Clauses with sub-processors in third countries in accordance the Clauses. As an additional transfer tool, transfers may also be based on an "adequacy decision", cf. article 45 GDPR, such as a potential Trans-Atlantic Data Privacy Framework Agreement between EU and U.S, (if applicable).

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

1. The Data Processor shall, upon the Data Controller's written request, provide the Data Controller with documentation of the Data Processor's compliance with these Clauses, with the instruction and with the relevant articles in the GDPR regarding the personal data being processed on behalf of the Data Controller. The documentation may consist of self-audit report(s) prepared by the Data Processor and will be prepared or updated annually or when deemed necessary. The self-audit will follow the principles and control objectives of the ISAE 3000 auditing standard as laid down by Common Strategic Framework (CSF) - Danish Auditors and the Danish Data Protection Agency, and/or other internationally recognized standards such as ISO/IEC 27701:2019 and/or other recognised standards (at the Data Processor's discretion). At its own initiative, the Data Processor may also, but is not obligated to, obtain an external audit report by an independent auditor. The Data Processor will also share relevant audit material obtained from its sub-processors to the extent this is not marked confidential by the sub-processor.

2. The Data Processor's documentation shall be sent to the Data Controller within a reasonable time after receiving the request. The Data Processor will usually respond within 14 days but is allowed up to 30 days to respond (and longer if specific information or documentation takes longer to obtain in which case the Data Controller will be informed).

3. The Data Controller may conduct an audit to verify the Data Processor's compliance by reviewing the self-audit report (or the external audit report if such has been conducted) and related documentation provided by the Data Processor. The related documentation may consist of compliance documentation from relevant sub-processors (some of which may be subject to signing a non-disclosure agreement). The Parties agree that such audit report and related documentation fulfils the Data Processor's obligation to contribute to audits. The Data Processor will provide this self-audit report (or the external audit report if such has been conducted) and related documentation free of charge.

4. The following applies if the Data Controller - in addition to or instead of the self-audit report (or the external audit report if such has been conducted) and compliance documentation already prepared by the Data Processor under C.7.1-3 - specifically requests an audit or inspection conducted by either the Data Controller itself or a third party (either a physical or written audit, e.g. by sending its own questionnaires): The Data Processor shall maximum once per year contribute to a physical or written audit conducted by either the Data Controller or an independent third party or otherwise contribute to obtain an auditor's report or inspection report from an independent third party concerning the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The auditor/independent third party in question must be subject to confidentiality under law or agreement. The Data Controller must notify the audit/inspection in writing with 30 days prior notice. For the sake of clarity, an external audit or inspection conducted by the Data Controller or a third party (either a physical or written audit) under this section C.7.4 includes, but is not limited to, written questionnaires to be answered by the Data Processor, additional questions or requests for additional information which is not already contained in either the self-audit report (or the external audit report if such has been conducted) or the compliance documentation already provided by the Data Processor under section C.7.1-3. The total frequency of audits (regardless of the method) conducted by the Data Controller shall not exceed once per year. The Data Controller is responsible for all costs and expenses, including any fees charged by any third party or auditor, in relation to any audits (whether physical or written) requested by the Data Controller under section C.7.4. The Data Processor's assistance with such audit is subject to separate remuneration. The Data Controller shall compensate the Data Processor for any time spent and costs incurred by the Data Processor.

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

Subject to C.7., the Data Processor shall once per year or when deemed required and at their own expense and at its own discretion obtain an audit report, inspection report or a self-declaration concerning the Data Processor's sub-processors' compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The Data Processor shall make relevant documentation available to the Data Controller at the Data Controller's request.

Appendix D – The Parties' terms of agreement on other subjects

D.1. Compliance with Clause 7.6.
The Parties agree that the Data Processor shall only comply with the obligation to include the Data Controller as a beneficiary third party in its agreements with sub-processors to the extent that this can reasonably be implemented vis-à-vis the relevant sub-processors.

D.2. Assistance to the Data Controller
The Data Processor's assistance under these Clauses is remunerated separately, including assistance and contribution in connection with clause 9, clause 12, appendix C.3, C.7-8, any assistance with matters to which the Data Controller has self-access or already received specific documents or information or which otherwise goes beyond basic needs for assistance compared to the majority of other Data Controllers. The remuneration is calculated on the basis of the Data Processor's hourly rates and expenses incurred for external assistance, including from sub-processors or advisers. The Data Controller may request information about the rates in connection with requesting such assistance.

D.3. Applicable terms specifically to international company groups with affiliates outside the EU/EEA (Summit provides services as a sub-data processor)

1. If it is specifically agreed between the Parties that the Data Processor shall provide services to the Data Controller's subsidiaries or affiliates established in third countries (outside the EU/EEA), such agreement must be considered as a tripartite agreement. In said tripartite agreement, i) the Data Controller's subsidiary or affiliate is regarded as an independent data controller (in this section defined as "Subsidiary Data Controller"); ii) the Data Controller is regarded as a data processor processing personal data on behalf of and as instructed by its subsidiary or affiliate (in this section the Data Controller is defined as the "Group Data Processor"); and iii) the Data Processor is regarded as the sub-processor ("Sub-Data Processor") engaged by the Data Controller (i.e. the Group Data Processor).

2. In terms of provision of the services to the Subsidiary Data Controller, the Sub-Data Processor is regarded to be solely engaged by the Group Data Processor and is only processing personal data under the instructions from the Group Data Processor. The Group Data Processor must ensure that these instructions are fully in compliance with the instructions provided by the Subsidiary Data Controller to the Group Data Processor. The Group Data Processor shall remain fully liable to the Subsidiary Data Controller for the Sub-Data Processor's performance of its obligations. Without changing the foregoing, communication about the practicalities related to performance of the services, including order forms, may be between the Sub-Data Processor and the Subsidiary Data Controller.

3. The Group Data Processor undertakes to ensure that the transfer of personal data from the Subsidiary Data Controller to the Group Data Processor and the further transfer of such personal data from the Group Data Processor to the Sub-Data Processor for the purpose of delivering services to the Subsidiary Data Controller located in a third country is in accordance with mandatory law, which the Subsidiary Data Controller is subject to.

4. The Group Data Processor undertakes to ensure that any transfer of personal data from EU/EEA to the third countries where Subsidiary Data Controllers are established is in accordance with applicable data protection legislation, including the GDPR, and shall be held fully liable for any damage suffered by the Sub-Data Processor by any lack of such compliance with applicable data protection legislation, including the GDPR. This includes, but is not limited to, an obligation for the Group Data Processor to

prepare transfer impact assessments, the establishment of a legal basis for the transfer of Personal Data to the specific third country and the implementation of sufficient supplementary measures, etc., provided and to the extent it is required.

5. Where the Group Data Processor fails to fulfil its obligations pursuant to this section., the Group Data Processor shall remain fully liable for any damages suffered by the Sub-Data Processor.

6. In the event of conflict between the clauses in this section and other clauses in these Clauses, in the Agreement or in any other agreements between the Parties, the clauses of this section shall prevail.

D.4. Liability

1. In the event that liability to pay damages, compensation, tort or the like to data subjects, other relevant data subjects or third parties, has been imposed on one Party (the paying party) due to violations of data protection legislation, these Clauses, privacy notices, instructions to the Data Processor or the like, and the other Party (the responsible party) is fully or partly responsible for such violation, the responsible party shall indemnify the paying party with a proportionate share of the amount (including any related costs or fees) corresponding to the proportionate share of liability that is incumbent on the responsible party.

2. If one Party (the paying party) has been imposed to pay an administrative fine, fines or the like to public authorities or bodies or the like, due to a violation of data protection legislation, these Clauses, privacy notices, instructions to the Data Processor, or the like, and the other Party (the responsible party) is fully or partly responsible for such violation, the responsible party shall – to the extent permitted by applicable law - indemnify the paying party with a proportionate share of the amount (and any related costs and fees) corresponding to the proportionate share of liability that is incumbent on the responsible party.

3. If the Data Processor has paid full compensation for the damage suffered by a data subject, the Data Processor shall have claim of recourse against the Data Controller so that the final amount paid by the Data Processor does not exceed the amount set out in below section D.4.4.

4. Notwithstanding anything to the contrary, the total liability of the Data Processor, including its affiliates, is limited to the amount which has been invoiced to the Data Controller in a period of six (6) calendar months prior to the month in which the loss incurred (but shall in no event exceed a maximum of DKK 100,000) for all aggregate damages and/or claims or the like that may arise from the Data Processor's performance of the services or in connection with these Clauses and this section D.4.

5. Neither Party limits nor excludes any liability that cannot be limited or excluded under applicable law.

D.5. Law and Venue

1. Any dispute arising from these Clauses shall be governed by the laws of Denmark, irrespective of any conflict-of-law principles, which may result in the application of the laws of another jurisdiction. The Courts of Denmark have exclusive jurisdiction to settle any dispute arising out of or in connection with these Clauses.
2. The Parties agree that the competent supervisory authority is the Swedish Data Protection Authority.

Appendix E – Technical and organisation safety measures

The level of security shall take into account:

- Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Data Processor must implement an appropriate level of security.
- That the processing involves a limited number of personal data which are subject to Article 6 of the GDPR.
- The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.
- The Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller.[2]

Category	Detailed description of measures
Measures of pseudonymisation and encryption of personal data:	We use Microsoft 365, including hosted services like SharePoint, OneDrive, Exchange, and Teams, and thus reference is made to Microsoft 365 GDPR compliance and documents. Files are encrypted in transit and at rest. Emails are encrypted with forced TLS in transit when supported by the recipient. Office 365 Message Encryption is used when deemed necessary to ensure encryption at transit and rest. Azure Rights Management is used to ensure data lifecycle management for specific data classifications. End-to-End encryption is used for chats, messages, and files in transit between recipients using Microsoft Teams. Teams uses forced Transport Layer Security TLS and MTLS to encrypt instant messages, Secure RTP (SRTP) for media traffic and FIPS (Federal Information Processing Standard) compliant algorithms for encryption key exchanges. DANE is utilized in Exchange Online when supported by Microsoft 365, thus mitigating risks of man-in-the-middle attacks. It provides an extra layer of verification on top of existing SSL/TLS certificate systems, making spoofing and interception more difficult. Microsoft Defender for Endpoint is enabled to ensure devices are protected against viruses and suspicious behaviour. Morphisec Guard is deployed to protect against zero-day exploits.

[2] These measures do not include the online platform(s) such as HALO but are solely the Data Processor's security measures

	All mobile devices are mandated to use Outlook with enforced App Protection Policies, and to run with up-to-date operating systems and application versions. The setting for iOS updates in employee mobile phones is per default set to automatic. Laptops are updated automatically once every week, and any new updates take effect the first time the laptop connects to the internet after that.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.	Microsoft Defender for Endpoint is enabled to ensure devices are protected against viruses and suspicious behaviour. Morphisec Guard is deployed to protect against zero-day exploits. All mobile devices are mandated to use Outlook with enforced App Protection Policies, and to run with up-to-date operating systems and application versions. The setting for iOS updates in employee mobile phones is per default set to automatic. Laptops are updated automatically once every week, and any new updates take effect the first time the laptop connects to the internet after that.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	Summit has an offsite backup of data stored in the Microsoft 365 platforms. The backup is handled by Acronis, with a minimum of 180 days retention. This is located at the Acronis Cloud Backup ISO27001 certified datacentre in Frankfurt, Germany.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.	Supporters regularly assess and evaluate the effectiveness of their technical and organisational tools implemented with Summit. This ensures that workstations and software always is up to date. For further details: https://www.70253515.dk/media/driftsprocedurer.pdf
Measures for user identification and authorisation.	We use Microsoft 365 and access to all systems and services using Entra ID as identity provider, are forced to use strong passwords. Other critical systems incl. the online platform (HALO and Hogan Talent (HT)) uses similar measures. The Summit password expiration policy has been configured to enforce a 90-day validity period. This measure is implemented to mitigate the risk of potential data breaches resulting from compromised or outdated passwords. MFA is required to gain access to the Hogan online services and Microsoft 365 services. Security groups are created and maintained by Supporters.
Measures for the protection of data during transmission.	We have deployed industry-standard encryption protocols for data in transit. All user sessions are encrypted via enforced SSL/TLS 1.2. MDM policy disables Wi-Fi sense auto connect and blocks all incoming traffic. Organizational policy forces users to use mobile hotspot instead of free Wi-Fi. Microsoft Exchange Online Protection spam filter is implemented to identify and quarantine spam, safeguarding our communication channels from unwanted distractions and security threats. All emails

	are being scanned by a cloud-based scanning engine to minimize phishing attacks as well. In addition, all links and attachments are scanned by the scanning engine. A DMARC Reject policy is implemented to improve email security measures against email spoofing and phishing attacks ensuring that only authorized emails are sent under our domain protecting against unauthorized or malicious activity. DNSSEC has been implemented for summitlead.com and our sub-processor domain hoganassessments.com, so that users can be sure that the correct page is displayed when linking to our website and when the direct URL is used.
Measures for the protection of data during storage.	We have deployed industry standard, non-proprietary, encryption techniques for data at rest. • Data is encrypted on laptops. • Data in storage on servers (SharePoint Online) is encrypted. • Data backups in storage on data backup systems are encrypted. BitLocker is used in Microsoft datacentres. BitLocker and FileVault is also used on client machines, such as Windows and macOS computers.
Measures for ensuring physical security of locations at which personal data are processed.	Alarm system in the office and employee access cards. Guests are escorted in and out of the office.
Measures for ensuring events logging	Standard Microsoft logging and retention of logs.
Measures for ensuring system configuration, including default configuration.	Secure Configuration Management Policy is maintained and reviewed annually by Summit with assistance of Supporters. The purpose of this policy is to establish standards for the base configuration of internal computers that are owned and/or operated by us. We have established standards for the base configuration of internal computers that are owned and/or operated by us. Configuration management is performed by Supporters. Software downloads need approval either from a pre-approved list or from management.
Measures for internal IT and IT security governance and management	We use Supporters for our IT support and operations.
Measures for ensuring data minimisation	Conduct annual review to evaluate the suitability of existing retention and deletion policies. Auto deleting e-mails in trash is set up to 30 days and other emails as a main rule: 5 years. Summit will conduct annual awareness training of our information security policy for employees to store data correctly and align with the auto deletion set-up.
Measures for ensuring limited data retention	Company retention policies.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.	Included in our DPA/SCC with sub-processors.